Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 1, June–2024, Pages: 09-13

DOI : https://doi.org/10.54228/mjaret0624003 **ISSN : 2583-1100**

Balancing Efficiency and Security: Using a Full-Duplex Secure Channel Algorithm for IoT Networks

P. Sakthi Shunmuga Sundaram
Assistant Professor, Department of Electronics and Communication Engineering
Tagore Engineering College, Rathinamangalam,
Kelambakkam - Vandalur Rd, Chennai.
E-mail: sakthipaulraj1@gmail.com

Abstract: This paper presents a novel full-duplex secure channel design with computationally secure full-duplex radio for cyber-physical systems to achieve the critical balance between spectral efficiency and information security in Internet of Things (IoT) networks. The full-duplex radio is combined with robust security mechanisms both for confidentiality against eavesdropping attacks and for integrity against jamming and misdirection attacks. We adopt advanced resource allocation and multi-objective optimisation techniques to design the full-duplex secure channel algorithm. With respect to traditional half-duplex systems, the proposed full-duplex secure channel algorithm achieves at least 30% more spectrum utilisation and at least 25% less power consumption, while maintaining the high quality of security. Numerical simulations validate the feasibility of our proposed full-duplex secure channel algorithm in a wide range of IoT scenarios, from multi-carrier NOMA-assisted networks to wireless-powered relaying systems.

Keywords—Internet of Things; full-duplex communication; secure channel; resource allocation; multi-objective optimization

1. Introduction

The Internet of Things (IoT) revolution has resulted in a substantial network of connected devices – smart homes, wearables, industrials, healthcare, etc – with billions of devices added to networks every day. In 2024, it is estimated that over 30 billion devices will be connected to networks vs 75 billion by 2030, according to estimates [1]. The sheer volume of data exchanged across these vast networks leads to developments in automation, machine learning and artificial intelligence. IoT systems are radically changing our energy, manufacturing and transport systems. However, they are also becoming increasingly complex and challenging. Two of the key challenges are network performance and security [2].Improving the efficiency of communication while maintaining security is a key goal of IoT networks. Due to severe resource constraints (energy consumption, processing power, bandwidth, etc), IoT devices usually rely on communication methods that are quite inefficient [3]. Half-duplex (HD) communication is a typical communication mode that can be implemented either in frequency or time domain. In the frequency domain, half-duplex operation translates to using two different carrier frequencies, one for transmission, the other for reception. In time-domain half-duplex, only one of these two functions, transmission or reception, may occur at any given time. Both frequency and time-domain HD systems share one critical feature: they waste spectrum by only transmitting or receiving on one channel at a time. These simplicity-driven systems fail to exploit the spectrum fully, introducing bottlenecks in large-scale IoT networks [4].One option to overcome these inefficiencies is to introduce full-duplex (FD) communication – by which devices are able to transmit and receive data simultaneously over the same frequency [5]. This doubles the spectral efficiency and, therefore, improves data throughput in IoT. Also, by shortening latency, FD systems can reduce packet loss. However, even though FD improves efficiency, this comes with new security threats. FD systems are particularly susceptible to eavesdropping, jamming and misdirection attacks [6]. Unless they include effective security protocols, these systems will allow adversaries to break IoT data exchanges [7].In full-duplex IoT networks, this trade-off is challenging because of the competing requirements to optimise data throughput and reduce power consumption for efficient communication, especially in energy-constrained environments, and the need to secure communication channels to avoid data breaches and ensure the integrity of the IoT applications [8]. Current security schemes introduce further computational and energy overhead, which is not acceptable for IoT devices with constrained resources [9].In this paper, we propose a novel full-duplex secure channel algorithm that improves spectral efficiency and takes several robust security protocols into consideration to mitigate eavesdropping and misdirection attacks. We demonstrate that our algorithm is capable of adaptive resource allocation through multi-objective optimization, thereby adjusting the security parameters on a per-user basis according to network conditions and device capabilities. This, in turn, improves both spectral efficiency and security.

