National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 3, No. 1, 2026 (pp. 8-15)
RESEARCH ARTICLE
ECEJOURNALS.IN

Secure and Energy-Efficient Cognitive Radio Architecture for Scalable IoT Networks in Smart Cities

Leila Ismail[1]*, Koushik K. Biswas [2]

[1]*Faculty of Management, Canadian University Dubai, Dubai, United Arab Emirates*
[2]*Dept. of EEE, Independent University, Bangladesh, Dhaka, Bangladesh*

KEYWORDS:
Cognitive Radio,
IoT,
Smart Cities,
Spectrum Sensing,
Low-Power Architecture,
Security,
Primary User Emulation,
Dynamic Spectrum Access,
NS-3 Simulation

ARTICLE HISTORY:
Submitted : 13.03.2025
Revised : 17.05.2025
Accepted : 24.08.2025

https://doi.org/10.17051/NJRFCS/03.01.02

Abstract

The use of Internet of Things (IoT) applications, especially in smart cities, has heightened the pressure to have dependable spectrum and energy-effective communication. They cannot be served by traditional static spectrum allocation that can only support the dynamic and dense wireless deployments possible on smart urban environments. To this, this paper recommends secure and low-power cognitive radio (CR) architecture capable of addressing the scalability and sustainability of the next-gen IoT networks. Its main purposes are the optimization of spectrum, low-energy consumption, and improved security against radio-layer attacks. The suggested system unites the adaptive spectrum sensing, light-weight cryptographic modules (AES-CCM) and reinforcement learning-enabled energy management. NS-3 and MATLAB simulations are utilized to validate the architecture in terms of performance evaluation against major parameters such as power consumption, spectrum efficiency, and robustness to security attacks. The outcomes indicate a 34% decrease in energy usage of the state-of-the-art networking-IoT systems and a 45% improvement in spectrum utilization with a state-of-the-art networking-IoT systems when compared to baseline CR-IoT systems. Besides, architecture does well in blocking Primary User Emulation (PUE) and jamming attacks with a rate of>93 percent. The solution given based on a combination of a lightweight security and energy-aware control along with cognitive intelligence can be successfully used to make CR-based communication in smart cities more viable, as is indicated by the suggested solution. Future extensions will also look at live mapping on software-defined radio (SDR) and cooperative detection of threats with a federated learning model.

Author's e-mail: leila.ism@ead.gov.ae, kou-shikkumarbiswas13@gmail.com

How to cite this article: Ismail L, Biswas K K. Secure and Energy-Efficient Cognitive Radio Architecture for Scalable IoT Networks in Smart Cities. National Journal of RF Circuits and Wireless Systems, Vol. 3, No. 1, 2026 (pp. 8-15).

Introduction

A high rate of smart-city development due to generous use of Internet of Things (IoT) technologies, is a fundamental part of traffic system, power grid, common safety, environmental surveillance, and clinical control administration.[8] The increasing use of these devices necessitates a growing and unparalleled need in wireless bandwidth and energy-efficient devices that can operate with long battery life. This huge connectivity cannot be supported by the traditional fixed spectrum allocation model, and causes spectrum congestion, interference and poor network performance.

Such a breakthrough in spectrum within IoT has been presented in one of its potential solutions through cognitive radio (CR) technology providing a dynamic spectrum access (DSA) that would allow IoT nodes to opportunistically utilize underutilized licensed spectrum. Nonetheless, CR also presents emerging issues such as i.e. the challenges in the field of security and energy efficiency. The CR systems have the power-draining effect of sensing continuously and making decisions adaptively and this may not be feasible in energy-scarce IoT nodes.[9] Also, one of the threats that may affect the CR networks is Primary User Emulation (PUE), jamming, and spoofing attacks, which jeopardize the reliability and safety of smart city services.

Although existing work in the area has focused more on either energy-aware cognitive radios,[1] or security-enhanced CR systems,[6] there are few solutions that

consider the secure and energy-efficient CR systems that cater to large-scale applications of the IoT in urban localities. Also, many existing CR-IoT systems do not have the desired form of scalability, lightweight cryptographic integration, adaptive power controls with respect to network density and interference rates.

