Computers and Electrical Engineering 81 (2020) 106502

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A secured and reliable communication scheme in cognitive hybrid ARQ-aided smart city☆

Fazlullah Khan, Ateeq ur Rehman*, Mian Ahmad Jan*

Department of Computer Science, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa 23200, Pakistan

ARTICLE INFO

Article history:
Received 15 December 2018
Revised 29 May 2019
Accepted 30 October 2019
Available online 14 November 2019

Keywords:
Security
Reliability
PU modeling
Smart city
HARQ
Cognitive radio networks

ABSTRACT

Due to advancements in communication technologies, specifically, the Internet of Things (IoT)-based smart cities, the allocation of spectral bands is a major challenge. To overcome this challenge, the cognitive radio network (CRN) has widely been accepted for efficient utilization of the available spectrum. Hence, efficient spectrum utilization and secured communication have attracted significant attention in recent years. However, due to the involvement of smart wireless devices in CRN, the cognitive radio (CR) systems are vulnerable to security threats that mainly target the weaknesses of CR communication and networking. Considering the efficient utilization of spectrum and secured smart city applications, this paper proposes a Secured and Reliable Cognitive Hybrid Automatic Repeat reQuest (SRC-HARQ) scheme. The SRC-HARQ models the primary user (PU) channel by Hidden Markov Model (HMM) to identify the unoccupied spaces. Based on the HMM results, the cluster head (CH) in a smart city determines the activity pattern of PUs and detects idle channels. After the detection of an idle channel, the CH broadcasts a beacon. Upon the reception of a beacon, each member node responds with a ready-to-send (RTS) message along with an encrypted message. The CH replies with a clear-to-send (CTS) signal after the successful decryption of the received message. Furthermore, a 4-state Markov Chain is used for reliability in terms of false alarm and misdetection. The closed-form expressions for mean packet delay, end-to-end delay, and throughput are derived and validated using Monte Carlo simulations.

1. Introduction

In recent years, smart mobile platforms and wireless communication technologies have witnessed significant advancements. The mobile applications are popular among mobile users and business organizations because they can bring significant enhancements in contemporary services. These applications and smart devices have evolved the concept of the Internet of Things (IoT). IoT plays an essential role in the evolution of smart societies. In IoT, every physical object is connected to the Internet to make them smarter. However, the advanced capabilities of IoT are not thoroughly investigated in terms of spectrum utilization and spectrum scarcity. In the context of a smart city's enabled IoT services, spectrum scarcity is one of the main challenges [1]. To resolve the scarcity issue, spectrum regulatory body, i.e., the Federal Communication Commission

☆ This paper is for CAEE special section SI-spsc. Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Weizhi Meng.

* Corresponding authors.
E-mail addresses: fazlullah@awkum.edu.pk (F. Khan), ateeq@awkum.edu.pk (A.u. Rehman), mianjan@awkum.edu.pk (M.A. Jan).

