SpEED-IoT: Spectrum Aware Energy Efficient Routing for Device-to-Device IoT Communication

Saptarshi Debroy[1], Priyanka Samanta[1], Amina Bashir[1], Mainak Chatterjee[2]
[1]City University of New York, [2]University of Central Florida
Emails: saptarshi.debroy@hunter.cuny.edu, psamanta@gradcenter.cuny.edu, amina.bashir80@myhunter.cuny.edu, mainak@eecs.ucf.edu

Abstract

In order to meet the growing demands for high-throughput, cost-effective, and energy efficient solution for the emerging device-to-device (D2D) based Internet of Things (IoT) communication, Dynamic Spectrum Access (DSA) and sharing based protocols have been proposed. However, due to the temporal and spatial transience of spectrum utilization by licensed incumbents, optimal spectrum resource management becomes critical for: a) effective D2D communication without disrupting the licensed incumbents, and b) sustained operation in a multi-hop mesh environment due to the inherent energy constraint of IoT devices.

In this paper, we propose SpEED-IoT: Spectrum aware Energy-Efficient multi-hop multi-channel routing scheme for D2D communication in IoT mesh network. We assume the knowledge of a radio environment map (REM) obtained through dedicated spectrum sensors that capture the spatio-temporal spectrum usage. We exploit such REMs to propose a multi-hop routing scheme that finds the: (a) best route, (b) best available channels at each hop along the route, and (c) optimal transmission power for each hop. SpEED-IoT also employs an evolutionary game theoretic route allocation model to sustain parallel D2D communication. SpEED-IoT ensures: i) licensed incumbent protection, ii) IoT device energy preservation, iii) effective end-to-end data rate optimization, and iv) fast convergence and fair route assignment among interfering D2D communications. Through simulation-driven GENI-based IoT testbed, we evaluate SpEED-IoT's performance in terms of: a) ensuring connectivity and reachability among the IoT devices under varying spectrum usage conditions, b) data rate optimization of the assigned routes and the overall IoT network, c) effectiveness in licensed incumbent protection, and d) degree of fairness while assigning routes to multiple interfering devices.

1 Introduction

With the proliferation of Internet of Things (IoT) based applications in fields such as manufacturing, energy, transportation, healthcare, and emergency/disaster response, autonomous deployments of large scale IoT networks will ace the burden of hauling large volume of produced and consumed data. Since most of the IoT devices are expected to be connected wirelessly, there will be an unprecedented need for higher capacity wireless networks. Naturally, the current wireless networks that operate on the Industrial, Scientific and Medical (ISM) or licensed bands will fall short. As a remedy, *dynamic spectrum access* (DSA) and sharing have been proposed as a high-throughput, cost-effective solution for the growing demands [11]. Using DSA, unlicensed (i.e., secondary) IoT devices will opportunistically use the underutilized or unused channels for licensed or primary users/network (PU). In recent times, DSA based solutions are being proposed and pursued for the growing demands of commercial networks [14], smart cities with smart vehicular networks (VANET) [16], smart grids [21], and military communications [52], to name a few. Since

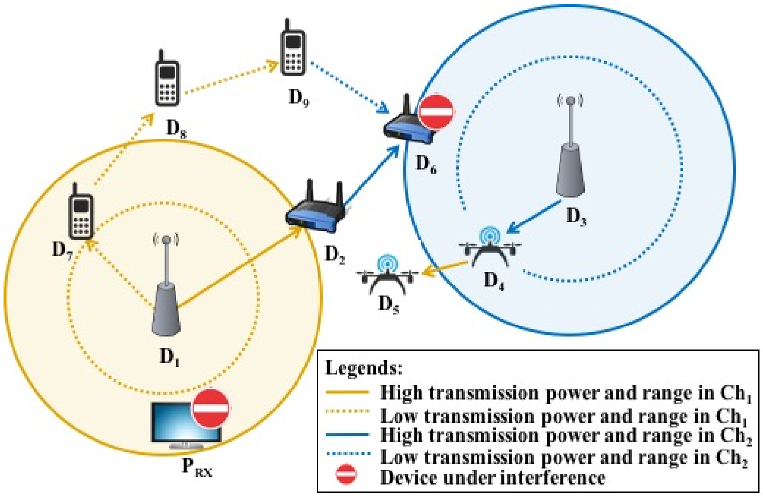

D$_9$
D$_8$
D$_6$
D$_3$
D$_7$
D$_2$
D$_4$
D$_5$
D$_1$
P$_{RX}$
Legends:
High transmission power and range in Ch$_1$
Low transmission power and range in Ch$_1$
High transmission power and range in Ch$_2$
Low transmission power and range in Ch$_2$
Device under interference

Figure 1: Inefficient multi-hop routing among secondary IoT devices causing interference to primary receivers and other hidden/exposed IoT devices

the spectrum availability is space and time variant, selection of the best among the available channels between a given pair of IoT devices becomes very crucial. This is especially true for Device-to-Device (D2D) communications, such as [12, 39] where data needs to be routed over multiple hops. Sophisticated multi-hop routing algorithms are needed that can find the best end-to-end route in terms of quality of service (QoS) metrics and the best channels at each hop.

The primary challenges for such multi-hop D2D IoT communications in using DSA over dedicated spectrum are: a) the need for spatio-temporal spectrum-awareness in terms of finding unused or underused channels at different locations along an end-to-end route, b) protecting licensed primary transmission on channels when and where they arrive from harmful interference caused by secondary IoT communication, and c) ensuring power controlled IoT communication to maintain the strict energy preservation requirements of the IoT devices. Due to these reasons, the state-of-the-art Internet routing protocols, such as, LSR [35], and OSPF [42], or traditional wireless mesh network routing protocols, such as, DSR and AODV cannot be seamlessly applied to DSA based IoT communications. Figure 1 shows one such scenario where an inefficient multi-channel route from source IoT device (D_1) to the destination (D_6) yields harmful interference to primary receiver (P_{RX}) when an alternate multi-channel route ($D_1 \rightarrow D_7 \rightarrow D_8 \rightarrow D_9 \rightarrow D_6$) is available that ensures primary protection as well as uses low power transmission (leading to multiple hops) ensuring energy preservation. The figure also shows that such suboptimal transmission power and route selection can cause interference among parallel D2D communications due to hidden/exposed terminal problems. In the example shown in Figure 1, D_6 is exposed to D_3's signal due to the usage of the same channel Ch_2. Such interference could have been avoided by intelligently choosing a lower transmission power that is just sufficient to reach D_4 but not as much that interferes with D_6. Therefore, designing efficient multi-hop routing solutions for secondary D2D IoT communication requires IoT network to be tightly coupled with real-time spectrum awareness such that the IoT devices can be continuously aware of the surrounding physical and spectral environment.

The traditional cognitive radio [20] enabled DSA networks achieve such coupling using devices that are sensing capable and perform local spectrum availability optimization. However, such techniques are useless for IoT networks as the device level spectrum sensing adds considerable time and power overhead on the already constrained IoT devices. As a solution, Federal Communications Commission (FCC) has recently proposed a network of dedicated spectrum sensors called Environmental Sensing Capability (ESC) [3, 13] to detect the presence of primary incumbents to aid secondary access, such as IoT communications. The recent advancements in developing ESC-driven radio environment or spectrum maps (REM) [18, 19, 23, 33] can work as ideal spectrum availability references that provide accurate and up-to-date spectrum availability visualization to the IoT network for a vast geographical region. Such spectrum map aided multi-channel routing scheme for multi-hop D2D IoT communication can: a) help find best end-to-end routes in terms of best hops and best channels at each hop, and b) suggest optimized transmission power at each hop that protects primary incumbents in the vicinity and also achieved energy efficiency.

In this paper, we propose SpEED-IoT: Spectrum aware Energy-Efficient multi-hop multi-channel routing scheme for D2D communication in IoT mesh network. SpEED-IoT utilizes a dedicated ESC to sense and build a spectrum map and use the spectrum availability information to identify the best possible end-to-end routes in terms of intermediate hops, and the best channel to use at each hop. With the help of the map, the sensors also compute the optimal power for each device and for each channel which simultaneously protects primary incumbents and other ongoing secondary IoT communications in the vicinity. The transmission power control proposed in SpEED-IoT uses a *selective flooding* technique to limit the overhead of route request forwarding and thereby preserves precious energy resources of the IoT devices. Through thorough analysis, we show that under different network connectivity conditions, SpEED-IoT maximizes end-to-end network performance metrics, such as, achievable data rate. For simultaneous and conflicting secondary IoT end-to-end route assignment, SpEED-IoT employs an evolutionary game theoretic approach played on behalf of the interfering end-to-end D2D routes. By analyzing the game, we show that there exists an equilibrium that the sensors can enforce which maximizes overall network performance and also achieves fairness unlike ad-hoc or greedy based route assignments.

Finally we evaluate SpEED-IoT through a rigorous simulation-driven GENI [1] based IoT testbed model. The results show that under realistic ESC parameters, SpEED-IoT ensures close to 100% D2D connectivity in the IoT network, or in other words, there will always exist at least one route from any IoT device to any other. The results reflect that when power control is used, the number of possible end-to-end routes decreases, but it still ensures reachability between source and destination device. The results show that SpEED-IoT power control achieves on average 70% transmission power reduction against traditional non-power controlled schemes. The results also show how SpEED-IoT ensures 100% primary receiver protection under different IoT network parameters. The results demonstrate how the SpEED-IoT game theoretic approach ensures fairness and overall IoT network data rate optimization unlike other spectrum agnostic and spectrum aware greedy route assignment schemes. Overall, the salient contributions of this work are as follows:

- The proposed SpEED-IoT routing scheme uses spectrum availability information from radio environment maps to guarantee incumbent and ongoing secondary communication protection.
- Through *selective flooding*, SpEED-IoT limits route request forwarding overhead and preserves critical energy

resources of IoT devices.

- SpEED-IoT employs an evolutionary game theoretic approach in provisioning end-to-end routes to competing IoT devices that maximizes achievable channel performance without compromising fairness.
- The simulation-driven GENI based IoT testbed evaluation results demonstrate close to perfect primary incumbent protection with 70% reduction in IoT transmission power while achieving close to 100% D2D connectivity under realistic conditions.

The rest of the paper is organized as follows. Section 2 discusses the related work in this area. Section 3 presents the system model. Section 4 presents the proposed power controlled routing scheme. Section 5 discusses the mathematical and game theoretic analysis of the proposed scheme. Section 6 describes the performance evaluation and results. Section 7 concludes the paper.

2 Related works

In recent times, multi-hop routing protocols have been proposed for D2D IoT networks, such as, [6, 28, 29, 37, 27, 26, 24] that mostly used licensed spectrum. In [27], authors discuss the applicability of IPv6 Routing Protocol for low-power and lossy networks (RPL) for de-facto routing standard in IoT networks. In [29], the authors propose a content centric routing scheme where end-to-end routing paths are determined by content. This scheme also aims to reduce energy consumption by managing redundant transmission. Authors in [28] propose a scalable routing architecture using Bloom Filters for mobility management in IoT applications. In [37], the authors present a distributed geographic-based multicast routing protocols for IoT applications where they seek to reduce the number of transmission links and shorten path lengths in the constructed multicast paths. Authors in [26, 24] propose multicast, multi-path routing for IoT networks with specialized functions such as, multimedia applications and fault tolerant communications respectively. In [6], the authors propose LinGO, a link quality and geographical beacon-less opportunistic routing scheme for efficient video dissemination for mobile IoT network. LinGO supports transmission of video flows, which can be delivered to multimedia platforms for further processing and analysis. Most of these works are only applicable for IoT networks working on dedicated spectrum as primary incumbents.