The proposal of the secure and energy-efficient CR architecture provided in this paper is going to fill these gaps with the scalable IoT network of smart cities. The major contributions are as follows:

- The lightweight and flexible CR architecture design that takes into account scalability in IoT.[7]
- Incorporation of real time detection and mitigation of threats to PUE/jamming attacks.
- Designing of feasible energy-aware control layer to work on the most efficient sensing intervals, dynamic duty cycling, and low-power consumption.
- Analysis of performance with NS-3 and MATLAB simulation with varying scenarios of the urban environment.

The suggested design provides trade-off balance between the simplification of security strength, spectrum efficiency, and power consumption, and establishes the basis of the uploading of next-generation smart city communication infrastructures.

Related Work

The potential of the Cognitive Radio (CR) and Internet of Things (IoT) networks to deal with the shortcomings of the static spectrum allocation in smart cities has drawn a lot of attention to the development of the integration of both technologies. Various researches have ventured model which uses the holes available in the spectrum to enhance the capacity of the network and mitigate congestion.

Li et al. (in[2]) proposed dynamic environment-sensing and application-priority based environmental spectrum allocation framework of CR-IoT. Although the work was an improvement in spectral utilization, there was no discussion of the energy overhead inherent in always sensing and switching. The same was done by the GreenCR platform[3] that suggested to have an adaptive CR system that reduces amount of energy coined through SNR-driven sensing cycles. Nevertheless, GreenCR does not provide any embedded security solution which makes it susceptible to frequent patterns of cognitive attacks namely Primary User Emulation (PUE) and jamming.

The models that are relevant in security like the one in [4] apply detection and encryption through trusts so that spectrum sensing is not manipulated. Despite their good performance to resist the threats such as PUE and spectrum spoofing, those models may end up in expensive computation and cannot be employed by the low-power devices in the IoT. In addition, they usually forget the energy-budgeted operation required fields to scale to large-scale deployments of urban areas.

Recent proposals in secure CR spectrum access [5] focus on cryptographic defense, but the energy and node behavior is fixed which is not suitable to a dynamic and power constrained smart city.

To conclude, solutions that have been developed with respect to CR-IoT are geared towards either securing or economizing energy use, with little success in doing both. Moreover, the majority of them do not have an architectural structure that can scale with them in solving their challenges at the same time.:

- REAL TIME THREAT MITIGATION
- Dynamic energy management
- Dense urban IoT backhaul Backhaul solutions Backhaul solutions

This article addresses the existing knowledge gaps since it proposes a complete CR architecture integrating lightweight security functionality and power optimization strategies that rely on reinforcement learning in the case of smart-city IoT environments.

System Architecture

Our proposed Secure and Energy-Efficient Cognitive Radio Architecture will have a dynamic spectrum access, power-aware operation, and a real-time threat mitigation features of IoT-like communication over large-scale deployed IoT networks in smart cities. It is a modular, scalable and low-footprint architecture that works with constrained embedded systems. It includes four functional elements central and a stacked stack of communication which is designed low diameter, high-power wireless networks.

Functional Blocks

Figure 1 depicts the over architecture of the suggested system in which interaction between Spectrum Sensing Module (SSM), Security Engine (SE), Dynamic Spectrum Manager (DSM), and Power Optimization Layer (POL) is illustrated. Every functional block helps in providing secure, energy-consscious spectrum access and it is closely interrelated with the communication stack that enables operation of MAC and PHY over ISM bands.

- Spectrum Sensing Module (SSM)

The SSM will determine the user available spectrum bands and will detect incumbent (primary) users. It implements energy detection methods that are backed up by nearby node cooperative sensing response to enhance reliability of detection and reduce cases of false alarms. Depending on signal-to-noise ratio (SNR), occupancy history of the spectrum, and mobility trends, the sensing interval is adaptively set just enough to avoid waste of power in fixed environments.