https://doi.org/10.1016/j.compeleceng.2019.106502
0045-7906/

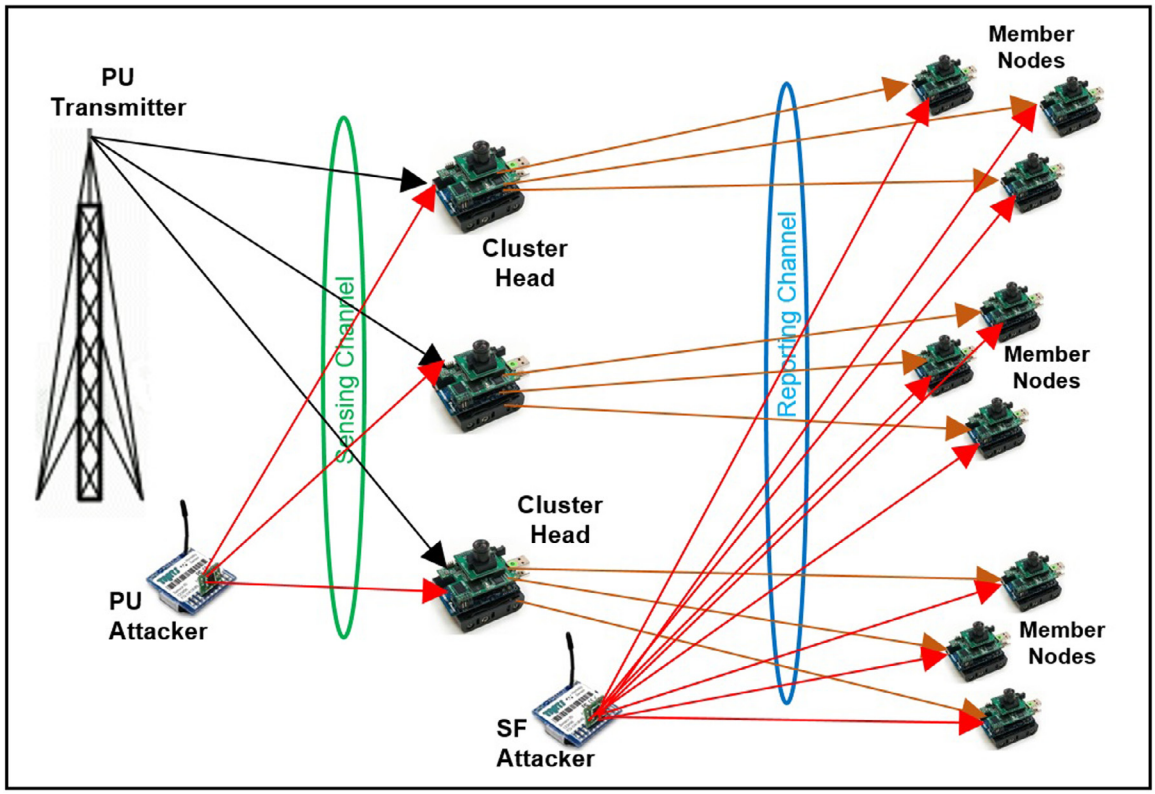


Fig. 1. Network model for the proposed system.

(FCC) has studied the spectrum usage in various regions of the world at different time intervals [2]. These studies revealed that the spectrum scarcity is a man-made problem as 15% to 85% of the spectrum is underutilized due to a static spectrum allocation (SSA) policy [2]. Because of the SSA policy, the spectral bands are exclusively allocated to the primary users (PU), which lead to spectrum scarcity. Therefore, FCC has recommended a dynamic spectrum allocation (DSA) policy to access the idle spectral bands by cognitive radio (CR) users without causing harmful interference to the PUs [2]. The concept of CR emerged after the FCC recommendations, and as a result, it is extensively accepted and adopted by IEEE communication standards, i.e., 802.16h, 802.22, 802.11y, and 1900 [3]. Likewise, the CR concept has been integrated into IoT and smart city applications [4]. There are numerous studies on various aspects of CR-based networks [5,6]; however, security and reliability are still open challenges that need to be addressed. For example, unlike ubiquitous networks, secured and reliable communication in CR-based networks is not only affected by the quality of channel but also by the PU activity over the channel. Therefore, accurate modeling of the PU activity over a channel is essential.

Minimal research work has been conducted for achieving reliability and security in CR networks. The sensing and learning ability of a CR user is one of the weaknesses that can be exploited by a malicious node [7]. For instance, an adversary can quickly launch a primary user emulation (PUE) attack or sensing falsification (SF) attack, which results in the denial of service (DoS), as shown in Fig. 1. In this context, the authors in [8] have studied the reliability, while ignoring the security and activity patterns of the PUs over a channel and their effect on the CR networks. On the other hand, the authors in [7] have analysed security in the CR networks by focusing on the physical layer and proposed a defence mechanism against PUE attacks. In [9], the authors have studied the authentication of PUs using authentication tags and signal properties. Reliable communication in smart cities is achieved using the best quality channel via channel management strategies. In this context, the authors in [10] have proposed on-demand and interference-free solutions, based on adaptive CR networks, for avoiding the jamming attack. The authors in [11] have proposed a secured communication scheme with a lower delay for a cognitive-aided Internet of Vehicles (CIoV). The recent developments in CR-based IoT, sensor networks, and 5G have been studied in [12], whereas, the security and privacy issues in smart city applications and IoT have been investigated in [13] and references therein.

To investigate security and reliability challenges in a CR-based smart city, this paper presents a Secured and Reliable Cognitive Hybrid Automatic Repeat reQuest (SRC-HARQ) scheme. In SRC-HARQ scheme, a cluster head (CH) senses a licensed channel, and once it finds a free time interval (T_I), it broadcasts a beacon. In response, each member node (MN) replies with an RTS along with an encrypted message. If the CH successfully decrypts the message, it sends a CTS to the respective MN; otherwise, the subsequent MN is selected for authentication. The selection process of MNs is based on the principle of first

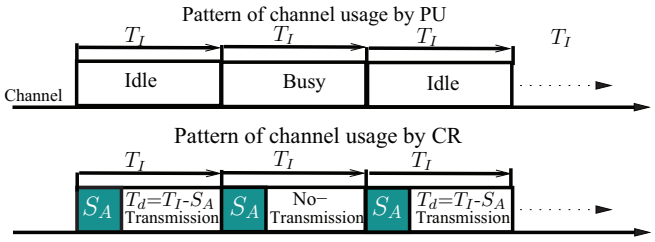


Fig. 2. A licensed channel is equally divided into time intervals T_I, where idle and busy represent the activity of a PU.

come first serve. The CH authenticates MNs to avoid denial of service and replay attacks. Upon authentication, an MN starts data transmission using the principles of SRC-HARQ scheme. By contrast, if the channel is detected busy, the CH waits until the end of T_I and performs sensing again. The CH continuously performs this procedure until a free T_I is detected. To achieve reliability, the system modeled by using a 4-state Markov Chain to avoid the false alarm and misdetection of the PU activity. A CR-based multimedia sensor network is deployed in a smart city, where a CH communicates with MNs using PU channels as depicted in Fig. 1.

The main objectives of this paper are to utilize the spectrum and achieve secured and reliable communication efficiently. Following are the major contributions of this paper:

1. The operation of CH in a smart city is redesigned to observe the PU activity pattern using HMM that results in the detection of unoccupied spaces in the PU channel.
2. For secured communication, the authentication of MNs is performed by the CH in the initial communication.
3. To achieve reliable communication, the SRC-HARQ scheme is modeled using a 4-state Markov Chain. Moreover, for data integrity, each data packet is encoded with a Reed-Solomon scheme to minimize the packet error rate.
4. The proposed scheme is analytically modeled using probabilistic methods to derive closed-form expressions for the *end-to-end delay, mean packet delay*, and *throughput*. The derived closed-form expressions are verified and validated through Monte Carlo simulations.