DSA based end-to-end routing protocols are broadly categorized into two main classes: full spectrum knowledge [4, 25, 48, 51] and local spectrum knowledge [8, 15, 17, 22, 38, 45, 46]. Although these works make valid contributions, most of them fail to guarantee primary receiver protection and optimize desired routing performance metric at the same time. Also most of these works require the secondary devices to be cognitive radio enabled which adds too much energy overhead on the IoT devices. The authors in [51] propose a comprehensive framework to jointly address channel assignment and routing in semi-static multi-hop cognitive radio networks. In this work, the PU dynamics are assumed to be low enough such that the channel assignment and the routing among secondaries can be statically designed. In [25], the focus is on the problem of designing efficient spectrum sharing techniques for multi-hop secondary networks. It introduces a Mixed Integer Non-Linear Programming (MINLP) formulation whose objective is to maximize the spectrum reuse factor throughout the network, or equivalently, to minimize the overall bandwidth usage throughout the network. A graph structured based approach is proposed in [4], where a colored graph is used to represent the network topology. Route and spectrum selection in networks with single transceiver half duplex cognitive radios are addressed in [48]. The proposed solution decouples routing and channel (spectrum) assignment.

Among the notable works on routing protocols with limited/local spectrum knowledge, the distributed algorithm presented in [45] addresses the scheduling, power control, and routing problems simultaneously. Authors in [15], introduce a metric for multi-hop secondary networks which is aware of both the switching delay between frequency bands and back-off delay within a given frequency band. In [46], a distributed resource management strategy to support video streaming in multi-hop secondary networks is presented. The Spectrum Aware Mesh Routing (SAMER) proposed in [38] is a routing protocol that accounts for long term and short term spectrum availability. SAMER seeks to utilize available spectrum blocks by routing data traffic over paths with higher spectrum availability, without ignoring instantaneous spectral conditions. Link stability is considered in [8] where link stability is associated to the overall route connectivity via a mathematical model based on the Laplacian spectrum of graphs. In [22], a route stability oriented routing analysis and protocol are presented where a novel definition of route stability is introduced based on the concept of route maintenance cost. In [17], SEARCH routing protocol is designed for mobile multi-hop secondary networks based on geographic forwarding principles.

In recent times, cognitive radio based spectrum aware IoT networks that operate have been proposed for 5G applications such as, smart grid [32, 31]. Among the recent works that propose unlicensed spectrum access schemes by IoT networks, [53, 36] are notable. Authors in [53] propose a learning algorithm based spectrum access scheme for cognitive radio enabled IoT network comprising of wireless sensors that tries to maximize the overall system throughput. In [36], the authors analyze the possibility of using underutilize FM spectrum for low-power short-range IoT devices enabled with cognitive radio devices. Among the works pertaining to DSA based D2D communications in IoT networks, [10] is notable where the authors propose CEEA, a data delivery scheme for large-scale IoT networks for disaster management. However, most of such works assume an over-conservative primary contour protection scheme which considerably decreases the achievable secondary throughput.

3 System Model and Background

We consider a geographic region consisting of a primary network, secondary network comprising of IoT devices, and a collection of sensors comprising the ESC that periodically sense primary activity and create a spectrum map.

Primary network: In this work, we consider a centralized primary network consisting of licensed base stations as transmitters and a collection of receivers associated with such base stations, e.g., cellular networks, TV bands [7]. The

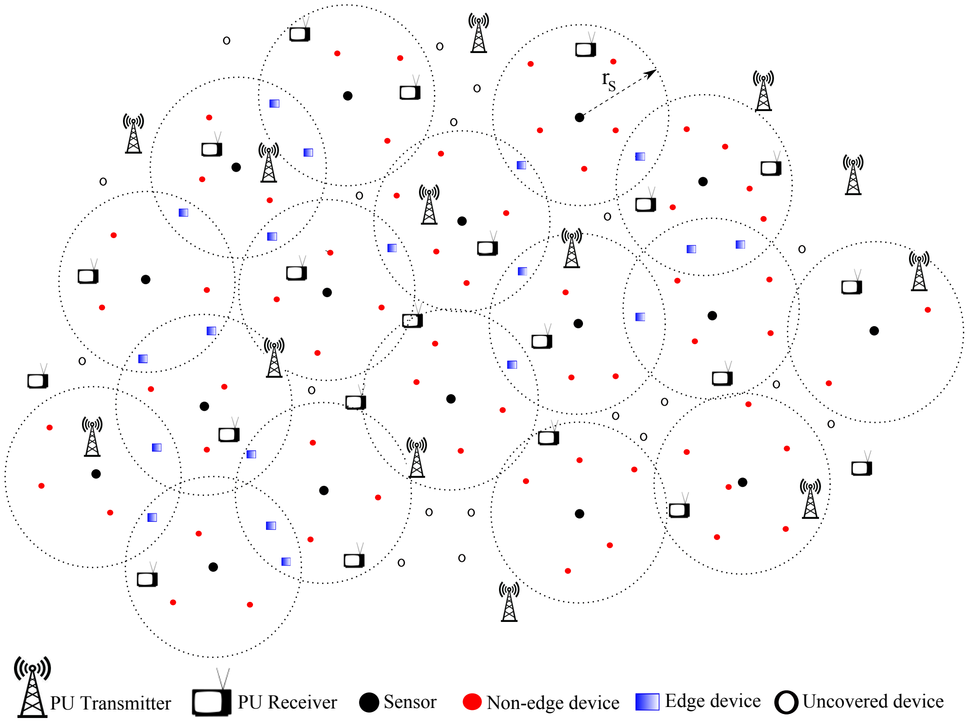


Figure 2: Proposed IoT network environment with primary transmitters, primary receivers, ESC sensors, edge, non-edge, and uncovered IoT devices

primary networks operate independent of the secondary IoT devices. These primary networks have prioritized access to the licensed spectrum. For our analysis, and later simulation, we assume that the primary base station and receiver locations are Poisson distributed as characterized in [41] for centralized TV transmitters. These primary transmitters operate on pre-defined channels and follow the well-known ON-OFF [30, 49] model for transmission pattern. We assume that the signal strength diffuses isotropically in the environment and is received at any location with a power reduced due to isotropic dispersion and absorption in the environment. For our analysis, we do not assume any fixed transmission range/radius for the base stations as assumed in works with Boolean model [34, 40]. Rather, we use more fundamental computation of received signal to noise ratio at any location to determine the presence of the primary at any location and analyze network connectivity [9].

Environmental sensing capacity: We assume that the sensors comprising the ESC are deployed in the area of interest either at strategic locations or randomly depending on the technique used for the construction of the spectrum map. Each sensor has a transmission range of r_s and secondary IoT devices within the range, i.e., the sensor's domain are under the purview of the sensor. The sensors' responsibilities are broadly two-fold: spectrum map creation and route discovery. The sensors periodically sense the spectrum for primary activities, share the information among themselves and create the spectrum map. The latter function includes receiving route requests (RREQ) from secondary IoT devices within the domain, finding routes to the final destination or local forwarding device based on network topology, and caching potential routes. Sensors communicate with each other using dedicated low bandwidth control channel/s. The same control channel is used to communicate with the IoT devices with the domain as well. The underlying sensor-to-sensor, and sensor-to-device communication details using the dedicated control channel/s in terms of frame structure are properties of medium access control (MAC) protocol and can be integrated with any of the state-of-the-art wireless MAC protocols.

Spectrum map: The spectrum map or REM created periodically by the ESC is a 3-dimensional representation of spectrum utilization in a geographical region [18, 19, 23, 33]. The models/techniques for creating such maps allow secondary networks to compute or predict the spectrum usage at arbitrary locations. Most of these spectrum map construction techniques are flexible enough to be used for varied cross-layer secondary network services ranging from resource allocation, MAC design to routing schemes. Although our proposed routing scheme can utilize any of such map construction techniques, their design and implementation specifics are beyond the scope of this paper. Algorithm 1 describes one such ESC-driven spectrum map creation pseudocode that we used for our analysis and simulation later. Figure 3 presents the visual representation of a spectrum map in terms of power spectral density (PSD) of primary channel usage for one channel of 100 kHz bandwidth using 40 sensing locations [19]. Locations of the sensors used for estimation are shown in darker shades. As discussed in previous works, the accuracy of such spectrum map depends on the number and orientation of the sensor locations.

Algorithm 1: Spectrum map creation algorithm

```
Data: Set of sensor nodes $S^i = \{\delta_i\}$
Data: Sensor radius $r$
Data: Power spectral density $e_q^i$ for each node in $S^i$ for each channel $q$
Result: Estimated power spectral density in a region for each channel
for all locations $(x_t, y_t)$ in the region do
    for all channels $q$ do
        for all sensor nodes $i$ in the set $S^i$ do
            if $0 \leq d_i^t \leq \frac{r}{3}$ then
                $disFact_i^t \Leftarrow \frac{1}{d_i^t}$
            else if $\frac{r}{3} < d_i^t \leq r$ then
                $disFact_i^t \Leftarrow \frac{27}{r}(\frac{d_i^t}{r} - 1)^2$
            for all sensor nodes $k \; \forall \; k \neq i$ do
                $angFact_i^t \Leftarrow angFact_i^t + disFact_i^t \times ((x_t - x_i)(x_t - x_k) + (y_t - y_i)(y_t - y_k))/disFact_i^t$
            end
            $fnlWght_i^t \Leftarrow (disFact_i^t)^2(1 + angFact_i^t)$ $powSpecDnst_q^t \Leftarrow powSpecDnst_q^t + \frac{fnlWght_i^t \times e_q^i}{fnlWght_i^t}$
        end
    end
end
```

Secondary IoT network: The secondary IoT devices seek to access the channels not being used by the primaries. We assume that these IoT devices are deployed irrespective of primary and sensor locations as a two dimensional Poisson point process. The IoT devices are not cognitive radio enabled and thus have no spectrum sensing capability. The devices are instructed by the sensors to use a particular channel intended for a particular destination. According to our SINR model, an IoT device is a transceiver with no fixed transmission range. The connectivity among the devices is a function of the availability of free channels, IoT transmission power, path loss and other propagation characteristics like shadowing and fading. IoT devices that are under the purview/domain of a single sensor are called *non-edge* devices; while IoT devices situated in the overlapping regions/domains of two or more sensors are called *edge* devices. The edge devices can listen to multiple sensors using the control channel. As we mentioned earlier that the details of the MAC design of the control channel is beyond the scope of this work. All the communication among IoT devices and the sensors uses network layer addressing. IoT devices outside the domain of any sensor is an uncovered device. For simplicity of modeling and analysis, in this work we only consider IoT devices that are static or slow moving.

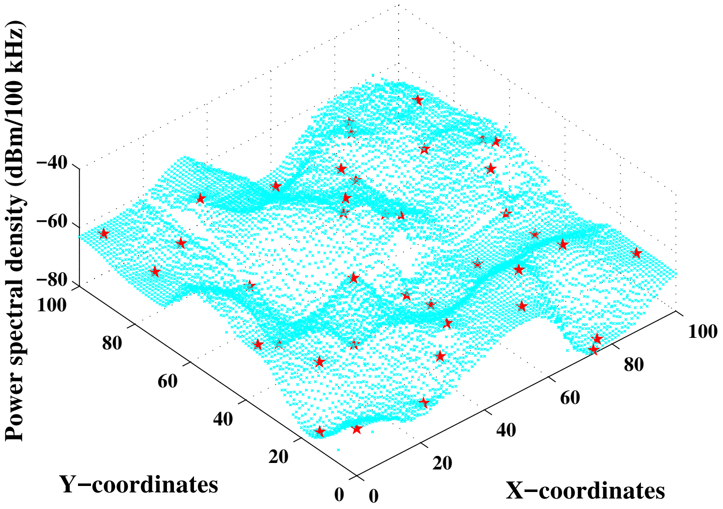


Figure 3: Estimated power spectral density for ESC with 40 sensors

However, the principles of spectrum aware D2D IoT communication proposed in this paper can be easily extended to mobile IoT devices.