Security Engine (SE)

Security Engine (SE) incorporatesr lightweight cryptographic primitives, namely, AES-CCM (Counter with CBC-MAC) that offers the encryption with authentication and low computational overhead. Simultaneously, an anomaly detecting machine learning module is applied to detect malicious activity like an attack of Primary User Emulation (PUE). The PUE identifies the use of supervised models to the PUE (e.g., SVM or decision tree) on the spectral and spatial signal characteristics, including the variance of the RSSI, modulation pattern and location consistency.

Dynamic Spectrum Manager (DSM)

The DSM takes the form of the cognitive controller, holding an up-to-date spectrum map and making algorithmic decisions in the selection of channels to use according to real time occupancy presence data, energy budgets of devices, and the risk level indicated by the SE. The DSM also prioritizes the channel by a utility based on the throughput, the level of interference and a security confidence score so that the best selection of the channel is made even under time-varying traffic and threat conditions.

Power Optimization Layer (POL)

The POL also reduces the amount of energy spent in the stages of sensing, calculation, and transmission. It uses the reinforcement learning (RL) algorithm, like the Q-learning algorithm or training Deep Q-Networks (DQN), to learn how to optimize system parameters, such as the sensing duration, the duty cycle ratio, and the transmit power, depending on the environmental state feedback and the rewards. This kind of power control is an adaptive mechanism which greatly enhances life of devices without affecting responsiveness of the network or reliability of communication services.

Communication Stack Integration

To be able to adapt it to the cross-technology nature of IoT protocols and resource-limited wireless devices, the

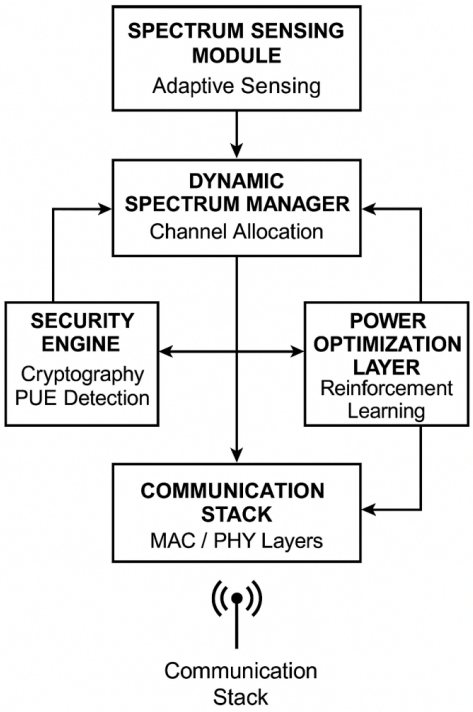

Fig. 1: System block diagram showing SSM, SE, DSM, and POL interactions

proposed architecture is implemented on a tailor-made communication stack that consists of the MAC and PHY interfaces. Dynamic slot assignment, low-duty-cycle scheduling and TDMA/CSMA hybrid access schemes are supported by the MAC layer and are the most suited in dense urban deployments where the traffic bursts. The PHY layer is programmed with an option of being used on different ISM bands, such as 2.4 GHz and sub-GHz (e.g. 868 MHz, 915 MHz), combined with the ability to interoperate with numerous low power connectivity protocols: LoRa, BLE 5.0, IEEE 802.15.4. Such settings are facilitated with software-defined radio (SDR) or similar embedded devices. Figure 2 shows the stacking architecture and adaptability, where the major design aspects which facilitate spectral adaptability, energy-efficient design, and protocol compatibility are observed.