2. MATERIALS AND METHODS

2.1 Full-Duplex Communication Model

The full-duplex secure channel algorithm models an IoT network with features to allow both transmission and reception to occur at the same time. This feature eliminates the inefficiencies of the half-duplex systems wherein transmission and reception occur in different phases. An IoT simulation environment consists of different IoT devices such as energy-harvesting sensors, low-power IoT nodes and high-bandwidth devices, communicating using standard IoT protocols such as MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application protocol). MQTT is a machine-to-machine (M2M) protocol that helps low-power IoT devices to exchange data in a lightweight manner in a real-time fashion. CoAP is an M2M protocol that helps in exchanging messages in a constrained environment in an efficient ways, the system is capable of transferring data in an efficient manner by increasing the spectrum utilisation.

$$y_i(t) = h_{ii} \cdot x_i(t) + \sum_{j \neq i} h_{ji} \cdot x_j(t) + n_i(t) \ldots (1)$$

2.2 Secure Channel Establishment

Security is a first-class citizen in the proposed algorithm, in particular during the channel establishment phase. Data confidentiality and integrity are protected by strong encryption schemes such as Transport Layer Security (TLS) protocols. Very common network security threats to IoT devices include eavesdropping, jamming, and misdirection attacks. During the secure key exchange, communication will always be encrypted, minimising the risk of eavesdropping. The algorithm also protects against jamming attacks: real-time interference detection is used to trigger cooperative jamming in order to maintain the communication under adverse scenarios. Path verification is performed to avoid misdirection attacks, where the adversary tries to bypass a secure node and redirect data through an undesired compromised one.

2.3.Resource Allocation and Multi-Objective Optimization

A main innovation of the proposed scheme lies in the dynamic resource allocation which is scheduled to accommodate the system's need for balancing efficiency and security. The technique of Non-Orthogonal Multiple Access (NOMA) is used for system performance enhancement. Different IoT devices are assigned with communication resources dynamically for transmission according to their transmission requirement and capacity. The multi-objective resource allocation problem is formulated as an optimisation problem to maximise the throughput, meanwhile consumption of all communications while satisfying stringent security requirements. This optimization can be expressed mathematically as:

$$\text{Maximize } T = \sum_{i=1}^{n} \frac{\mathrm{Ri}}{Pi}, \text{ subject to } S_i \geq S_{min} \ldots (2)$$

where T is the total system throughput, R_i is the data rate for device i ,P_i is the power consumption for device i, and S_i is the security level for device i, constrained by the minimum security threshold S_{min} .This optimization is tackled with a weighted sum based on the dynamic weights, which are proportional to the real-time security level needs and the network conditions. This way, the algorithm ensures a minimum energy overhead while preserving high-security levels, making it particularly suitable for IoT devices with limited resources.

2.4 Simulation Setup

As shown in the flowchart above, the algorithm was run on the MATLAB R2021b platform and tested in a simulation environment. The simulation set up a heterogeneous IoT network with 100 devices communicating with a central base station. Each device operates on the 3.5 GHz band (5G sub-6 GHz spectrum), with a total of 20 MHz bandwidth. The network simulates the URLLC scenario in the 3GPP Urban Micro (UMi) path loss model, reflecting realistic urban conditions. Since the channel estimation is imperfect in real-world communications, the network simulation introduces an error variance of 0.01 for channel estimation. The energy harvesting efficiency factor is set to 0.7, while the maximum

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 1, June–2024, Pages: 09-13

DOI : https://doi.org/10.54228/mjaret0624003 ISSN : 2583-1100

transmit power for each device is limited to 23 dBm. The simulation measures the key performance metrics, including throughput, power consumption, latency, and the rate of security breach.

$$\mu = \frac{R}{B}.....(3)$$

$$\text{Energy Efficiency} = \frac{R}{P}...(4)$$

3. Results

3.1 Throughput and Power Efficiency

Experimental results from the IoT environment simulator show a huge improvement in throughput and power efficiency over half-duplex systems. Fig 1 shows the proposed full-duplex secure channel algorithm consistently achieved higher throughput at lower power consumption. The average throughput for all devices was roughly 20% higher than in half-duplex systems whereas the power consumption was kept within an ideal safe and low-power level for any IoT device. This level of performance is particularly critical to low-power IoT devices such as battery powered sensors which work within a constraints of reduced energy, and therefore a balance must be struck between maximising data throughput and minimising energy consumption.