Any IoT device requiring route information to a destination initiates a route request to the associated sensor. The sensor, using our proposed SpEED-IoT routing algorithm finds an optimal route to the intended destination based on the availability of free spectrum and relay IoT devices or hops, and orientation of primary receivers. In our model, we also consider scenarios where multiple source-destination (SD) pairs request route assignment with or without channel and hop conflicts increasing the complexity of the route assignment problem. A pictorial representation of the entire system model is shown in Figure 2.

4 SpEED-IoT Scheme Overview

Discovery of a route is initiated when an IoT device sends a route request (RREQ) to the associated sensor on the control channel. SpEED-IoT employed by the sensor seeks to optimize two main aspects in the route establishment: next hop and channel selection to minimize interference and end-to-end data rate maximization, and optimal power control for primary receiver protection.

4.1 Route discovery

A route from source to destination can be of two kinds depending on their relative locations: intra-domain and inter-domain. When the source and destination devices are under the purview of the same sensor then it is called intra-domain and when under different sensors it is inter-domain. We will first discuss intra-domain routing and then explain how inter-domain routing is treated as a collection of intra-domain routing.

4.1.1 Intra-domain routing

A sensor upon receiving the RREQ checks whether the destination is associated with it i.e., is within r_s from it. If so, for each source device i, the sensor consults the most recent spectrum map and eliminates all the channels which are occupied. For all the available channels in the spectrum, the sensor calculates $\overline{P}_i^n$ which is the upper bound on secondary transmission power while using channel n so that no primary receivers are interfered on that channel.

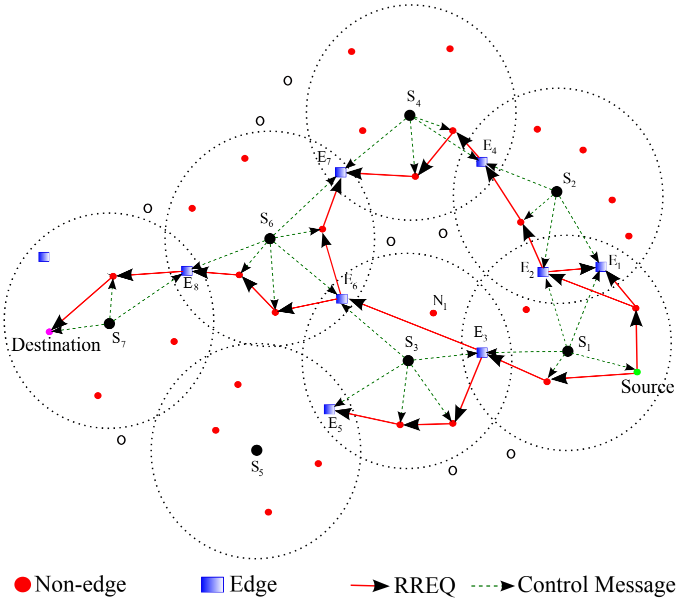


Figure 4: Inter-domain routing: RREQ selective flooding controlled by sensors

Graph creation: We define $\mathcal{P}_i^n = min\{P_{hw}, \overline{P}_i^n\}$ to be the optimum power to be used on channel n which will maximize the channel performance while protecting the primary receivers on that channel. P_{hw} is the maximum secondary IoT transmission power due to hardware constraints and we assume it to be same for all IoT devices. For every device $j(j \neq i)$ within the domain, if $RSS_{ij}^{n}/\eta_{j}^{n} \geq \delta$ then there exists an edge between devices i and j for channel n. Here, RSS_{ij}^{n} is the received signal strength at device j on channel n when device i transmits with power $\overline{P}_{i}^{n}\}$ estimated by the sensor, η_{j}^{n} is the noise on channel n at j from the spectrum map, and δ is the signal to noise threshold for successful IoT communication. The sensor in consideration can easily calculate RSS_{ij}^{n} using any sophisticated pass-loss model; the more sophisticated the model is, better is the estimation. Therefore, for all such n channels between i and j, there exists an edge e_{ij}^{n} from i to j. Each such edge is associated with a cost ζ_{ij}^{n}. Although the cost function can be designed as a complex combination of classical and novel route quality metrics, for simplicity we design the cost as a reciprocal of achievable Shannon's capacity [43] of channel n in order to satisfy the design end-to-end data rate objectives. Therefore,

$$\zeta_{ij}^{n} = Blog_{2}(1 + \frac{RSS_{ij}^{n}}{\eta_{j}^{n}}) \tag{1}$$

which in our case is inversely proportional to the achievable capacity of channel n raised to the power α. The achievable channel capacity is calculated using the bandwidth of channel n and signal to noise ratio $RSS_{ij}^{n}/\eta_{j}^{n}$. With the edges calculated for each SD pair, the sensor creates the connectivity graph within its domain for the current primary usage scenario. By employing any well known shortest path algorithm (such as Dijsktra's), the sensor determines the shortest path between the source and destination within its domain. The shortest path thus contains the next hop network address, channel to be chosen for each hop, and IoT transmission power for each such channel at each hop. Once the path is determined, the sensor sends the routing instructions on the control channel to the all IoT devices working as hops along the route.

$\overline{P}_{i}^{n}$ **estimation:** Evaluating $\overline{P}_{i}^{n}$ is an intuitive reverse calculation to protect primary contour. Let $\overline{d}_{i}^{n}$ be the distance between device i and the nearest location from i where channel n is no longer vacant, called the *safe zone* distance.

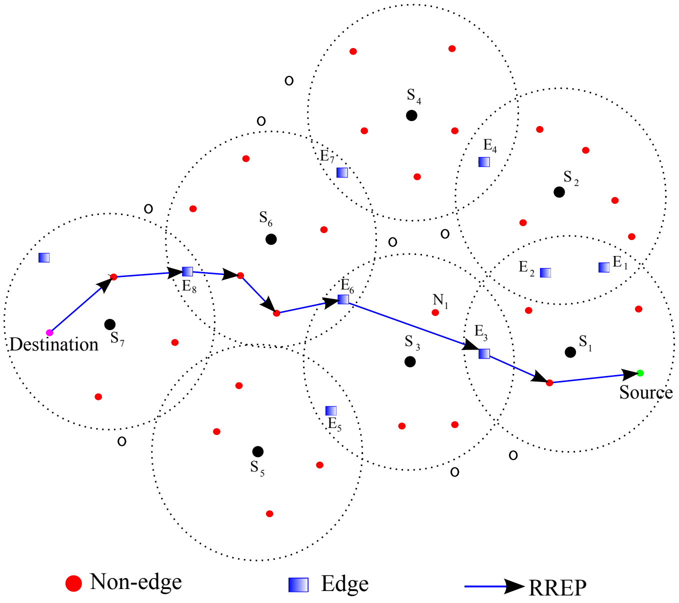


Figure 5: Inter-domain routing: Unicast RREP involving only IoT devices

This distance can easily be measured by the sensor from the spectrum map. Therefore, the circle with radius $\overline{d}_i^n$ with device i at the center has the smallest area where the primary receivers are interference-free on channel n. It is to be noted that this so-called *safe zone* for the primary receivers is independent of the primary receiver distance from the secondary IoT device i. Now if $\overline{RSS}_i^n = f(\overline{d}_i^n, \overline{P}_i^n)$ is the estimated received signal strength at the perimeter of the circle, and κ is the secondary to primary interference tolerance threshold, then to guarantee primary receiver protection,

$$\frac{\overline{RSS}_i^n}{\eta_{sz}^n} \leq \kappa \tag{2}$$

where η_{sz}^n is the noise on channel n at the perimeter of the safe zone. We use a highly sophisticated path-loss model proposed in [5] for the sensors to estimate $R\bar{S}S_i^n$. Therefore $\overline{P}_i^n$ is given as,

$$\overline{P}_i^n = \frac{\eta_{sz}^n \times \kappa \times 16\pi^2 (\overline{d}_i^n)^\gamma}{\lambda^2 d_0^{\gamma-2}} \tag{3}$$

where γ is the average path-loss factor, d_0 is the antenna far field, and λ is the wavelength of light.

4.1.2 Inter-domain routing though selective flooding

When the the source and destination devices are not under the same sensor, the idea is to flood the route request in the neighboring domains. However, due to the inherent energy constrains of the IoT devices, DSR or AODV inspired flooding may not be the best options. Therefore, SpEED-IoT uses a *selective flooding* approach where once the sensor determines the need of inter-domain routing, it finds the shortest route from the source to each of the edge devices within its domain. The edge devices, upon the reception of a RREQ where the edge device itself is not the final destination, forwards the RREQ to the other sensor/s it is associated with. For example for an edge device k having $\{S_2, S_5, S_1\}$ as its sensor association, signifying that k is currently covered by S_2, S_5, and S_1. Such associations are created on k's ability to receive periodic beacons from each of these sensors on the control channel. Once a sensor receives a RREQ from the edge device, it follows the same recursive process of finding a route to the destination or to the edge device until the final destination is found. In case of an edge device receiving same RREQ from generated from two different sources, it forwards the RREQs on first come first serve basis and drops duplicate RREQs. The proposed SpEED-IoT selective flooding considerably decreases the route discovery overhead without compromising the discovery of multiple routes to the destination.

In Figure 4, we show SpEED-IoT selective flooding and explain the duplicate RREQ scenarios. We also show the control messages from sensors directing source, destination, and intermediate relay devices along the route. We show the case of a sensor getting the same RREQ from two edge devices: sensors S_2 and S_4 receive the same route request from E_1,E_2, and E_4,E_7 respectively. However, they only forward the RREQ that arrived first, i.e., RREQs from E_2 and E_4 for S_2 and S_4 respectively. Noticeably S_2 forwards RREQ from E_2 to E_1 as the latter is an edge device, assuming S_2 received RREQ from E_2 earlier to E_1. Now E_1 receiving the duplicate RREQ generated from E_2 simply drops the RREQ. Same set of events happen for sensor S_4 with devices E_4 and E_7. In this figure, we also illustrate power control by relay devices. Edge device E_3 forwards RREQ directly to E_6 bypassing a potential relay device N_1

by transmitting with a seemingly high power. This was achieved because the channel used for transmission between devices E_3 and E_6 was free in a larger geographical region around E_3 and such high secondary IoT transmission power did not cause any interference to the primary receivers around E_3. In Figure 5, we show the RREP packet flow from the final destination to the source. As explained earlier, there is no sensor involvement during the RREP flow.

4.2 Route discovery for multiple interfering SD pairs

When more than one SD pair requires route assignment with potential interference, the route discovery optimization undertaken by the sensor becomes non-trivial. A global optimization approach although benefit the overall secondary IoT network in terms of free channel utilization, such method can prove to be counter-productive for individual SD pairs who logically should always try to maximize their own effective end-to-end data rate. Now, according to our proposed SpEED-IoT scheme, the route discovery responsibility relies with the ESC sensors, rather than the IoT devices themselves in order to preserve energy. Thus in cases of route discovery for multiple interfering SD pairs, the sensors use an evolutionary game theoretic model by treating each interfering SD pair as a selfish player exhibiting non-cooperative behavior and trying to maximize their own payoffs.