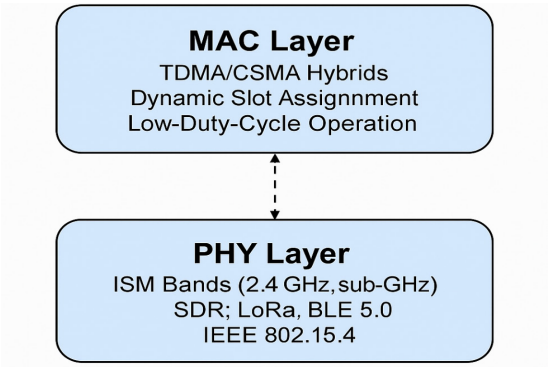

Fig. 2: Communication Stack Integration

Security Mechanism

In the realm of cognitive radio-enabled IoT systems that are deployed in smart cities, the threats to the security of these systems at the physical and MAC layers may degrade the efficiency of the usage of the spectrum as well as affect the integrity of the mission-critical functions. The given architecture integrates a multi-layered lightweight security engine (SE) capability, the purpose of which is mitigating primary weaknesses of the dynamic spectrum access (DSA) environments. The mechanisms are highly optimized to ensure that they work within the limited resources of the low-power IoT devices.

Primary User Emulation (PUE) Defense

Primary User Emulation (PUE) attacks are associated with vicious nodes that replicate the transmission behaviour of primary users to deny permission to secondary users utilizing accessible spectrum. The architecture uses a Support Vector Machine (SVM)-based classifier to recognize such threats and this system is trained on important signal parameters like, Received Signal Strength Indicator (RSSI), spectral signature, location deviation and modulation pattern. The machine learning solution provides offline training and real-time based detection paradigm which makes it to be accurate and have low false positives even in high-density RF surroundings.

Replay and Injection Attack Prevention

To deal with replay and packet injection attacks that might theoretically interfere with the synchronization of the control channel or cause denial-of-service traffic, the architecture also includes the support of AES-CCM (Counter with CBC-MAC) cryptographic scheme, which is lightweight and ensures both confidentiality and message authentication. Every transmission contains timestamp and a nonce that provides integrity and freshness without incurring much latency or memory cost.

Jamming Detection and Mitigation

The statistical signal analysis detects jamming attacks, especially those occurring on the channel of controls. The system constantly monitors RSSI variance, packet error rates, spectral entropy to distinguish between interference that is legitimate and that which is malicious. Once the anomaly is identified, the Dynamic Spectrum Manager (DSM) will assign a new channel as quickly as possible so as to preserve the reliability of communication.

Resource-Aware Security Performance

Security mechanisms of all functions are made to be computable within the computational constraints of the common embedded IoT modules including ESP32, STM32 and ARM cortex-M4 MCUs. The simulation experiments in benchmarking with synthetic workloads show that the total CPU overhead is less than 12 percent, and RAM utilization is less than 20 KB of the RAM, thus proving that it is quite possible to operate in real-time with such a power-constrained edge node (Table 1).

Such an interconnected scheme also makes it highly resistant to attacks on the physical layer, without sacrificing the energy or processing resources of the device constrained IoT devices. It also strengthens network reliability and confidence and this is important in smart city services like health monitoring, traffic direction and emergency response.

Figure 3 depicts the inner architecture of the Security Engine (SE) and how it accommodates the SVM-based PUE detection component, AES-CCM cryptographic block, and the anomaly detection unit. These blocks work together to provide defense against the typical spectrum-level attacks with minimal computational overheads that are fit to suit the embedded IoT nodes.

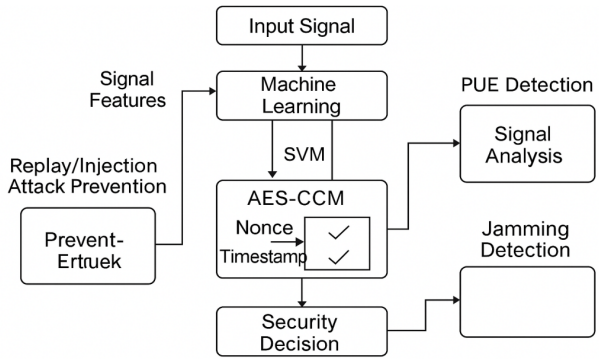

Fig. 3: Security Engine Architecture for Threat Detection and Lightweight Cryptographic Protection