The rest of the paper is organized as follows. The system model is elaborated in Section 2, followed by the primary user modeling using HMM in Section 3. Section 4 describes the modeling of the SRC-HARQ scheme, whereas the analytical modeling of the SRC-HARQ scheme is discussed in Section 5. The results and discussions are given in Section 6. Finally, Section 7 provides future research directions and concludes the paper.

2. System model

The network model of the proposed SRC-HARQ scheme is shown in Fig. 1. A CH senses the PU channels to communicate with the MNs. In this figure, the green color indicates a CH performing sensing of PU channels, whereas, the blue color represents the communication channels, i.e., data transmission is performed between the CH and member nodes. In other words, when a CH identifies vacant channels, it informs MNs to use these channels for communication. Few assumptions are made while designing the SRC-HARQ scheme. These assumptions are:

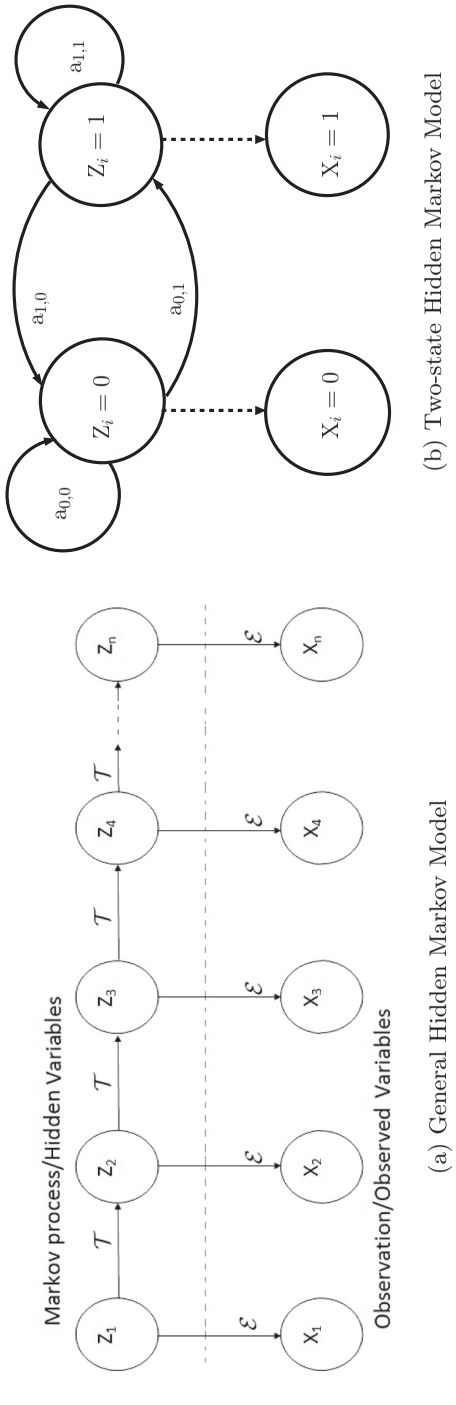
- The sensors are multimedia nodes having higher processing and transmission capabilities.
- The CH is a legitimate node and does not need to participate for authentication.
- The CH shares its secret key (λ) with the MNs during the pre-deployment phase.

2.1. Primary user modeling

In this section, a licensed band is considered that is exclusively assigned to a PU, where each channel is divided into equal length time intervals (T_Is). Each T_I is independent and identically distributed, as shown in Fig. 2. Therefore, a T_I can either be idle or busy. For example, if a T_I is occupied by a PU, it will be occupied till its end. Similarly, if a T_I is found idle, then it is considered idle till its end. In the proposed system, PUs are synchronized to acquire the channel and utilize it, based on T_Is. Moreover, the activity and the transmission pattern of a PU resembles the beginning and end of the T_I. Following the assumptions made in this section, the transmission pattern of a PU follows the natural numbers. In other words, the transmission will not follow the floating points, and hence, the T_I index will always be a discrete number.

3. Primary user activity modeling using HMM

The Hidden Markov Model (HMM) is derived from the Markov model. It can handle real-world applications and is used for sequential or temporal data chain in which the states are partially observable. Fig. 3a depicts the graphical representation of HMM.



(a) General Hidden Markov Model

(b) Two-state Hidden Markov Model

Fig. 3. Hidden markov models.

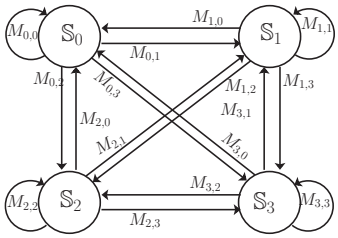


Fig. 4. Four state-Markov Chain representing various cases of attack and no attack, where state $\mathbb{S}_0 = \{0, 0\}$ denotes the scenario in which the channel is idle from PU, and it is correctly sensed to be idle (reliable sensing and no attack), $\mathbb{S}_1 = \{0, 1\}$ illustrates that a channel is idle but falsely detected to be busy (unreliable sensing and attack), likewise are the definition of $\mathbb{S}_2$ and $\mathbb{S}_3$.