The entire route discovery process in such cases are broken down into domain specific route discovery exactly the way route discovery happens for a single SD pair. First the sensor decides whether the final destinations for the requesting routes belong to its domain or not and based upon that the RREQs are decided to be forwarded either to the final destinations or to all the edge devices. In any case, the sensor computes all possible route options for the interfering SD pairs using the optimal power $\mathcal{P}_i^n$ as explained earlier. Next, these possible routes for each of the SD pairs comprise the set of strategies for the players, i.e., the SD pairs. Routes with higher achievable end-to-end data rates (i.e., data rate of the intermediate link that has the minimum data rate in a route) define utility maximizing strategies for the SD pair. The sensor then models the strategy choice outcomes of all SD pairs as either the well known *Reverse battle of sexes game* or *Hawk and dove game* based on the interference scenarios. Then from the outputs of such non-cooperative games that maximize only individual utilities, the sensor evolves the strategies to be chosen by each SD pair by analzing past best strategies and corresponding payoffs and thus leading to a evolutionary stable strategy (ESS) model. Next with the help of replicator dynamics, the sensor will ensure that the ESS is the best overall strategy for long term involving all SD pairs and converge to an equilibrium. In case of intra-domain routing, routes belonging to the equilibrium are thus discovered and are used for RREQ forwarding. In case of inter-domain routing, the best routes thus computed for all the interfering SD pairs end at the edge devices of the sensors from which point the same route discovery method is followed by the next sensor along the route.

4.3 Route maintenance

Route maintenance in secondary IoT network is more involved than traditional wireless networks. Caching routes for future use may not be a great idea as routes can become non-existent due to temporal variation of available channels. In SpEED-IoT, route maintenance is carried out only by sensors as they are aware of the current spectrum usage scenario. Route caching at IoT devices can reduce signaling overhead and latency, but it cannot guarantee primary protection as such sensing disabled IoT devices have no way to gauge primary activity. Therefore, only the sensors are responsible for caching routes. Sensors typically cache only those routes which connect each edge devices to all other edge devices in their domain. This is because those routes connecting the edge devices are the most popular routes for inter-domain routing and in most cases include subsets of intra-domain routes as well. Sensors use the cached route only when there is negligible change in the spectrum maps. Secondary IoT devices along such cached routes automatically benefit from such caching.

5 SpEED-IoT Analysis

In this section, we analyze SpEED-IoT performance in terms of IoT network connectivity and existence of an equilibrium in game theoretic route discovery for interfering SD pairs. Here we assume a deployment of ESC sensors in a deterministic grid pattern equidistant from horizontal and vertical neighbors for relative simplicity of analysis. However, the principles of our mathematical deduction hold true for any deployment of sensors and IoT devices. We consider a grid of $l \times l$ dimension as our area of interest. The distance d_{ij} between sensors i and j are kept in such a manner that every sensor domain overlaps with the four neighboring sensors but the overlapping regions of the domains do not overlap with each other. We assume all the sensors with same domain radius r_s. An example of such a deployment is shown in Figure 6. Note, that for the following deployment $\sqrt{2}r_s \leq d_{ij} \leq 2r_s$.

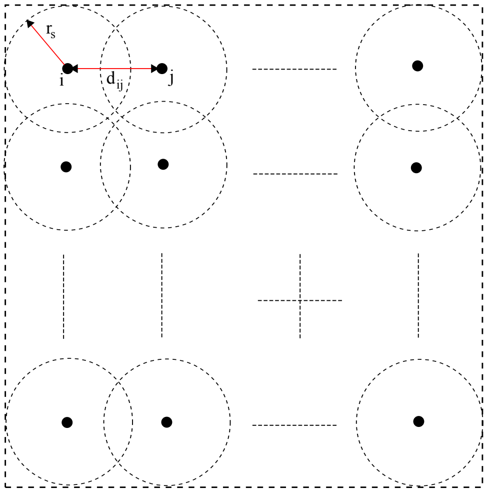


Figure 6: Deterministic grid deployment of ESC sensors for SpEED-IoT analysis

5.1 Ensuring route discovery

For a successful route discovery from any source to destination using our proposed SpEED-IoT scheme requires two conditions to be satisfied: i) both source and destination need to be associated with some sensor, i.e., located in some domains and ii) those domains need to be connected with each other directly or indirectly though other domains.

5.1.1 Edge device probability

The first condition is fulfilled when the source and the destination devices are any edge or non-edge devices under the purview of a sensor.

Definition 1 *Edge device probability is defined as the probability of any IoT device to be an edge device, i.e., be in an* *overlapping region.*

For the above mentioned deployment, the total number of overlapping regions, N_{overlap}, is $2\sqrt{\mathcal{N}_{sen}}(\sqrt{\mathcal{N}_{sen}}-1)$. $\mathcal{N}_{sen}$ is the number of deployed sensors in the grid. The area under each overlapping region is:

$$A_{\text{overlap}} = r_s^2(\theta - sin\theta); \tag{4}$$

where $\theta = 2\tan^{-1}\left(\frac{\sqrt{4r_s^2-d_{ij}^2}}{d_{ij}}\right)$. Therefore edge device probability can be expressed as:

$$p_{edge} = \frac{N_{\text{overlap}} \times A_{\text{overlap}}}{l \times l} \tag{5}$$

The expected number of edge devices is:

$$\text{E[Number of edge devices]} = \mathcal{N}_{IoT} \times p_{edge} \tag{6}$$

where $\mathcal{N}_{IoT}$ is the number of IoT devices in the secondary network, i..e, in this case, the grid. Using an ideal combination of higher $\mathcal{N}_{sen}$ and r_s, if we can ensure zero uncovered devices, then non-edge device probability can be expressed as:

$$p_{non-edge} = 1 - \frac{N_{\text{overlap}} \times A_{\text{overlap}}}{l \times l} \tag{7}$$

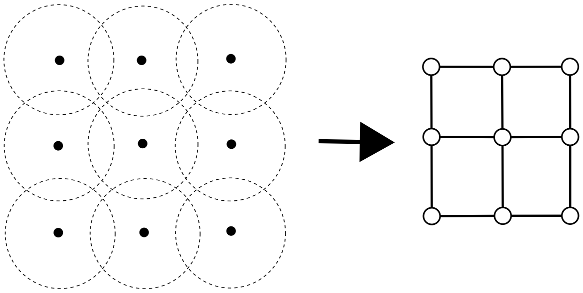


Figure 7: Sensor deployment mapping to an undirected grid

5.1.2 Connectivity condition

The second condition is dependent on the overlapping regions of the domains and presence of edge devices in those overlapping regions. This is because, edge devices are essential for inter-domain RREQ flooding. The number and locations of such overlapping regions in turn depend on the deployment of the sensors and their relative orientation. We further investigate the conditions that dictate the connectivity of sensor domains.

Definition 2 (Connectivity Condition) *The connectivity condition of any secondary IoT network is defined as the sufficient condition for the existence of at least one path from any domain to all other domains in the network.*

We formulated the *Connectivity Condition* by mapping the secondary network into a connected undirected graph with domains as vertices and overlapping regions as the edge between the vertices as shown in Figure 7.

Definition 3 (Mapped Graph) *The graph representation of a secondary network with domains as vertices and overlapping regions as edges is called a mapped graph.*

Lemma 1 *The connectivity condition for a secondary IoT network is that there exists at least one edge device at each of the edges of any one of the minimum spanning trees of the mapped graph.*

Lemma 1 provides the connectivity condition of such a mapped graph. A minimum spanning tree (MST) of an undirected unweighted connected graph connects all the devices in the graph and has the minimum number of edges.

proof 1.1 *Let $G_{n\times n}$ be a mapped graph of any above mentioned sensor deployment with n^2 vertices. Let us assume that it has $\tau(G_{n\times n})$ MSTs. Then each such MST has (n^2-1) edges that connect all the vertices. If we remap the MST into a sensor deployment then it represents a network of minimum number of overlapping regions connecting all domains. Presence of any edge device in each of such overlapping regions will guarantee at least one path from all covered devices to all other covered vertices in the secondary IoT network. Thus the total number of overlapping regions is a measure of minimum number of edge devices required for a network to be connected. Hence proved.*

For a secondary IoT network deployment shown in Figure 6, there are $\mathcal{N}_{sen}$ sensors; hence $\mathcal{N}_{sen}$ domains. Therefore the mapped graph of the network will look like a $\sqrt{\mathcal{N}_{sen}} \times \sqrt{\mathcal{N}_{sen}}$ grid. The number of edges in any of the MSTs of such a mapped graph is the count of minimum number of edge devices required for the corresponding IoT network to be connected. If τ is the total number of possible minimum spanning trees in such a grid, then each MST contains $\big(\mathcal{N}_{sen} - 1\big)$ edges.

Therefore, the probability of connectivity condition is given as:

$$\begin{aligned} p_{conn} = \tau \times \text{Prob}\{Z_1 \geq 1, Z_2 \geq 1, \cdots Z_{\mathcal{N}_{sen}-1} \geq 1 \mid \\ Z_1 + Z_2 + \cdots + Z_{\mathcal{N}_{sen}-1} \leq \mathcal{N}_{IoT}\} \end{aligned} \tag{8}$$

where Z_i is the random variable denoting the number of edge devices in the ith edge of the mapped graph. For a $\sqrt{\mathcal{N}_{sen}} \times \sqrt{\mathcal{N}_{sen}}$ square grid, $\tau \approx 3.209^{\mathcal{N}_{sen}}$ for $\mathcal{N}_{sen} \to \infty$ [47, 50]. In Section 6, we will evaluate p_{conn} for a given secondary IoT network deployment.

5.2 Game theoretic modeling and analysis

We assume each interfering SD pair to have a set of $R = \{1, 2, \cdots, r\}$ end-to-end routes where each route has a utility represented by the set $U = \{u_1, u_2, \cdots, u_r\}$ derived from the effective end-to-end data rate of the routes described earlier. This means that the desirable route for a SD pair will have higher data rates. We already discussed that the sensors assume that all the interfering SD pairs are selfish players exhibiting non co-operative behavior in order to maximize their own payoffs. The players, i.e., SD pairs select a strategy/action from a set of action space $A = \{a_1, a_2, \cdots, a_r\}$. These strategies create rules of the game and each strategy results different payoffs of the SD pairs from the set U. Each SD pair has its own route preferences arranged in an non-increasing fashion in terms of effective end-to-end data rate, i.e., the first route in the list is always the first preference. This list of route preferences comprises the strategy/action space of each SD pair, i.e., each action or strategy by a SD pair signifies which route from the ordered list the SD pair is trying to choose and the net payoff is the utility of the routes. If two or more SD pairs choose actions that have an interfering channel/s at any hop along their routes, the net utility for all the SD pairs is considered to be 0.

5.2.1 Game formulation for dynamic networking environment

The interference scenario stated above can generate two generic game situations. In the first case, as each SD pair has its own route metric and thus will choose the best route available to maximize payoff. However, it may so happen that the best strategies, i.e., the best route options for both the SD pairs lead to interference. In other words, if both pairs take their greedy choices, it leads to interference resulting zero payoffs for both. This scenario generates the well known *Hawk dove* game as shown in Table 1.

Table 1: Hawk dove game

	a_k	a_j
a_k	$0, 0$	u_k, u_j
a_j	u_j, u_k	u_j, u_j

In the second game situation, if both pairs play the same strategies or choose their same route preferences, i.e., either their first, or their second, and so on, it will lead to interference resulting zero payoffs for both. This scenario generates the well known *Reverse battle of the sexes* game as shown in Table 2. For these two game matrices, the primary assumption is $u_k > u_j$, where u_k is the payoff for strategy/action a_k if no other pair is selecting routes that conflict with the channels in route k. We will first analyze the game for two route options, i.e., two strategies/actions a_k and a_j. Later in replicator dynamics strategy set, we will include the entire action space $A = \{a_1, a_2, \cdots, a_r\}$.

Table 2: Reverse battle of the sexes game

	a_k	a_j
a_k	$0, 0$	u_k, u_j
a_j	u_j, u_k	$0, 0$

5.2.2 Pure Strategy Nash Equilibrium

From the definition of Pure Strategy Nash Equilibrium (PSNE), we observe that for hawk dove game in Table 1, there are two PSNEs, (a_k, a_j) and (a_j, a_k). In this case, as $u_k > u_j$, when a pair chooses strategy a_j, then choosing a_k by another pair will be strictly dominant strategy over choosing a_j. This is because, if the other pair switches to strategy a_j, then its overall incentive/payoff gets decreased.