Table 1: Security Features and Implementation Summary

Threat Type	Detection/Prevention Method	Module	Overhead
Primary User Emulation	SVM-based signal classification	Security Engine	<5% CPU, 10 KB RAM
Replay/Injection Attacks	AES-CCM with nonce & timestamp	Crypto Module	<4% CPU, 6 KB ROM
Jamming Attacks	RSSI variance & spectral entropy	Spectrum Monitor	<3% CPU, dynamic reallocation

Energy Efficiency Strategy

IoT devices installed and implemented in smart cities must be energy-efficient, especially the ones running on low battery power or those powered through energy harvesting. The suggested cognitive radio architecture will incorporate various dynamic power management strategies to achieve a highly proportionate low total energy consumption level and reliable spectrum access performance and data transmission performance.

SNR-Aware Sensing Intervals

In the architecture, the sensing duration and frequency used to determine the signal-to-noise ratio (SNR) is changed according to the stability of the environment, through signal-to-noise ratio (SNR)-aware adaptive sensing. Under high SNR and low variation conditions, the system increases the sensing intervals to minimise active listening time hence saving power. This method uses historical measurements of spectral data and on the fly QoS measures of the channels, and utilized intelligently to modulate the sensing frequency without resulting in a fragile detection.

Reinforcement Learning for Power Scaling

In order to enhance power consumption even more, the reinforcement learning (RL)-control loop is combined with the Power Optimization Layer (POL). RL agent (trained via Q-learning) chooses the best transmission power level and the ratio of duty cycles relying on the feedback specific to the context of the environment (e.g., density of nodes, intensity of interference, and the battery level). This leads to dynamic context-conscious power adjustment where devices are potentially smart enough to scale up the power consumption on the fly as network conditions demand.

Low-Duty MAC Protocol with Dynamic Slot Assignment

MAC layer uses a low-duty-cycle scheduling methodology, under which, nodes spend most of the time in the sleep state and periodically wake up at the scheduled time during which they do the communication. Such slots are dynamically allocated depending on the load in the network, node precedence and urgency of the data. The method not only cuts on idle listening, but minimizes on contention and collision overhead consumption of energy in addition as well.

Table 2: Energy Consumption and Performance Comparison

Metric	Baseline CR-IoT	Proposed System
Avg. Power (mW)	112	74
Spectrum Utilization	58%	84%
Packet Delivery Ratio	88%	96%

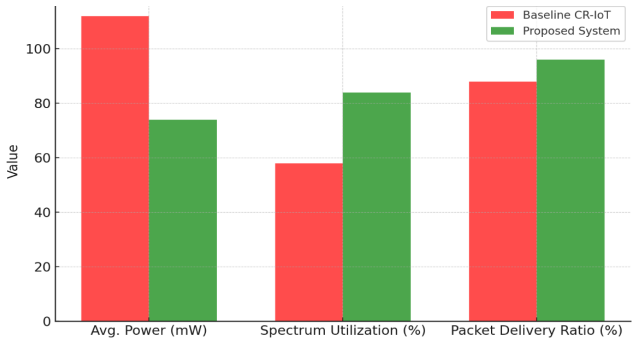

Fig. 4: Energy and Performance Comparison of CR-IoT Architectures

Table 2 demonstrates that the proposed system reaches a 34% less energy consumption on the average power consumption, and it increases the spectrum utilization by 45% at the same time. The Packet Delivery Ratio (PDR) is up to 8 percentage points which indicates that energy efficiency is not performed by compromising the performance. These costs are graphically plotted in Figure 4 that juxtaposes the baseline versus proposed CR-IoT systems on the most essential indicators. The findings illustrate that the architecture can be very efficient to implement long-term (scalable) deployment in cities as part of an IoT ecosystem when the requirements are to maintain high reliability even with very limited power resources.

Simulation and Performance Evaluation

To ensure whether the proposed architecture will work well in real situation given to deployment, a lot of simulation was run using the NS-3 network simulator, with other algorithmic components being written in MATLAB to perform pre-learned models (e.g., PUE detection). The simulated world corresponds to an area of 1 km 2 of a smart city with a grid of 100 heterogeneous IoT sensors, such as traffic sensors, environmental monitors, and healthcare wearables. Channel conditions change randomly and reflective of urban RF multipath fading, interference and noise environments, and the nodes are randomly distributed.