In HMM, the discrete random variables are $Z = Z_1, Z_2, \ldots, Z_n \in \{1, 2, \ldots, m\}$, and X=$X_1, X_2, \ldots, X_n \in$ X={discrete values, real values, R^d }. Here, X is the observed random variables, and Z are hidden variables. In the proposed model, the hidden variables represent the actual PU activity, whereas observed variables are energy on a spectrum under sensing by a CH. The joint distribution of these random variables is factorized in the following way, which corresponds to the HMM model of Fig. 3a.

$$P(X_1, X_2, \ldots, X_n, Z_1, Z_2, \ldots, Z_n) = P(Z_1)P(X_1|Z_1)\Pi_{k=2}^{n}P(Z_k|Z_{k-1})P(X_k|Z_k). \quad (1)$$

The final observe results, $P(X_k|\ X) = \beta_k(Z_k)\alpha_k(Z_k)$, is obtained using HMM. It means that for an observed value of X, the values of Z can be predicted. The detailed description of the Hidden Markov Model can be studied in [14,15].

For easy understanding, the spectrum sensing model is used based on 2-state HMM. The 2-state HMM is based on two hypotheses: 1) H_0 $\{Z_i = 0\}$ (No activity on PU channel), and 2) H_1 $\{Z_i = 1\}$ (PU channel is busy). These hypotheses show that T_I is free or busy, respectively. The prior probabilities of state 0 and state 1 are $P_{(H_0)}$, i.e., α, and $P_{(H_1)}$, i.e., β, respectively. The PU activity is modeled using 2-state homogeneous Markov chain with the state space Z_i, where $Z_i \in$ {0,1}. Here, Z_i variables are hidden because they are not directly observable due to the impact of additive white Gaussian noise and the channel fading [16]. The CR senses the PU channel and receives its observation result X_i, which is the local decision of a CR for a particular T_I. The observation state space is X_i, where $X_i \in$ {0, 1}. An HMM can be denoted by $\lambda = (\pi, T, \varepsilon)$, where π is the initial state distribution, i.e., $\pi = \{\pi_i\}$, and $\pi_i = P(Z_1 = i)$, $\forall$ i $\in$ Z. The transition probability matrix, $T = \{a_{ij}\}$, $a_{ij} = P(Z_{t+1} = j|Z_t = i.)$, $\forall$ i, j $\in$ {0, 1}; The emission probability matrix: $\varepsilon_i = \{b_{jk}\}$, and $b_{jk} = P(X_t = k|Z_t = j)$, $\forall$ j $\in$ Z, and $\forall$ k $\in$ X. In the sensing scenario, $\pi_i = P_{(H_i)}$, $\forall$ i $\in$ X, $\varepsilon = P_{(H_k|H_j)}$, $\forall$ j $\in$ Z, and $\forall$ k $\in$ X.

3.1. Channel modeling by CR-cluster head

To perform data transmission over a licensed channel, each T_I is further arranged into two periods, as discussed in Section 2.1. It is to be noted that when a CH performs accurate sensing, then the 2-state Markov Chain or HMM is a better choice. However, in the presence of an attacker or due to channel impairments, the sensing results of HMM cannot be accurate, and thus, these models are not fit to configure the system accurately. As a result, this paper modeled the CR activity by a 4-state Markov Chain to incorporate the scenarios raised due to false alarm (P_{fa}) and misdetection (P_{md}).

In this paper, the CR activity is modeled by a 4-state Markov Chain to consider the scenarios of unreliable sensing, i.e., (P_{fa}) and (P_{md}). For instance, when the sensing operation declares that T_I is in the busy state, but in reality, it is in the idle state, as in the case of unreliable sensing. P_{fa} represents this case. Similarly, when T_I is in use of a PU and is considered free to be used by MNs. P_{md} represents this case. In Fig. 4, a 4-state Markov Chain is graphically illustrated, where the state index is based on two binary digits, i.e., Ψ_a and Φ_s. The digit in Ψ_a represents the actual status of T_I whereas Φ_s illustrates the sensed status of T_I. Mathematically, it can be presented as in [17]:

$$\Psi_a = \begin{cases} 1, & \text{PU is active in real,} \\ 0, & \text{PU is not active in real.} \end{cases} \quad (2)$$

$$\Phi_s = \begin{cases} 1, & \text{CH sensed that PU is active,} \\ 0, & \text{CH sensed that PU is not active.} \end{cases} \quad (3)$$

Specifically, the state index can be obtained with the help of binary digits. For example, 0,0 becomes state $\mathbb{S}_0$ representing the channel is idle ($\Psi_a = 0$), and it is also sensed to be idle ($\Phi_s = 0$) (P_i and 1-P_{fa}). Similarly, $\mathbb{S}_1$ is the combination of 0,1 illustrating the situation in which a channel is free ($\Psi_a = 0$) but wrongly sensed to be busy ($\Phi_s = 1$), this is the case of P_i and P_{fa}. Likewise, the indices for states $\mathbb{S}_2$ and $\mathbb{S}_3$ are generated. The transition probabilities between states are illustrated in Fig. 4, and the probability matrix $\boldsymbol{M_m}$ is presented as,

$$\boldsymbol{M_m} = \begin{bmatrix} M_{0,0} & M_{0,1} & M_{0,2} & M_{0,3} \\ M_{1,0} & M_{1,1} & M_{1,2} & M_{1,3} \\ M_{2,0} & M_{2,1} & M_{2,2} & M_{2,3} \\ M_{3,0} & M_{3,1} & M_{3,2} & M_{3,3} \end{bmatrix}.$$