For the reserve battle of the sexes game shown in Table 2, there are two PSNEs, (a_k, a_j) and (a_j, a_k). In this case, if one pair chooses strategy a_k, then there is only one dominant strategy for the other pair which is a_j as choosing a_k will be a strictly dominated strategy. Now if the first pair shifts to strategy a_j, then for the other pair there is no strategy other than playing a_k because then strategy a_j will be a strictly dominated strategy. Thus this game has two PSNEs.

5.2.3 Mixed Strategy Nash Equilibrium

Now for both the games, the interfering SD pairs can mix their strategies with probabilities α and β. Thus for both reverse battle of sexes and hawk dove games, the expected utility $EU_m(a_k)$ of SD pair m for choosing strategy a_k is given by $EU_m(a_k) = \alpha u(a_k, a_k) + \beta u(a_j, a_k) = \alpha(0) + \beta u_k$. Similarly, the expected utility $EU_m(a_j)$ of pair m for choosing strategy a_j is given by $EU_m(a_j) = \alpha u(a_k, a_j) + \beta u(a_j, a_j) = \alpha u_j + \beta(0)$. According to the definition of Mixed Strategy Nash Equilibrium (MSNE), it only exists when:

$$
\begin{aligned}
EU_m(a_k) &= EU_m(a_j) \\
\Rightarrow \beta u_k &= \alpha u_j \\
\Rightarrow \alpha &= \frac{u_k}{u_k + u_j} \\
\& \;\; \beta = 1 - \alpha &= \frac{u_j}{u_k + u_j}
\end{aligned}
$$

Therefore, when both pairs select strategies a_k and a_j with probabilities α and β, respectively, then their opponents, i.e., rest of the interfering SD pairs will be indifferent about the outcomes of their choices. This means that all IoT SD pairs in a given region form a polymorphic population in which every SD pair mixes its choice of available routes according to the probability distribution, which is the MSNE for the evolutionary route discovery game. The probability distribution also represents the proportions of the SD pair population adopting different strategies at any given stage of the game. To generalize, the expected utility for any pair m in a $|R|$ route discovery game is given as follows:

$$EU_m(a_i) = \sum_{i=1}^{|R|} u_i.p_i, \forall\, i \in R$$

where p_i represents the probability of a SD pair selecting strategy a_i, i.e., route i and all other SD pairs not selecting route i.

5.2.4 Learning, strategy evolution and converging stability

We have extended the above two player game scenario to multiple interfering SD pairs using an evolutionary game theoretic approach. The idea is to create a multistage game where the set of players learns from the strategy and outcomes of the players playing in the previous stage and evolve their own strategies to maximize profit and eventually achieve equilibrium. This evolutionary behavior of the players perfectly portrays the Darwinian competition for "Survival of the fittest". In this model, the interfering SD pairs will play the game randomly in a pairwise manner and will mix their strategies resulting new payoffs after every stage called *fitness*. Based on the fitness, each SD pair at each stage of the game will learn the other pairs' strategy. Through this process, the pairs will gain knowledge and accordingly modify or evolve their strategies by *replicator dynamic process*. Thus eventually the game will reach a evolutionary stable state (ESS) and can not be invaded by any mutant strategy.

Now let us assume that $\hat{s}$ is an incumbent strategy, s' is a mutant strategy taken by a small portion of population, and $u(\hat{s}, \hat{s})$ be the utility that measures how the incumbent strategy perform against itself. For the strategy $\hat{s}$ to be ESS, it must satisfy the following conditions:

- $u\left(\hat{s}, \hat{s}\right) \geq u(s', \hat{s})$

- if $u\left(\hat{s}, \hat{s}\right) = u(s', \hat{s})$ then $u\left(\hat{s}, \hat{s}\right) > u(s', s')$

where $(\hat{s}, \hat{s})$ is a symmetric Nash Equilibrium.

ESS for PSNE: For the hawk dove game from Table 1, there is no symmetric Nash equilibrium because if the pairs choose the same strategy set $(\hat{s}, \hat{s})$, i.e., (a_k, a_k), the payoff is zero. Whereas, if they choose (a_j, a_j), then the payoff is (u_j, u_j). However, as $u_k > u_j$, so this also cannot be considered as symmetric Nash and hence $u\left(\hat{s}, \hat{s}\right) < u(s', \hat{s})$. For the reverse battle of the sexes game from Table 2, there is no symmetric Nash equilibrium because if the pairs choose the same strategy set $(\hat{s}, \hat{s})$, i.e., (a_k, a_k) or (a_j, a_j), then the payoff is zero and hence $u\left(\hat{s}, \hat{s}\right) < u(s', \hat{s})$.

ESS for MSNE: For the reverse battle of the sexes game from Table 2, if a SD pair selects strategy a_j with probability β then the other pair will select a_k with probability α. Again if the first pair selects a_k with probability α then the other pair will select a_j with probability β. Therefore, in this case $u(\hat{s}, \hat{s}) = \alpha\beta u_k + \alpha\beta u_j = \alpha\beta(u_k + u_j)$. Now we have to calculate $u(s', \hat{s})$ and if we can prove $u(\hat{s}, \hat{s}) > u(s', \hat{s})$ then we can conclude that MSNE is ESS.

In order to do so, we assume a mutant strategy which is greedier than the incumbent strategy by an amount δ so that other pairs either choose more preferred route with higher probability $(\alpha + \delta)$ or lesser preferred route with lower probability $(\beta - \delta)$. Now payoff $u(s', \hat{s})$, i.e., how the mutant strategy works with incumbent strategy is the expected utility of one pair selecting strategy a_k with probability α and another pair selecting strategy a_j with probability $(\beta - \delta)$ and vice versa. Thus $u(s', \hat{s}) = \alpha(\beta - \delta)u_k + \beta(\alpha + \delta)u_j = \alpha\beta(u_k + u_j) - \delta(\alpha u_k - \beta u_j)$. As $u_k > u_j$, therefore the second part of the expression is positive and hence $u(\hat{s}, \hat{s}) > u(s', \hat{s})$. Therefore, we can conclude that the MSNE is ESS for reverse battle of the sexes. Similarly, we can show that for the hawk dove game, the MSNE is ESS as well.

5.2.5 Strategy evolution through replicator dynamics

Let u_0 be the initial fitness of every interfering SD pair, and the average payoff of pairs selecting route k at a given stage of the game can be calculated as $u_k = u_0 + \sum_{j=1}^{|R|} p_k u\left(a_k, a_j\right), \forall\, k, j \in R$. Here $u\left(a_k, a_j\right))$ is the fitness of a SD pair selecting route k in a pairwise competition against another pair selecting route j, and p_k is the proportion of the interfering SD pair population that selects route k at any given time. If $\bar{u}$ is the average payoff of the entire interfering SD pair population at any given time, then

$$\bar{u} = \sum_{i=1}^{k} p_i u_i, \forall\, i \in R \text{ and } p_k' = p_k + \frac{p_k \left(u_k - \bar{u}\right)}{\bar{u}}$$

where p_k' is the probability of a SD pair selecting channel k for the next stage of the game. This is the replicator dynamics of evolutionary game. This signifies that if selecting route k in the current stage results in a higher average fitness for the SD pairs that selected it than the overall fitness of the entire interfering SD population, then the proportion of the population selecting route k in the next time slot will increase. In other words: a) if $u_k > \bar{u}$, i.e., payoff of selecting route k is greater than the average utility then probability of selecting the same will increase in the next stage, and b) if $u_k < \bar{u}$, then $(u_k - \bar{u})$ will produce a negative result and probability ${p_k}'$ will decrease in the next stage.

6 Performance evaluation

In this section we discuss the performance of our proposed SpEED-IoT scheme using simulation.

Simulation setup: For simulation, we first create a realistic discrete-event simulation environment using C++ and use MATLAB scripts to generate different deployment and network characteristic scenarios. Each such simulation scenario is then integrated in the distributed GENI [1] environment to create new wireless testbeds based on the generated scenarios. Figure 8 shows one such GENI deployment derived from a simulation scenario. The overall environment deployed primary transmitters in a 100×100 geographical area using the deployment models from [41, 2]. For different scenarios, we generate a varying number of channels from 5 upto 20 with 1 MHz bandwidth each. The primary uses a well-known ON-OFF model for transmission [30]. Each primary transmitter has a fixed transmission power of 50 Watts and the primary detection threshold is kept at -116 dBm. For all scenarios, nine sensors are deterministically deployed in a grid pattern as discussed in Section 5. For each GENI implementation, the sensors have direct connections with the domain devices, and devices may or may not be connected to other devices depending on channel availability between them according to the corresponding simulation scenario. Multiple links between the devices signify presence of more than one available channels.

The secondary IoT devices are deployed following a Poisson Point Process to ensure that their locations are not inter-dependent. The maximum IoT transmission power is kept at 100 mW. We used the highly realistic path-loss model proposed in [5] which mimics the real life propagation characteristics in an urban macro-cell. The co-channel interference threshold for primary receivers caused due to IoT communication is kept at -80dBm. On top of implementing our proposed SpEED-IoT routing scheme, we also implemented a greedy wireless route assignment scheme that is spectrum aware but non-power controlled, such as SAMER [38], and a typical IoT D2D channel assignment scheme that is spectrum agnostic, but power controlled due to IoT constraints, such as LinGO [6]. Based on the inputs from the simulation model, we generate outputs from the GENI testbed. Below, we showcase SpEED-IoT performance results, and comparison results (against SAMER and LinGO) based on the testbed outputs.

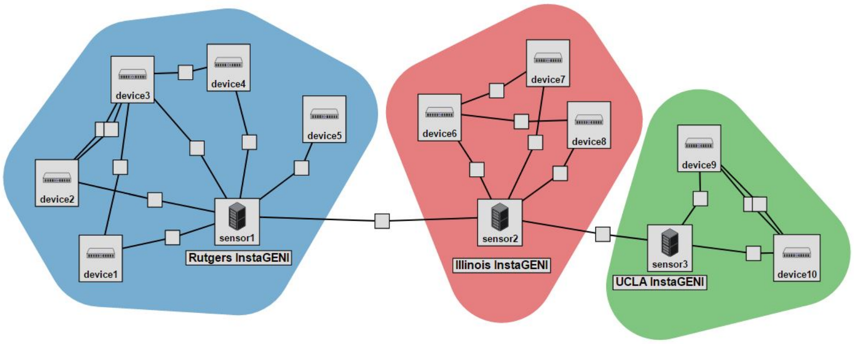
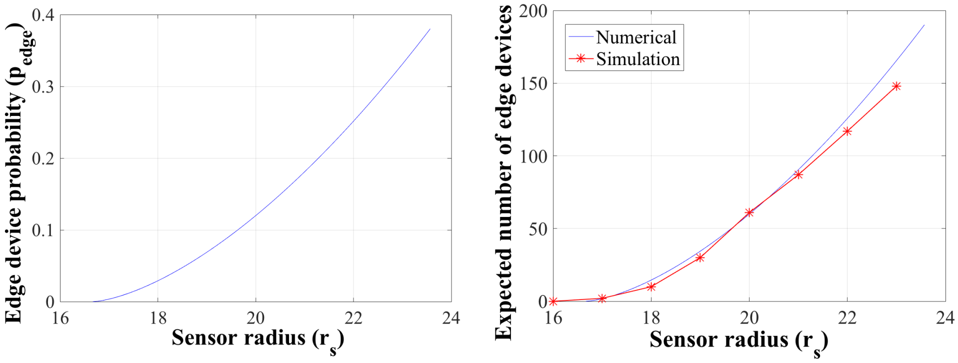


Figure 8: Sample experiment topology in GENI testbed

Edge device probability: In Figure 9(a), we show the nature of probability of edge devices (p_{edge}) with varying radius of sensors, r_s. The value of r_s is varied from $\sqrt{2}r_s \leq d_{ij} \leq 2r_s$ (16 to 24) as this is the range where the domains start overlapping but the overlapping regions do not overlap with each other as discussed in Section 5. We see that within this range of r_s, p_{edge} increases rapidly. In Figure 9(b), we plot Eqn. (6) against the same range of r_s and compare the numerical and simulation values. The simulation results closely match with the numerical trend from Eqn. (6) which in turn validates the mathematical analysis.