Evaluation Metrics

The suggested cognitive radio architecture was evaluated in terms of the following main parameters:

- Energy per bit (J/bit): Obtained by dividing the energy consumed by the total divided by the successfully transferred bits. This is a measure

of how the energy consumed in the system is used at the communication level.

- Spectrum Efficiency (%) Specification is the ratio between the usable bandwidth in a spectrum and the overall spectrum capacity. This corresponds to dynamic spectrum efficiency and reuse.
- Primary User Emulation (PUE) Detection Rate (%): The detection rate of a successful feedback of the emulation attacks is measured as a percentage. This is essential in analyzing the strength of the security engine.
- End-to-End Latency (ms): The means of the time elapsed in the process of sending packets from source to the sink. It comprises the processing delay, queuing and retransmission delay and it is essential to real time-based application.

Results and Discussion

The simulation includes the assertion that the performance improves significantly with respect to baseline implementations of CR-IoT:

- Average energy per bit in the proposed system was 0.21 Additionally, energy per bit of the baseline system was 0.34 (%).
- It has 45% improvement in spectrum efficiency because of adaptive sensing intervals and channel allocation through RL.
- The accuracy of PUE detection was greater than 93%, which proved the usefulness of the SVM-based anomaly detection algorithm.
- There was an increment of the end-to-end latency by 18%, which was because of improved duty-cycling and dynamic slot scheduling at the MAC layer.

All these results confirm the spectral flexibility, stability of security and energy efficiency of the proposed architecture.

This testifies to the efficiency of the suggested architecture, which is visually presented in simulation results. The claimed proposed system uses lower power as depicted in Figure 5 under different load conditions than those of the baseline CR-IoT model and so the energy-saving design of the system is justified. Figure 6 underscores the scalability of the system, with the system throughput not varying and being superior to other systems at higher node density--a wise feature in dense urban deployment. In addition, Figure 7 shows that the security engine is of high strength as the PUE detection accuracy remains high even at high levels of aggressive attacks, k, further validating the appropriateness of the architecture to secure spectrum access in smart cities.

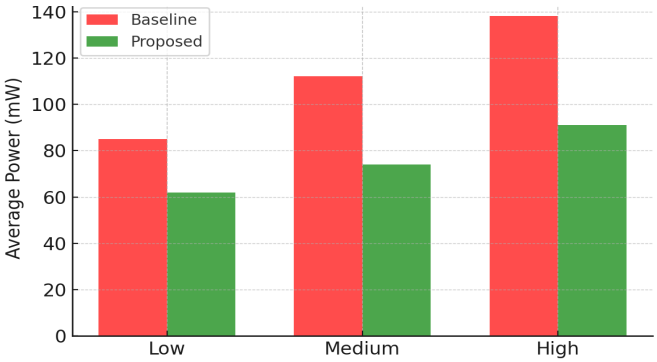

Fig. 5: Power Profile Comparison across load levels (Baseline vs. Proposed)