The state to state transitions are shown in Matrix $\boldsymbol{M_m}$, and probabilities are given below,

$$\begin{aligned} M_{0,0} &= M_{1,0} = M_{2,1} = M_{3,1} = P_i \times (1 - P_{\text{fa}}) \\ M_{0,1} &= M_{1,1} = M_{2,1} = M_{3,1} = P_i \times P_{\text{fa}} \\ M_{0,3} &= M_{1,3} = M_{2,3} = M_{3,3} = P_b \times (1 - M_d) \\ M_{0,2} &= M_{1,2} = M_{2,2} = M_{3,2} = P_b \times M_d. \end{aligned} \tag{4}$$

Similarly, the idle and busy states, P_i and P_b, for 2-state Markov Chain in terms of probability can be written as in [18],

$$P_i = \frac{\alpha}{\alpha + \beta} \quad \& \quad P_b = \frac{\beta}{\alpha + \beta}, \tag{5}$$

where P_i is the probability that a channel is in an idle state, and P_b is the probability that a channel is in a busy state, respectively. For clarification, the transition from any state going to $\mathbb{S}_0$ means that the channel is free (P_i) and no false alarm happened, i.e., $(1 - P_{fa})$. Therefore, in Eq. (4), the associated transition probabilities for all states can be shown. Let $\pi = [\pi_0, \pi_1, \pi_2, \pi_3]^T$ represent the probabilities of each state when the Markov Chain became steady. This is achieved by evaluating the following equation [19]:

$$\pi = \boldsymbol{M}^n \times \pi. \tag{6}$$

The steady-state (π) is the right eigenvector of M^n having eigenvalue one. Hence, Eq. (6) gives the following,

$$\pi = [\pi_0 \quad \pi_1 \quad \pi_2 \quad \pi_3]^T. \tag{7}$$

Substituting the transition probabilities from Eq. (4) in the transition matrix $\boldsymbol{M_m}$, the closed-form expression for each steady state is derived through Gaussian elimination method as below,

$$= \sigma \times \left[\frac{\alpha \times (1 - P_{\text{fa}})}{\beta \times (1 - P_{\text{md}})} \times \quad \frac{\alpha \times (P_{\text{fa}})}{\beta \times (1 - P_{\text{md}})} \times \quad \frac{(P_{\text{md}})}{(1 - P_{\text{md}})} \times \quad 1 \right]^T, \tag{8}$$

where $\sigma \in \mathbf{R}$[1], satisfying the condition of

$$\sum_{i=0}^{3} \pi_i = 1. \tag{9}$$

results in

$$\sigma = P_b \times (1 - P_{\text{md}}). \tag{10}$$

Following the probabilities of steady-states, i.e., $\mathbb{S}_0, \mathbb{S}_1, \mathbb{S}_2$ and $\mathbb{S}_3$, of the proposed model, results in Eq. (11)

$$\pi_0 = P_i \times (1 - P_{\text{fa}}), \quad \pi_1 = P_i \times P_{\text{fa}}, \quad \pi_2 = P_b \times P_{\text{md}}, \quad \pi_3 = P_b \times (1 - P_{\text{md}}). \tag{11}$$

4. Secure and reliable cognitive HARQ (SRC-HARQ) scheme

The proposed system carries out two primary operations: reliable sensing and secured data transmission. Using these two operations, the cognitive-based CH initiates sensing process and allow/do not allow an MN for data transmission to transmit data based on the sensing results obtained from HMM. For reliable sensing of the PU activity, the 4-state Markov Chain is used. The purpose is to countermeasure the PUE and SF attacks on CHs and MNs. Likewise, for secured communication, the CH authenticates each MN to avoid DoS and replay attacks. For example, when the CH detects a free T_I, it broadcasts a beacon message to all MNs. Upon receiving the beacon, an MN sends an RTS along with an encrypted message in the current T_I. The MN encrypts its ID using λ that was shared in the pre-deployment phase, as discussed in Section 2. If the CH decrypts the message correctly, it sends a CTS message to the MN. Otherwise, the CH starts authenticating the RTS received from the subsequent MN. Note that, the CH follows the principles of first come first serve for MN authentication. When authentication is successful in a free T_I, then the respective MN starts data transmission based on the principles of SRC-HARQ. In contrast, if the channel is detected busy, the CH waits until the end of T_I and performs sensing again. The CH continues this procedure until an idle T_I is detected. Furthermore, in the presence of an attacker, the CH may incorrectly decide a busy T_I to be idle (P_{md}), or an idle T_I to be busy (P_{fa}). This is known as Intelligence Compromise (IC) attack in which the CR activity could not be performed intelligently. This results in either collision with PU transmission or decreases the opportunities of data transmission over a PU channel.