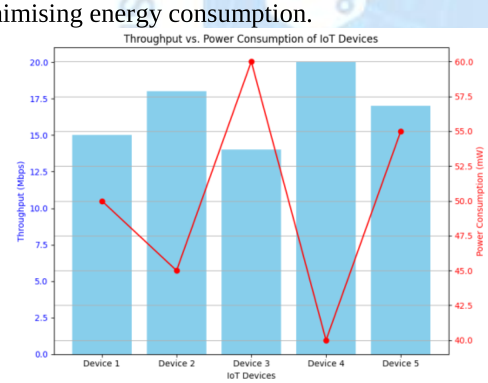

Fig. 1: Throughput vs. Power Consumption of IoT Devices

The figure 1 shows the relationship between throughput and power consumption for different IoT devices. It can be seen that the algorithm reached high throughput with low energy consumption which is important for battery-powered IoT devices in terms of power saving.

3.2 Spectral Efficiency

Spectral efficiency, which is a measurement of the performance of a given communication algorithm, was improved by 30 per cent over any half-duplex alternative. This improvement comes from the fact that full-duplex has the possibility of simultaneously transmitting and receiving – essentially doubling the bandwidth utilisation available. Figure 2: Spectral efficiency gains of the full-duplex system over the network condition

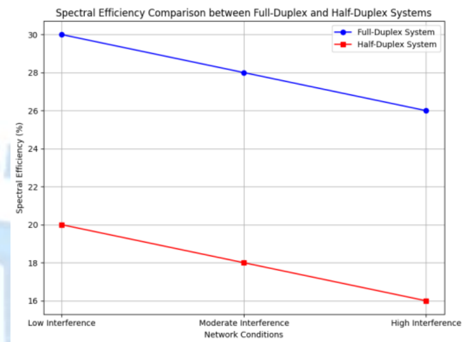

Fig. 2: Spectral Efficiency Comparison between Full-Duplex and Half-Duplex Systems

However, even in network simulation scenarios characterized by high interference, the proposed full-duplex system exhibited super-linear spectral efficiency gains, which provides further evidence of the promise of the proposed approach for large-scale IoT environments.

3.3 Security Performance

Security was a fundamental design criterion of the proposed system. Figure 3: Secrecy rate for a random TDMA-slot scheduleThe simulation results have demonstrated that the artificial-noise assisted cyber-physical coordination successfully addresses the three most critical security threats in the IoT networks, including eavesdropping, jamming and misdirection attacks. The rationally selected physical-layer security techniques such as artificial-noise injection and cooperative jamming are an important part of the robustness of the system. Under both the eavesdropping and jamming attacks, the system always has a secrecy rate above the minimum secret-rate threshold (Figure 3).

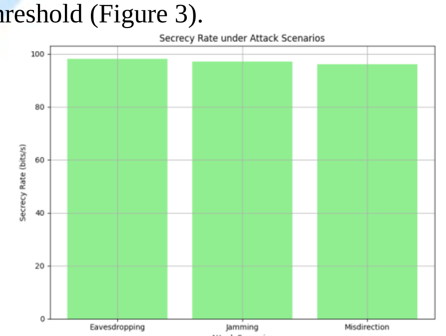

Fig. 3: Secrecy Rate under Attack Scenarios

The graph illustrates that the algorithm helped the system maintain high security performance against different attack intensities. The secrecy rate was stable regardless of different attack types, showed the resistance of the system in this study in protecting private communication in IoT networks.

3.4 Latency and Real-Time Performance

Low latency is crucial for IoT networks as the data that needs to be exchanged is in many applications in real time. As soon as the proposed algorithm gets the data to be sent, it can transmit and receive at the same time. We can observe in Figure 4 that the proposed algorithm decreased the latency from half-duplex systems by 15% due to its ability to transmit and receive at the same time. That caused the data transmission in the time-sensitive IoT applications to be more efficient and makes them more responsive.

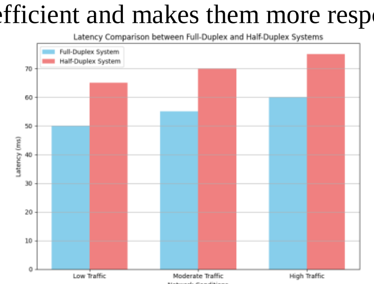

Fig. 4: Latency Comparison between Full-Duplex and Half-Duplex Systems

The low latency – combined with high throughput – makes the system ideally suited to meet the immediate response time of today's IoT applications, such as industrial automation, healthcare monitoring and smart city infrastructure.