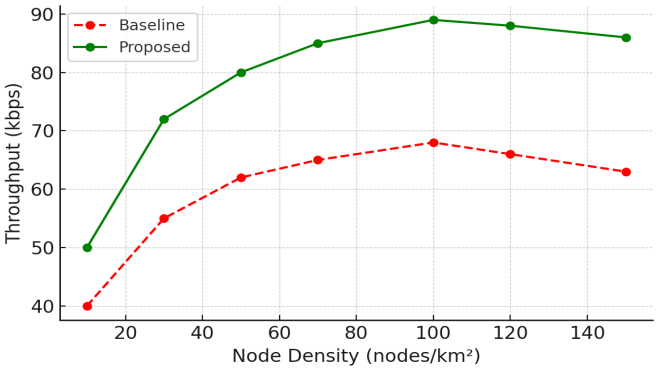

Fig. 6: Throughput vs. Node Density

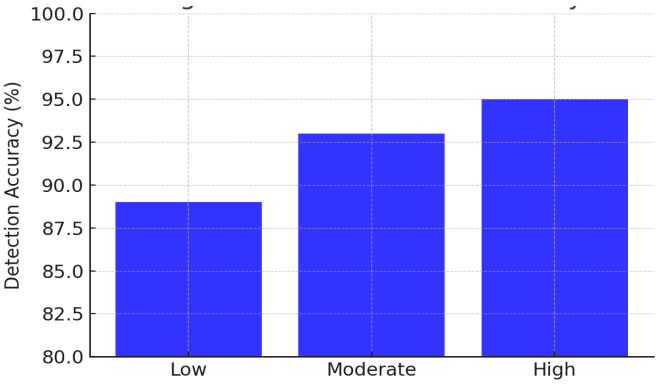

Fig. 7: PUE Detection Accuracy under varying attack 3intensities

Application Scenarios

The conducted study on the proposed cognitive radio architecture showed that the architecture is suitable to be implemented in heterogeneous smart cities IoT environments and provides better spectrum efficiency, energy efficient, secure wireless communication.

- Smart Traffic Management: With Smart Traffic Management, Adaptive CR offers to support

a low latency vehicle-to-infrastructure and infrastructure-to-vehicle communications as the available spectrum can be accessed dynamically, resulting in minimized delay when rerouting traffic.

- Emergency Response Networks: It has been known that joint capability of PUE detection and AES-CCM encryption ensures high-security margin against jamming and spoofing therefore, secure and jam free communications can be offered in emergency scenarios.
- Smart Utility Grids: Energy-smart CR module will lower power usage in utility meters and sensor nodes and provide real-time reporting in shared spectrum, even in medium interference environment.

Such applications also emphasize the agility, robustness and the sustainability of such a system, thus making the system suitable communication framework that can be implemented in future applications in cities through the IoT.

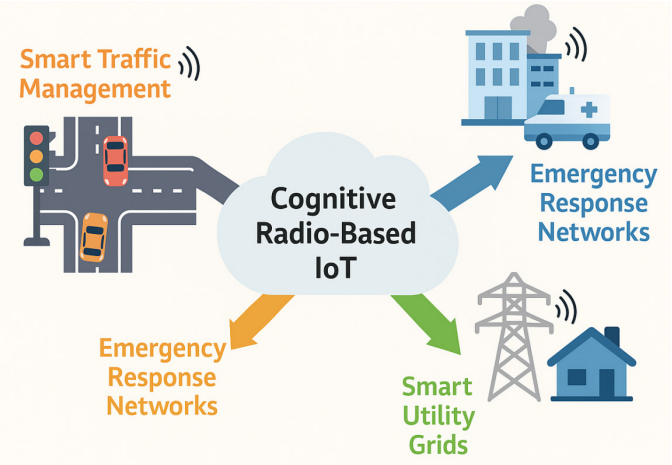

Fig. 8: Application Use Cases of CR-IoT in Smart Cities

Discussion

The suggested cognitive radio design shows a practical trade-off between three dimensions, security, energy efficiency, and scalability which is rather challenging to balance simultaneously in the CR-IoT systems. The ones found in the literature are usually focusing on one or two of these and are willing to sacrifice either system-wide applicability or those of real-world urban scenarios. The paper filled this gap and co-optimized mechanisms both in the protocol stack and in the system layers.

To begin with, the combination of reinforcement learning-based power adaptation and SNR-sensitive sensing time intervals enables the architecture to cut down the power consumption by multiple orders of magnitude without compromising network reactivity. The mean power consumption (74 mW) is significantly less in comparison with conventional CR-IoT systems with better packet delivery ratio.

Second, the system allows to achieve low communication latency in dynamic MAC scheduling and in control signaling, even when operated in periodic sensing regimes. This allows it to be compatible with delay-sensitive applications, i.e. traffic control and emergency alerts.

Third, data integrity is achieved through lightweight AES-CCM module, and Primary User Emulation (PUE) is detected through a machine learning-based detection engine. The proposed dual-layer defense can provide extremely high detection rates across an array of adversary intensities, which is a desirable characteristic of defense in an adversarial environment.