To attain the integrity of data, Reed-Solomon (RS) encoding/decoding method is considered for the sake of identifying and/or rectifying erroneously received packets. To do so, every data packet is encoded with RS code-word, RS(N_d, K_d) [20], where N_d represents the appended RS symbols, and K_d shows information bits. Each MN requires a T_p second for the transmission of an encoded packet, where a T_I has one or more T_ps, i.e., $T_I > T_p$. When an encoded packet is received at the CH, the decoding technique of an RS is applied to retrieve the original information bits. For simplicity, it is assumed that the

[1] **R** is rational number.

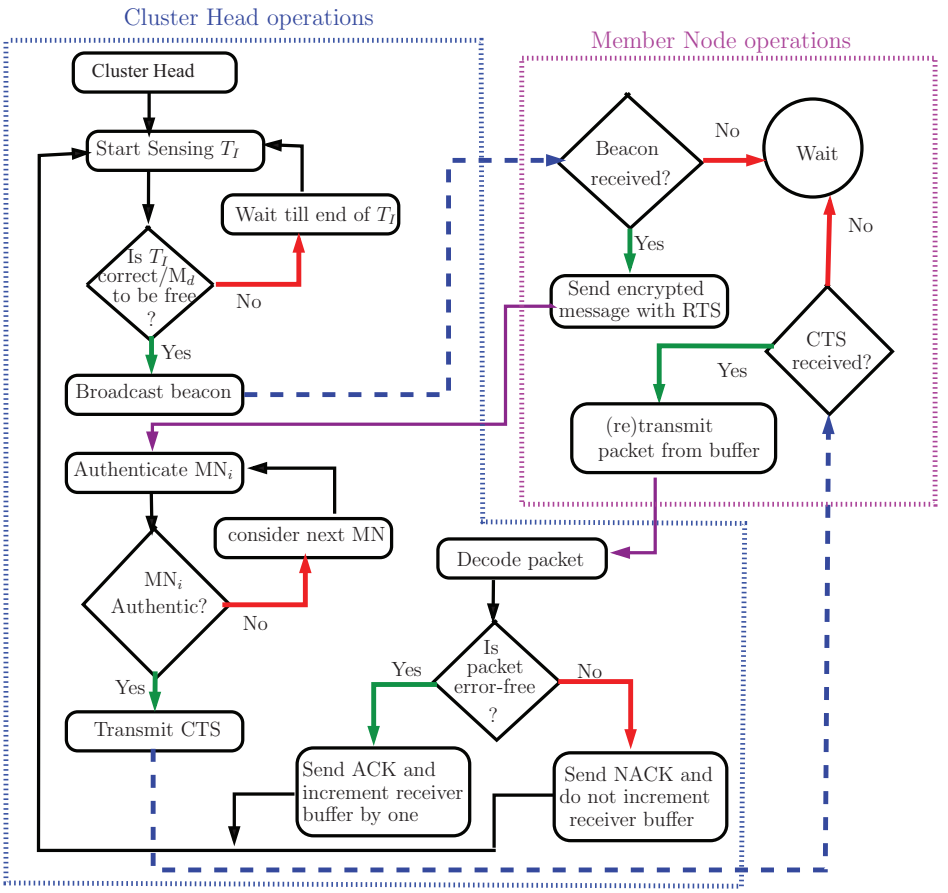


Fig. 5. Flow Chart of the Secured and Reliable Communication in SRC-HARQ Scheme.

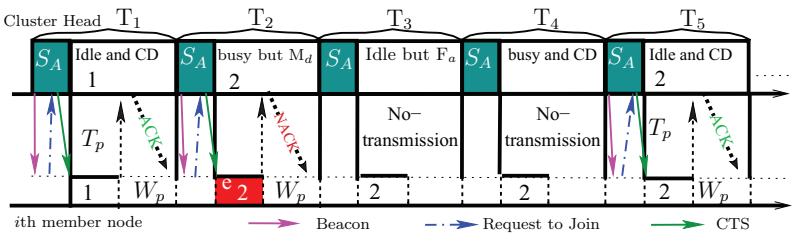


Fig. 6. Systematic diagram for packet transmission using a secured and reliable SRC-HARQ scheme, where CD represents the correct detection.

RS decoding operation correctly identifies the number of errors in a packet. If the number of errors exceeds the correction capacity ($e=\frac{N_d-K_d}{2}$) of an RS code, the packet is considered to be in error; otherwise, it is deemed rectified.

Using these arrangements, the SRC-HARQ scheme is designed, where data packets are transmitted between CH and MNs. The SRC-HARQ scheme is efficient against various attacks such as data forgery, data integrity, DoS, replay, and IC attacks. The working procedure of the proposed SRC-HARQ is given in Algorithm 1, and the flow chart is shown in Fig. 5. Moreover, the effect of reliable communication is depicted in Fig. 6, where T_1 is idle and correctly detected, and therefore, packet 1 is transmitted. On the other hand, T_2 is busy but misdetected. Hence, due to the collision, the packet is received in error, and a negative acknowledgment (NACK) has been transmitted. Similarly, T_3 is idle, but false alarm occurs; hence, no transmission takes place. Finally, in T_4, the channel is busy and correctly detected. Moreover, in Fig. 6, the handshake process using three different colors is shown. The pink color is the initial beacon transmitted by a cluster head after identifying vacant channels. The blue color arrow is the RTS from a member node that contains an encrypted message with the cluster head key (λ). Finally, the green color arrow shows the CTS from a cluster head to a member node.