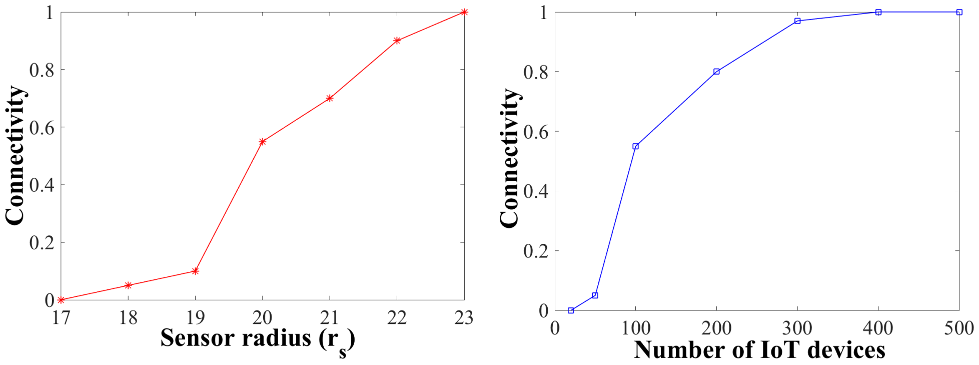


(a)

(b)

Figure 9: (a) Edge device probability with varying sensor radius, (b) Expected number of edge devices for simulation and numerical models

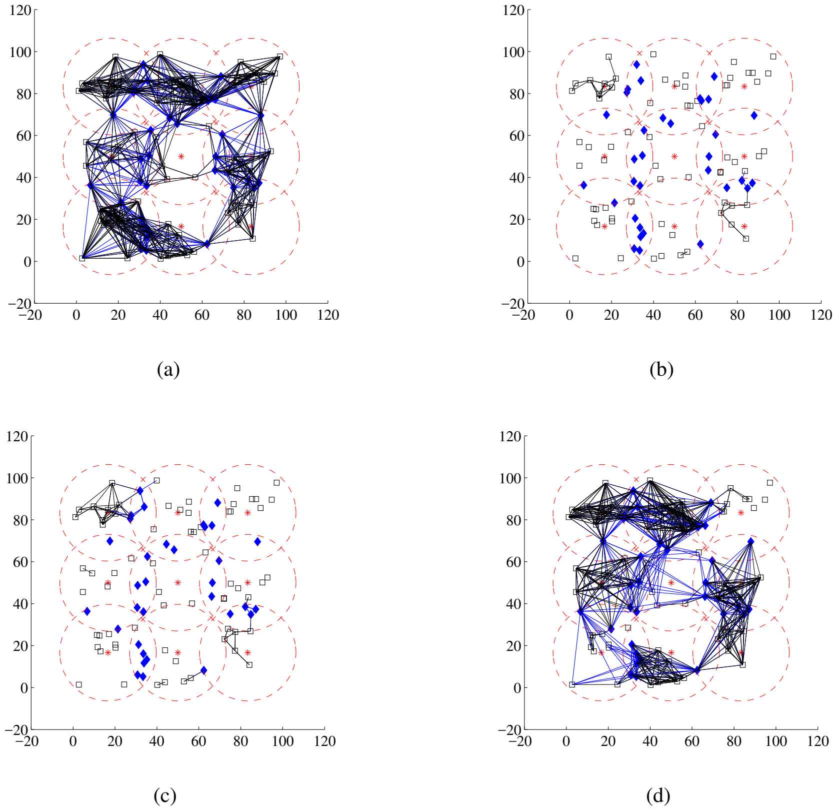
Connectivity: In Figure 10(a), we show how the probability of connectivity p_{conn} varies with r_s. Here N_{IoT} is kept constant at 100. We see as p_{edge} increases with r_s, so does p_{conn}. The IoT network reaches complete connectivity at r_s = 23, i.e., at this point at least one edge device is present on each edge of at least one of the spanning trees of the mapped graph. The nature is obtained by taking average of more than 20 different IoT network topologies. The nature of p_{conn} with varying N_{IoT} is shown in Figure 10(b) with r_s = 20. We see that with a denser network of secondary IoT devices the connectivity increases. With 300 IoT devices, the network is fully connected i.e., there is at least one route from each domain to each other.



(a)

(b)

Figure 10: Probability of connectivity condition with (a) with varying sensor radius, (b) with varying number of secondary IoT devices



(a)

(b)

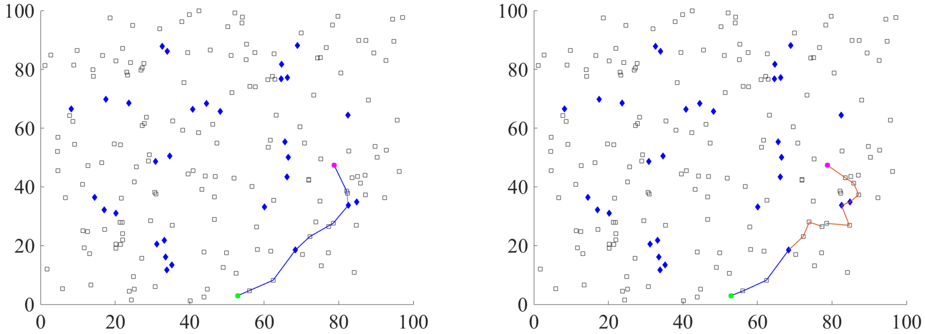
(c)

(d)

Figure 11: Reachability (a) without power control for 5 channels (b) with power control control for 5 channels (c) with power control control for 20 channels (d) with power control control for 5 channels and detection threshold -15 dBm

Reachability: In Figures 11(a)-11(d), we show the reachability among secondary IoT devices with and without power control. Non-edge and edge connections are shown in different colors. In Figures 11(a), we show the reachability with no power control, i.e., the scenario does not take into account the primary hidden terminal problem and thus does not protect any primary receivers that might be present within the IoT device's communication range. It is to be noted that in this scenario each link is bidirectional, i.e., a link represents both devices are reachable from each other. In Figures 11(b) and 11(c), we observe much less reachability when power control is applied on the IoT devices. We see that to protect possible primary receivers, the IoT devices had to use much less power thus the reachability decreases considerably. With more channels in Figure 11(c), the reachability increases marginally. However in Figure 11(d), when we change the detection threshold to -15dBm, which is more comparable with commercial IoT standards, we see reachability increasing even with power control. However, unlike no power control, each link may or may not be bidirectional. This is due to the fact that it is not always true that both devices connecting the links will not cause interference to primary receivers.

Route assignment: In Figures 12(a) and 12(b), we compare end-to-end multi-hop, multi-channel route assignment between the same pair of IoT devices under identical network and channel conditions, with and without SpEED-IoT power control respectively. We see that without SpEED-IoT power control the route takes less number of hops and also uses the same channel throughout the route. However, when we use power control to protect the primary receivers, number of hops increases and also the channels change along the route.

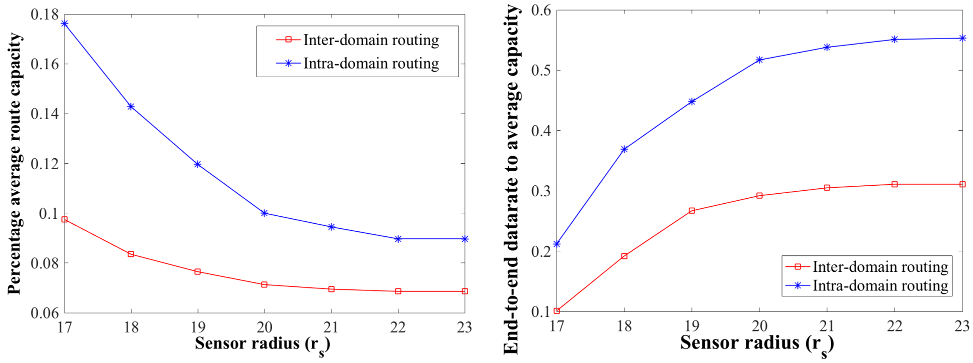


(a)

(b)

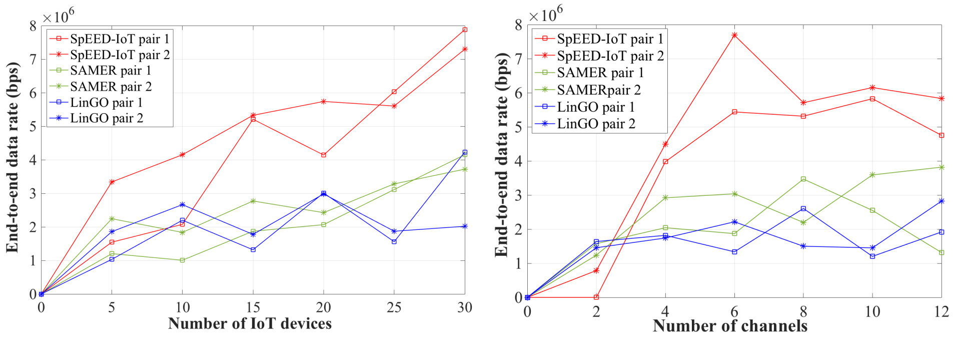
Figure 12: Routing (a) without power control between Node 158 and Node 42, (b) with power control between Node 158 and Node 42

End-to-end data rate: In Figures 13(a), and 13(b), we show the end-to-end data rate performance of SPAER for single SD pair in inter- and intra-domain scenarios. Figure 13(a) shows the percentage average route capacity with varying ESC sensor radius r_s. The percentage average route capacity is defined as the inverse of average hop count per route. We see that for both inter-domain and intra-domain routing, with higher r_s, the average hop count increases as there are more routes available with higher capacity. Thus the percentage average route capacity decreases sharply with r_s until it reaches a steady state when chances of finding better routes saturate. We show the nature of effective end-to-end data rate to average route capacity in Figure 13(b). With higher r_s, network connectivity increases, thus SpEED-IoT identifies better routes with higher end-to-end data rate. With inter-domain routing, the probability of a finding a link with lower data rate increases, thus we observe reduction in effective end-to-end data rate.



(a) (b)

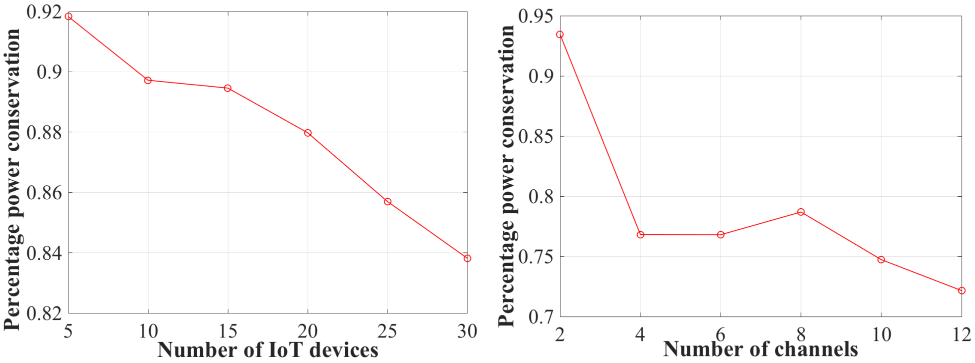
Figure 13: (a) Percentage average end-to-end data rate with sensor radius, (b) End-to-end data rate to average capacity with sensor radius



(a) (b)

Figure 14: Performance comparison for end-to-end data rate with (a) varied number of IoT devices, (b) with varied number of channels

In Figures 14(a), and 14(b), we compare SpEED-IoT's end-to-end data rate performance against SAMER and LinGO D2D routing schemes for scenarios when multiple SD pairs require route assignment. Figure 14(a) shows that with increasing number of IoT devices in the secondary network, SpEED-IoT's effective end-to-end data rate increases gradually with the rate of increase much higher than SAMER and LinGO. This is due to the fact that with more devices, the chances of getting routes with higher data rate links increase for SpEED-IoT. However, for SAMER and spectrum agnostic LinGO approaches, increase in such chances are negated by the fact the most of higher data rate links can not be used due to presence of primary incumbent. In Figure 14(b), similar characteristics can be observed, although the data rate seem to saturate after some value of the number of available channels. This is due to the fact that after a certain number of free channels, the probability of finding a better link in terms of data rate along an end-to-end route does not increase.