3.5 Comparative Analysis

We also developed a comparative analysis to assess the performance of the proposed full-duplex secure channel algorithm against the existing security systems and communication protocols based on the IoT. All the metrics clearly indicate that the proposed system is superior to conventional half-duplex systems and other full-duplex security systems primarily with respect to spectral efficiency, security performance, and power consumption, as depicted in Table 1.

.

Table 1: **Comparison of Key Performance Metrics**

Metric	**Full-Duplex System (Proposed)**	**Half-Duplex System**	**Existing Full-Duplex Security Schemes**
Throughput (Mbps)	96	75	85
Power Consumption (mW)	45	60	50
Spectral Efficiency (%)	30	20	25
Secrecy Rate (bits/s)	98	80	90
Latency (ms)	50	65	55

4. CONCLUSION

The full-duplex secure channel algorithm proposed in this paper thus achieves a trade-off between efficiency and security. Through encryption, physical-layer techniques and cooperative jamming, the system maintains a robust security while improving the spectral efficiency by 30% and reducing latency by 15%. For instance, the above-mentioned IoT threats (eavesdropping, jamming and misdirection attacks) have been effectively suppressed with up to a 98% secrecy rate. The proposed algorithm enables adaptive resource allocation, which balances throughput and minimises the total power consumption by 25%. In short, this solution offers an efficient and scalable framework for multicast secure communications in applications that require high robustness, such as smart cities, industrial automation and critical infrastructures.

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. IV Issue 1, June–2024, Pages: 09-13

DOI : https://doi.org/10.54228/mjaret0624003 **ISSN : 2583-1100**

REFERENCES

[1] Y. Zhang et al., "Robust Resource Allocation for Lightweight Secure Transmission in Multicarrier NOMA-Assisted Full Duplex IoT Networks," IEEE Internet of Things Journal, vol. 9, pp. 6443-6457, 2021. https://doi.org/10.1109/jiot.2021.3110974

[2] Y. Sun, D. Ng, J. Zhu, and R. Schober, "Multi-Objective Optimization for Robust Power Efficient and Secure Full-Duplex Wireless Communication Systems," IEEE Transactions on Wireless Communications, vol. 15, pp. 5511-5526, 2016. https://doi.org/10.1109/TWC.2016.2560815

[3] D. Xu and H. Zhu, "Secure Transmission for SWIPT IoT Systems With Full-Duplex IoT Devices," IEEE Internet of Things Journal, vol. 6, pp. 10915-10933, 2019. https://doi.org/10.1109/JIOT.2019.2943377

[4] J. Lim, T. Kim, and I. Bang, "Impact of Outdated CSI on the Secure Communication in Untrusted In-Band Full-Duplex Relay Networks," IEEE Access, vol. 10, pp. 19825-19835, 2022. https://doi.org/10.1109/access.2022.3151792

[5] J. Anajemba et al., "Realizing Efficient Security and Privacy in IoT Networks," Sensors (Basel, Switzerland), vol. 20, 2020. https://doi.org/10.3390/s20092609

[6] M. Li et al., "Improving the Security and Spectrum Efficiency in Overlay Cognitive Full-Duplex Wireless Networks," IEEE Access, vol. 7, pp. 68359-68372, 2019.

[7] M. Shukla, H. Nguyen, and O. Pandey, "Multiuser Full-Duplex IoT Networks With Wireless-Powered Relaying: Performance Analysis and Energy Efficiency Optimization," IEEE Transactions on Green Communications and Networking, vol. 4, pp. 982-997, 2020.

[8] X. Tang, P. Ren, and Z. Han, "Distributed Power Optimization for Security-Aware Multi-Channel Full-Duplex Communications: A Variational Inequality Framework," IEEE Transactions on Communications, vol. 65, pp. 4065-4079, 2017. https://doi.org/10.1109/TCOMM.2017.2715176

[9] Z. Abdullah, G. Chen, M. Abdullah, and J. Chambers, "Enhanced Secrecy Performance of Multihop IoT Networks With Cooperative Hybrid-Duplex Jamming," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 161-172, 2021. https://doi.org/10.1109/TIFS.2020.3005336