Algorithm 1 Secured Communication over Unreliable Channel in SRC-HARQ Scheme.

Initialization: N_s = total packets, k = 1, T_I = 1
Input: packet

1: **procedure**
2: **while** $k < N_s$ **do**
3: **if** a packet in CH buffer? **then**
4: RS decoding is applied on the packet ▷ For data integrity
5: **else** CH senses channel in T_I
6: **if** T_I is idle (correct/P_{md}) **then** ▷ P_{md} is due to an unreliable sensing & it is considered as a PUE attack
7: CH broadcasts a beacon message
8: MN(i) sends RTS with an encrypt message ▷ An MN enrypts its ID with λ, and sends to CH after receiving a beacon.
9: CH decrypts, the encrypted message received from MN(i) with its secret key λ
10: **if** the message is encryptable by the CH **then**
11: CH transmits CTS to MN(i)
12: **else** discard MN(i) and consider next node
13: i=i+1 and goto **line 7**
14: end **if**
15: **if** MN(i) receives a CTS or Acknowledgment **then**
16: (re)transmit a packet
17: **if** the received k^{th} packet is error-free **then**
18: ACK signal is sent to the respective MN(i) by the CH
19: k = k+1
20: **elseif** k^{th} packet is in error **then**
21: NACK is sent by the CH
22: The process reiterates from **line 15**
23: end **if**
24: end **if**
25: **else** keep on wait until a beacon is received
26: end **if**
27: **else** the T_I is busy (correct/P_{fa}) ▷ P_{fa} is due to unreliable sensing and IC attack
28: The CH does not send beacon and wait until the end of a T_I.
29: $T_I = T_I + 1$
30: The process reiterates from **line 5**
31: end **if**
32: end **if**
33: end **while**
34: **end procedure**

4.1. Authentication of member nodes

The authentication scheme is resilient against forgery, DoS and replay attacks. Each MN utilizes a channel sensed "free" by a CH, and the user of a channel may be an authentic user or an attacker. Before utilizing a channel, it is assumed that the CH is authentic, and has shared a 128-bit secret key, λ, with the MNs. It is assumed that λ is known to the CH and all the MNs in a network. Once the CH senses a free channel, it broadcasts a beacon message. The MN sends an RTS along with a message containing its ID encrypted with λ. The CH decrypts the message received along with RTS using its key λ and authenticates the MN. If it is unable to decrypt the message, the MN is considered a malicious node. The procedure for the authentication of member nodes is shown in Algorithm 1.

4.2. Working principles of cluster head

As discussed above, in SRC-HARQ scheme, the CH performs two vital functions, i.e., reliable sensing and secured communication. Firstly, it initiates reliable sensing for analyzing PU activity over a licensed channel. That is, when CH senses and finds T_I to be busy, it will wait till the end of its duration and start sensing the next T_I. Once an idle T_I is detected, the CH transmits a beacon to all MNs and waits for their responses (RTS) along with an encrypted message for authentication. The CH select an MN based on first come first serve, i.e., all MNs transmit their RTSs along with encrypted messages. After reception of RTSs, the CH start authenticating the first RTS received from MN and acknowledged it by transmitting a CTS if authentication is successful. Otherwise, the subsequent RTS is processed. This process continues until an MN is authenticated. It is assumed that the sensing and authentication process takes T_p seconds. After authentication, when an MN

receives a CTS, it starts transmitting a packet from the buffer to CH and waits for its acknowledgment. If required, the CH decodes and rectifies the received packet, and generates ACK/NACK for error-free/erroneous packet, respectively. Moreover, the CH has a buffer of size 1, which is updated based on the packet reception. When a CH receives an error-free packet, it increments its buffer and sends an ACK to the MN. On the other hand, if the packet is received in error, i.e., forgery attack, a NACK is sent to the MN, and the buffer is not incremented. Similarly, when a T_I is found busy due to correct or misdetection, the CH will neither update its buffer nor broadcast a CTS. For example, at time T_1, the CH receives an error-free packet. Therefore, an ACK is transmitted to the given MN, and the buffer is updated from index 1 to 2, as shown in Fig. 6. On the other hand, at time T_2, the packet is erroneously received. Therefore, NACK is transmitted, and the buffer remains unchanged.

4.3. Working principles of a member node

In SRC-HARQ scheme, all MNs are assumed to have a joint buffer in which packets are stored in ascending order. Only one packet can be transmitted at a time by an MN from the buffer using the proposed scheme. The working principle of an MN is as follow: Initially, MNs are waiting for the reception of a beacon from the CH. When an MN receives a beacon, it replies with an RTS along with its encrypted ID (λ). When an MN is authorized by receiving CTS from the CH, it transmits any old or new data packet from the joint buffer over a PU channel. Otherwise, CH ignores this MN and starts authenticating the RTS and encrypted ID of the subsequent MN from the queue, as presented in Algorithm 1. The remaining MNs, remain silent during the transmission until the announcement of broadcasting a beacon. This concept is out of the scope of this paper. Furthermore, the MNs wait for W_p seconds to receive ACK/NACK signal, where W_p is the waiting period for feedback reception. Upon receiving an ACK, the MN removes the replica of a successfully transmitted packet from the buffer and increments it by one. If in the case, a NACK is received, the buffer is not incremented, and the erroneous packet is retransmitted by an MN in the next idle T_I. This procedure is repeated for every packet stored in the joint buffer of MNs.