(a)

(b)

Figure 15: SpEED-IoT power conservation against LinGO (a) for varied number of IoT devices, and (b) for varied number of channels

Power conservation: Figures 15(a) and 15(b) demonstrates the percentage power conservation of SpEED-IoT's intelligent power controlled routing in comparison to LinGO that do not use power control for primary protection. Interestingly we see that against both increasing number of IoT devices and number of channels, the power conservation magnitude albeit very high, gradually decreases which might be counter-intuitive. This is due to the fact that with more devices and channels in the network, other approaches, such as, LinGO need to use less average power for end-to-end communication thereby reducing the percentage power conservation benefits of SpEED-IoT. Even in such cases, the magnitude of SpEED-IoT's percentage power reduction is easily above 70% which is very high.

Primary receiver protection: In Figures 16(a) - 16(d), we demonstrate SpEED-IoT's performance in terms of primary receiver protection. Figures 16(a) and 16(b) show that the number of primary receivers protected increase with the number of secondary IoT devices and number of free channels due to the increase in finding more route options and thereby using less transmission power. Interesting to note that the number of primary receivers protected reaches a saturation point where the identity of the best route does not alter even if more IoT devices or channels are made

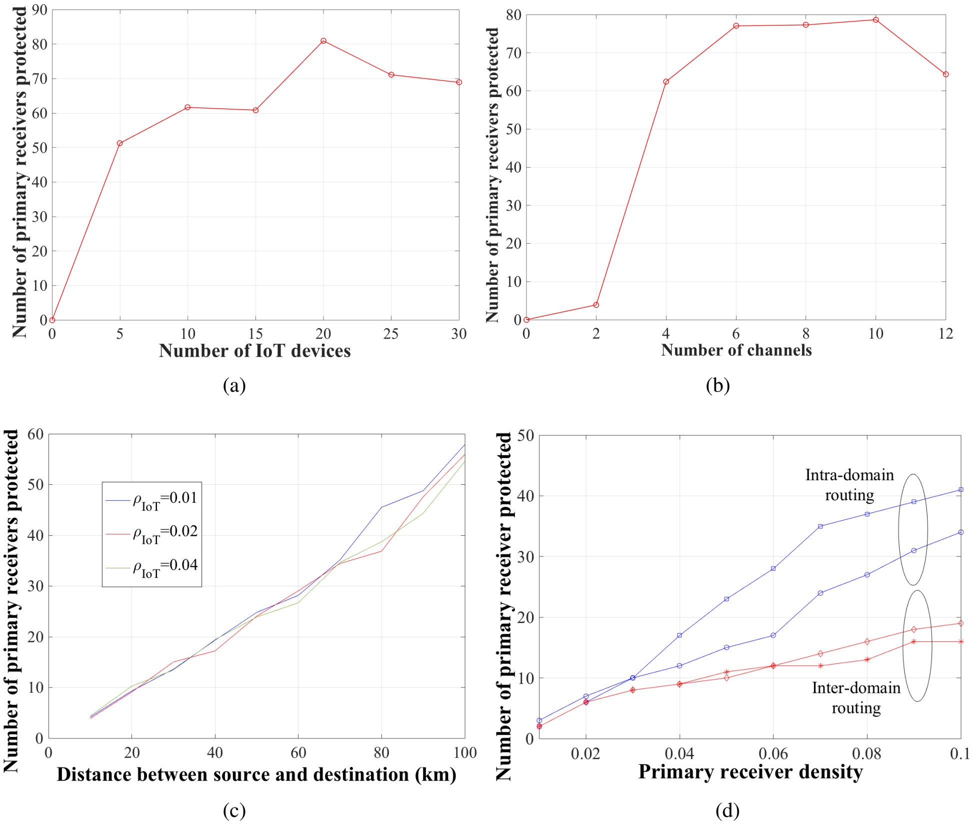
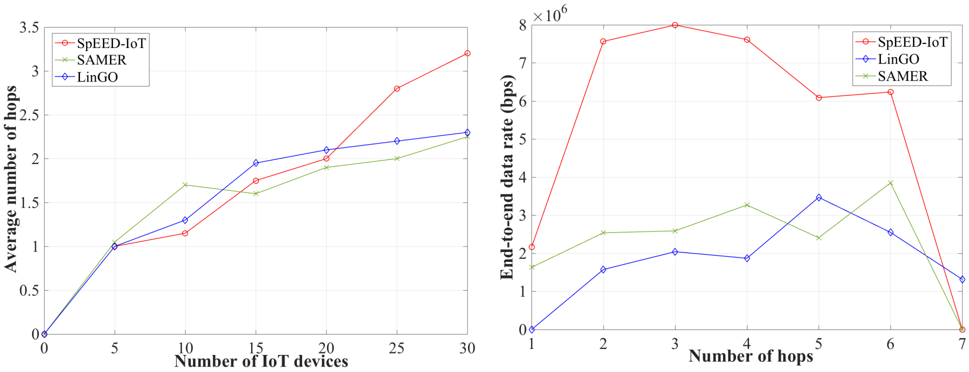


Figure 16: Characteristics of primary receivers protected with (a) varied number of secondary IoT devices in the network, (b) varied number of channels, (c) varied distance between the source and destination, (d) varied primary receiver density

available. In Figure 16(c), we show that the number of primary receivers protected increases as the distance between the source and destination increases. This is because when power control is not used, more primary receivers are interfered along the route. However, we observe that such nature is independent of the density of IoT devices in the network. Figure 16(d) shows that the number of primary receivers protected is increasing with primary receivers in the network for four different source-destination pairs, with a couple of cases each for inter-domain and inter-domain routing. As expected, the number of primary receivers protected is higher for inter-domain routing as more hops in inter-domain routing protects more receivers along the end-to-end route.

Hop count: Figures 17(a) and 17(b) compare SpEED-IoT performance in terms of number of hops used per route against SAMER and LinGO. From Figure 17(a), we see that with higher number of IoT devices in the secondary network, SpEED-IoT gets more options for better routes with lower transmission power which increases the number of hops. Whereas, SAMER uses less hops as it does not use power controlled transmission. Figure 17(b) shows that although SpEED-IoT uses more hops than other schemes, the average effective end-to-end data rate per route with any number of hops is much greater than other schemes.



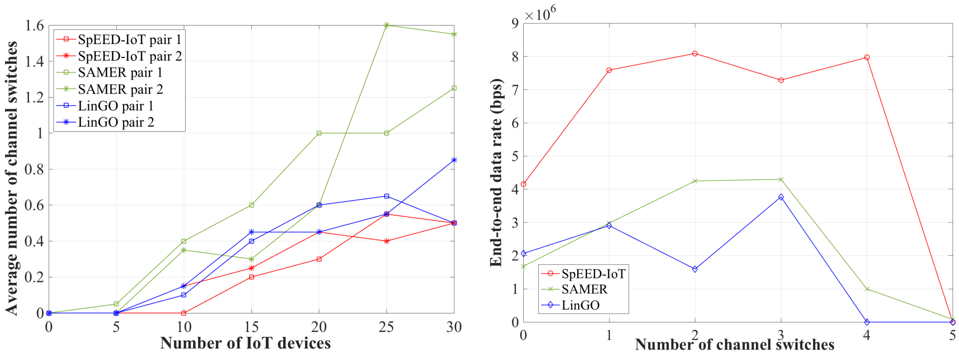
(a)

(b)

Figure 17: (a) Comparison for number of hops used for end-to-end routes, (b) End-to-end data rate with different number of hops per route

Channel switching: Switching channels along a route becomes essential for multi-hop, multi-channel D2D routing. However, frequent channel switching may lead to time and energy overheads for IoT devices. Thus, it is desirable for end-to-end routing protocols especially for IoT devices to keep such switching to a minimum. In Figure 18(a), we show that SpEED-IoT on an average ends up using less number of channel switches per route than SAMER and LinGO schemes in spite of using more hops per routes, as shown in Figure 17(a). This happens due to the fact that SpEED-IoT uses both spatial information for spectrum availability which ends up choosing channels that are suitable for both data rate and primary protection purposes. Thus, SpEED-IoT does not need to change channels that frequently along a route. However, SAMER and LinGO always perform local data rate optimization that leads to choosing different channels at different hops. Figure 18(b) is similar to Figure 17(b) where we show that for routes with any number of channels switches, SpEED-IoT ensures higher end-to-end data rate than other schemes. Notably, most SpEED-IoT routes have 1 to 2 channel switches, with only a handful of cases out of 20 runs having more than 2 switches.

Interestingly, there seem to exist an inflection point on the number of switches for SpEED-IoT that leads to maximum data rate. From Figure 18(b), such infection point is at 2 channel switches, beyond which the average end-to-end data rate value seems to drop.



(a)

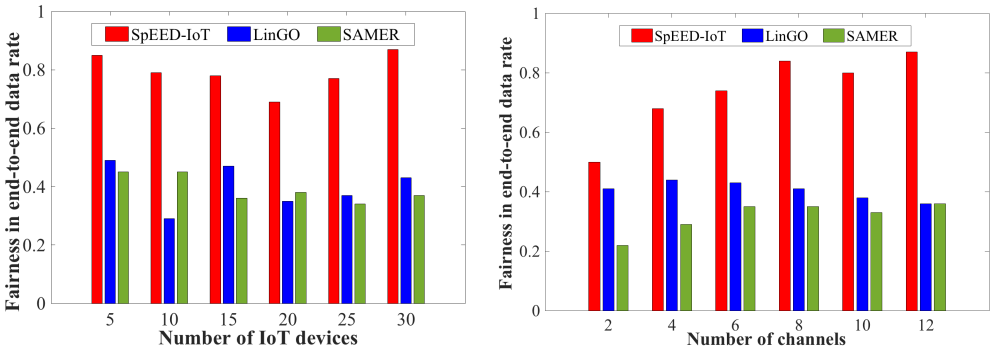
(b)

Figure 18: (a) Comparison for number of channel switches along a route for varied number of IoT devices, (b) end-to-end data rate performance for different values of channel switching

Fairness in route assignment: Finally, in Figures 19(a), and 19(b) we compare SpEED-IoT's fairness in route assignment in terms of effective end-to-end data rates of interfering IoT SD pairs against that of SAMER and LinGO. We apply the well known Jain's fairness index formula [44] on the simulation results for the fairness comparison. Figure 19(a) shows that for any number of IoT devices, SpEED-IoT ensures on an average 50% higher route assignment in terms of fairness when interfering IoT SD pairs require routes. Whereas, Figure 19(b) shows that for lower number of available channels, SpEED-IoT is not able to ensure fair assignment due to lack of channel choices. However, with more free channels, SpEED-IoT's fairness is significantly better than other schemes.