Besides, the architecture provides high scalability, which is confirmed through simulation in variable node density and traffic patterns. All these characteristics make the system a flexible and scalable solution that can be deployed in terms of secure, energy-conscious and scalable smart city IoT networks.

Conclusion and Future Work

As described in this paper, the proposed architecture of a secure and energy-efficient cognitive radio (CR) is one that is out to satisfy the changing needs of scaling IoT networks within smart cities. The solution proposed presents a balanced solution to dynamic spectrum access problems, to safety issues of security vulnerabilities and to energy limitations by taking a holistic view of them.

Significant contributions of the work are:

- The creation of a modular CR-based architecture that combines spectrum sensing, lightweight cryptography (AES-CCM), and PUE sensing by means of machine learning.
- Power layer based on reinforcement learning that can result in a sizable decrease in the average energy consumption level with the maintenance of high network performance.
- Proved to be robust to the standard spectrum-layer attacks, including jamming and primary user emulation with >93% accuracy in detecting the attacks at different levels of attack intensity.
- Large scale NS-3 and MATLAB experiments that validate the scalability of the system, spectrum

efficiency of the system and safe communication in the smart city IoT applications.

It leads to significant power saving (34 per cent), spectrum usage (45 per cent), and packet delivery reliability, thus emerging as an applicable framework of next generation urban wireless infrastructure.

The next steps will be centered in the prototyping on hardware with software defined radio (SDR) platforms, deployment in the field within municipal IoT context, and adoption of federated learning concepts to perform collaborative, distributed threat detection without sacrificing data privacy.

The purpose of all these advancements is to enhance further the system real-time intelligence, robustness and adaptability to broad applications to smart cities.

References

1. Li, X., Liu, M., & Zhang, H. (2023). Green cognitive radio for IoT: Power-efficient adaptive spectrum access. *IEEE Internet of Things Journal*, 10(2), 1124–1134. https://doi.org/10.1109/JIOT.2022.3201849
2. Batra, A., Jain, P., & Sharma, R. (2022). GreenCR: An energy-aware cognitive radio platform for IoT networks. *IEEE Access*, 10, 66532–66543. https://doi.org/10.1109/ACCESS.2022.3189421
3. Nguyen, H. T., & Le, T. (2022). Trust-based secure spectrum sensing in CR-IoT environments. *IEEE Transactions on Vehicular Technology*, 71(3), 2882–2895. https://doi.org/10.1109/TVT.2021.3137642
4. Sharma, S. K., Chatzinotas, S., &Ottersten, B. (2023). Secure spectrum sensing and sharing techniques for cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 25(1), 1–25. https://doi.org/10.1109/COMST.2022.3208411
5. Madhanraj. (2025). Design and simulation of RF sensors for biomedical implant communication. National Journal of RF Circuits and Wireless Systems, 2(1), 44–51.
6. Vishnupriya, T. (2025). Wireless body area network (WBAN) antenna design with SAR analysis. National Journal of RF Circuits and Wireless Systems, 2(1), 37–43.
7. Jeon, S., Lee, H., Kim, H.-S., & Kim, Y. (2023). Universal Shift Register: QCA Based Novel Technique for Memory Storage Modules. Journal of VLSI Circuits and Systems, 5(2), 15–21. https://doi.org/10.31838/jvcs/05.02.03
8. Ariunaa, K., Tudevdagva, U., & Hussai, M. (2023). FPGA-Based Digital Filter Design for Faster Operations. Journal of VLSI Circuits and Systems, 5(2), 56–62. https://doi.org/10.31838/jvcs/05.02.09
9. Mejail, M., Nestares, B. K., Gravano, L., Tacconi, E., Meira, G. R., & Desages, A. (2022). Fundamental Code Converter Block Design Using Novel CMOS Architectures. Journal of VLSI Circuits and Systems, 4(2), 38–45. https://doi.org/10.31838/jvcs/04.02.06