7 Conclusions and Future Work

In this paper we discussed the challenges of DSA based secondary routing in a D2D IoT network. We proposed SpEED-IoT, a spectrum aware, energy efficient multi-channel multi-hop routing technique among IoT devices with the aid of a spectrum map created by ESC sensors. A transmission power control based selective flooding technique is proposed to spread the route requests in the network without causing network wide transmission overhead. We



(a)

(b)

Figure 19: Fairness comparison in route assignment in terms of end-to-end data rate for (a) varied number of IoT devices, (b) varied number of channels

analyzed the connectivity condition among IoT devices using such methods. As part of the SpEED-IoT scheme, an evolutionary game theoretic model is also proposed that uses a dynamic learning algorithm to assign conflict free end-to-end routes to interfering SD pairs without compromising effective data rate and assignment fairness. Using an extensive simulation based testbed evaluation, we showed the SpEED-IoT performance in terms of ensuring IoT network connectivity, end-to-end data rate optimization, primary receiver protection, and route assignment fairness.

As part of future work, we will analyze the performance of our proposed scheme both theoretically and experimentally for different primary environments and IoT networks in terms of operational spectrum bands (such 3.5 GHz, TV white space), primary transmission characteristics, spectrum characteristics, and heterogeneous secondary IoT device communication mode/capabilities (full duplex). Finally, as part of long-term future plans, we plan to implement the proposed scheme and its future extensions into a newly developed software-defined radio enabled indoor IoT testbed for empirical results.

References

[1] NSF GENI Infrastructure. `https://www.geni.net/`.

[2] Proposal to administer environmental sensing capability. `https://ecfsapi.fcc.gov/file/60001841831.pdf`.

[3] Report and order and second further notice of proposed rulemaking. https://www.fcc.gov/rulemaking/12-354/.

[4] Cross-layer routing design in cognitive radio networks by colored multigraph model. *Wireless Personal Communications*, 49, 2009.

[5] Modelling and simulation of rayleigh fading, path loss, and shadowing fading for wireless mobile networks. *Simulation Modelling Practice and Theory*, 19(2):626 – 637, 2011.

[6] A beaconless opportunistic routing based on a cross-layer approach for efficient video dissemination in mobile multimedia iot applications. *Computer Communications*, 45:21 – 31, 2014.

[7] Primary radio user activity models for cognitive radio networks: A survey. *Journal of Network and Computer Applications*, 43(Supplement C):1 – 16, 2014.

[8] A. Abbagnale and F. Cuomo. Gymkhana: A connectivity-based routing scheme for cognitive radio ad hoc networks. In *INFOCOM IEEE Conference on Computer Communications Workshops.*, pages 1–5, March 2010.

[9] O. A. Al-Tameemi and M. Chatterjee. Percolation in multi-channel secondary cognitive radio networks under the sinr model. In *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pages 170–181, 2014.

[10] Fadi Al-Turjman. Cognitive routing protocol for disaster-inspired internet of things. *Future Generation Computer Systems*, pages –, 2017.

[11] Sergey Balandin, Sergey Andreev, and Yevgeni Koucheryavy. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART*

2015, St. Petersburg, Russia, August 26-28, 2015, Proceedings. Lecture Notes in Computer Science. Springer International Publishing, 2015. JUFOID=62555.

[12] Oladayo Bello, Sherali Zeadally, and Mohamad Badra. Network layer inter-operation of device-to-device communication technologies in internet of things (iot). *Ad Hoc Networks*, 57:52 – 62, 2017. Special Issue on Internet of Things and Smart Cities security, privacy and new technologies.

[13] S. Bhattarai, J. M. J. Park, B. Gao, K. Bian, and W. Lehr. An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research. *IEEE Transactions on Cognitive Communications and Networking*, 2(2):110–128, June 2016.

[14] H. Bogucka, P. Kryszkiewicz, and A. Kliks. Dynamic spectrum aggregation for future 5g communications. *IEEE Communications Magazine*, 53(5):35–43, May 2015.

[15] Geng Cheng, Wei Liu, Yunzhao Li, and Wenqing Cheng. Spectrum aware on-demand routing in cognitive radio networks. In *New Frontiers in Dynamic Spectrum Access Networks, DySPAN. 2nd IEEE International Symposium on*, pages 571–574, April 2007.

[16] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige. Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 ghz dedicated short range communication (dsrc) frequency band. *IEEE Journal on Selected Areas in Communications*, 25(8):1501–1516, Oct 2007.

[17] K. R. Chowdhury and M. D. Felice. Search: A routing protocol for mobile cognitive radio ad-hoc networks. *Computer Communications Journal (ELSEVIER)*, 32(18):1983–1997, Dec. 2009.

[18] S. Debroy, S. Bhattacharjee, and M. Chatterjee. Performance based channel allocation in ieee 802.22 networks. In *Personal Indoor and Mobile Radio Communications, PIMRC. IEEE International Symposium on*, pages 619–623, Sept. 2011.

[19] S. Debroy, S. Bhattacharjee, and M. Chatterjee. Spectrum map and its application in resource management in cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking*, 1(4):406–419, Dec 2015.

[20] S. Debroy, S. De, and M. Chatterjee. Contention based multichannel mac protocol for distributed cognitive radio networks. *IEEE Transactions on Mobile Computing*, 13(12):2749–2762, Dec 2014.

[21] Z. Feng, Q. Li, W. Li, T. A. Gulliver, and P. Zhang. Priority-based dynamic spectrum management in a smart grid network environment. *IEEE Journal on Selected Areas in Communications*, 33(5):933–945, May 2015.

[22] I. Filippini, E. Ekici, and M. Cesana. Minimum maintenance cost routing in cognitive radio networks. In *Mobile Adhoc and Sensor Systems, MASS. IEEE 6th International Conference on*, pages 284–293, Oct. 2009.

[23] T. Harrold, R. Cepeda, and M. Beach. Long-term measurements of spectrum occupancy characteristics. In *New Frontiers in Dynamic Spectrum Access Networks, DySPAN. IEEE Symposium on*, pages 83 –89, May 2011.

[24] M. Z. Hasan and F. Al-Turjman. Optimizing multipath routing with guaranteed fault tolerance in internet of things. *IEEE Sensors Journal*, 17(19):6463–6473, 2017.

[25] Y. T. Hou, Yi Shi, and H. D. Sherali. Spectrum sharing for multi-hop networking with cognitive radios. *Selected Areas in Communications, IEEE Journal on*, 26(1):146–155, Jan. 2008.

[26] J. Huang, Q. Duan, Y. Zhao, Z. Zheng, and W. Wang. Multicast routing for multimedia communications in the internet of things. *IEEE Internet of Things Journal*, 4(1):215–224, 2017.

[27] O. Iova, P. Picco, T. Istomin, and C. Kiraly. Rpl: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, 54(12):16–22, 2016.

[28] M. Ishino, Y. Koizumi, and T. Hasegawa. A study on a routing-based mobility management architecture for iot devices. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 498–500, Oct 2014.

[29] Yichao Jin, Sedat Gormus, Parag Kulkarni, and Mahesh Sooriyabandara. Content centric routing in iot networks and its integration in {RPL}. *Computer Communications*, 89???90:87 – 104, 2016. Internet of Things Research challenges and Solutions.

[30] J. W. Kang, A. Hussain, and S. H. Kim. Link scheduling schemes with on-off interference map for device-to-device communications. *IET Communications*, 9(3):359–366, 2015.

[31] A. A. Khan, M. H. Rehmani, and A. Rachedi. When cognitive radio meets the internet of things? In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 469–474, 2016.

[32] A. A. Khan, M. H. Rehmani, and M. Reisslein. Requirements, design challenges, and review of routing and mac protocols for cr-based smart grid systems. *IEEE Communications Magazine*, 55(5):206–215, 2017.

[33] Yun Li, Trung Tran Quang, Yoshihiro Kawahara, Tohru Asami, and Masanori Kusunoki. Building a spectrum map for future cognitive radio technology. In *Proceedings of the 2009 ACM workshop on Cognitive radio networks*, CoRoNet.

[34] D. Lu, X. Huang, P. Li, and J. Fan. Connectivity of large-scale cognitive radio ad hoc networks. In *2012 Proceedings IEEE INFOCOM*, pages 1260–1268, 2012.

[35] N. Michael and A. Tang. Halo: Hop-by-hop adaptive link-state optimal routing. *IEEE/ACM Transactions on Networking*, 23(6):1862–1875, Dec 2015.

[36] D. T. Otermat, C. E. Otero, and I. Kostanic. Analysis of the fm radio spectrum for internet of things opportunistic access via cognitive radio. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 166–171, 2015.

[37] Meng-Shiuan Pan and Shu-Wei Yang. A lightweight and distributed geographic multicast routing protocol for iot applications. *Computer Networks*, 112:95 – 107, 2017.

[38] I. Pefkianakis, S.H.Y. Wong, and Songwu Lu. SAMER: Spectrum aware mesh routing in cognitive radio networks. In *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, pages 1–5, Oct. 2008.

[39] Priyanka Rawat, Kamal Deep Singh, and Jean Marie Bonnin. Cognitive radio for {M2M} and internet of things: A survey. *Computer Communications*, 94:1 – 29, 2016.

[40] W. Ren, Q. Zhao, and A. Swami. Connectivity of heterogeneous wireless networks. *IEEE Transactions on Information Theory*, 57(7):4315–4332, 2011.

[41] J. Riihijarvi, P. Mahonen, M. Wellens, and M. Gordziel. Characterization and modelling of spectrum for dynamic spectrum access with spatial statistics and random fields. In *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1–6, 2008.

[42] F. J. Rodr?guez, S. Fernandez, I. Sanz, M. Moranchel, and E. J. Bueno. Distributed approach for smartgrids reconfiguration based on the ospf routing protocol. *IEEE Transactions on Industrial Informatics*, 12(2):864–871, April 2016.

[43] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[44] H. Shi, R. V. Prasad, E. Onur, and I. G. M. M. Niemegeers. Fairness in wireless networks:issues, measures and challenges. *IEEE Communications Surveys Tutorials*, 16(1):5–24, First 2014.

[45] Yi Shi and Y.T. Hou. A distributed optimization algorithm for multi-hop cognitive radio networks. In *Proceedings of the 29th conference on Information communications*, INFOCOM'10, pages 1292–1300, April.

[46] Hsien-Po Shiang and M. Van der Schaar. Distributed resource management in multihop cognitive radio networks for delay-sensitive transmission. *Vehicular Technology, IEEE Transactions on*, 58(2):941–953, Feb. 2009.

[47] Robert Shrock and F Y Wu. Spanning trees on graphs and lattices in d dimensions. *Journal of Physics A: Mathematical and General*, 33(21):3881.

[48] Qiwei Wang and Haitao Zheng. Route and spectrum selection in dynamic spectrum networks. In *Consumer Communications and Networking Conference, CCNC. IEEE*, volume 1, pages 625–629, Jan. 2006.

[49] M. Wellens, J. Riihijarvi, and P. Mahonen. Modelling primary system activity in dynamic spectrum access networks by aggregated ON/OFF-processes. In *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) Workshops,*, pages 1–6, June 2009.

[50] F Y Wu. Number of spanning trees on a lattice. *Journal of Physics A: Mathematical and General*, 10(6):L113.

[51] Chunsheng Xin, Bo Xie, and Chien-Chung Shen. A novel layered graph model for topology formation and routing in dynamic spectrum access networks. In *New Frontiers in Dynamic Spectrum Access Networks, DySPAN. First IEEE International Symposium on*, pages 308–317, Nov. 2005.

[52] O. Younis, L. Kant, A. Mcauley, K. Manousakis, D. Shallcross, K. Sinkar, K. Chang, K. Young, C. Graff, and M. Patel. Cognitive tactical network models. *IEEE Communications Magazine*, 48(10):70–77, October 2010.

[53] J. Zhu, Y. Song, D. Jiang, and H. Song. Multi-armed bandit channel access scheme with cognitive radio technology in wireless sensor networks for the internet of things. *IEEE Access*, 4:4609–4617, 2016.