5. Analytical modeling of SRC-HARQ scheme

In this section, the proposed SRC-HARQ scheme is analytically modeled in terms of the mean packet delay, end-to-end (E2E) packet delay, and throughput. The analysis used a probabilistic approach and compared analytical results with the simulation results. In the following subsection, the probabilistic analysis for mean packet delay is performed.

5.1. Mean packet delay

In traditional networks, apart from propagation delay, the delay occurs due to unreliable communication channel that results in the erroneous packets being retransmitted. Similar to the conventional networks, the delay in SRC-HARQ is caused by the adversaries and unreliability of the channel. The proposed scheme also faces additional delay due to P_{fa} and M_d of the PU channel. To examine the delay of SRC-HARQ scheme, the mean delay with Π is symbolized. There are two possibilities that a PU channel can be detected busy. These are:

1. T_I is correctly detected in a busy state.
2. T_I is falsely detected in an idle state, i.e., in the case of Intelligence Compromise (IC) attack.

Based on the definitions in Section 3.1, the probability that a CH detects a busy T_I can be mathematically evaluated as,

$$\begin{aligned} P_{busy} &= P_b \times (1 - P_{\text{md}}) + P_i \times P_{\text{fa}}, \\ &= \frac{\beta \times (1 - P_{\text{md}})}{\alpha + \beta} + \frac{\alpha \times P_{\text{fa}}}{\alpha + \beta}, \\ &= \frac{1}{\alpha + \beta} \times [\beta \times (1 - P_{\text{md}}) + \alpha \times P_{\text{fa}}]. \end{aligned} \tag{12}$$

In contrast, there are two possibilities for a CH to transmit the data over a PU channel:

1. T_I is correctly detected in an idle state, i.e., no P_{fa}.
2. T_I is misdetected as in the idle state. The M_d will cause a collision, and hence, the packets need to be retransmitted that causes a higher delay. One of the reasons behind M_d is a PUE attack.

Following the definitions of Section 3.1, the probability that a CH detects a T_I idle is computed as shown in Eq. (13),

$$\begin{aligned} P_{idle} &= P_i \times (1 - P_{\text{fa}}) + P_b \times P_{\text{md}}, \\ &= \frac{1}{\alpha + \beta} \times [\alpha \times (1 - P_{\text{fa}}) + \beta \times P_{\text{md}}]. \end{aligned} \tag{13}$$

Suppose $\Pi(i)$ is the delay imposed by $(i-1)$ busy T_Is before detecting an idle T_I, producing

$$\Pi(i) = (i - 1) \times T_I. \tag{14}$$

Then, the average delay (Π) faced by a CH to detect an idle T_I can be analytically expressed as follow,

$$\begin{aligned}\Pi &= E \times [\Pi(i)] = E \times [(i-1) \times T_I],\\ &= \sum_{i=1}^{\infty} (i-1) \times T_I P_{busy}^{i-1} \times P_{idle},\\ &= \frac{(P_{busy} \times P_{idle}) \times T_I}{(1-P_{busy})^2} = \frac{P_{busy} \times T_I}{(1-P_{busy})},\\ &= \frac{\alpha \times P_{\text{fa}} + \beta \times (1-P_{\text{md}})}{\alpha \times (1-P_{\text{fa}}) + \beta \times P_{\text{md}}} \times T_I. \end{aligned} \tag{15}$$

After detection of an idle T_I from Eq. (15), now the transmission delay introduced by unreliable sensing and/or PUE attack is formulated. Specifically, a delay of (T_I-S_A)T_p seconds is imposed, when a packet is correctly transmitted in the first attempt, while a delay of T_I seconds is imposed when a packet is received in error. Therefore, let $\xi(i)$ represents the delay of a packet that is successfully received by the CH after i attempts. It includes both the transmission delay and the delay of detecting an idle T_I. Hence, to formulate the transmission delay, a T_I can be in an idle state in two cases. First, when a T_I is correctly detected to be in an idle state, then Eq. (16) can be obtained,

$$\Omega = \frac{P_i \times (1-P_{\text{fa}})}{P_{idle}}, \tag{16}$$

where P_{idle} is given in Eq. (13). Second, when a T_I is misdetected to be free, then Eq. (17) can be obtained,

$$\Upsilon = \frac{P_b \times P_{md}}{P_{idle}}. \tag{17}$$

Hence, the total delay after the ith attempt is,

$$\xi(i) = i \times (T_I + \Pi), \tag{18}$$

where i is the number of transmission attempts for correctly transmitting a packet.

Following the principles of SRC-HARQ scheme, in every idle T_I, MN transmits a packet. Therefore, the mean packet delay (ξ) can be computed as,

$$\xi = \frac{1}{N} \times E[\xi(i)] = \frac{1}{N} \times E[i(T_I + \Pi)], \tag{19}$$

where $N=T_I - S_A$ is the amount of time taken by a packet from its transmission until its acknowledgement. Furthermore, the packet error probability is represented by P_e, denoting packets that are received in error after RS decoding. It is assumed that P_e for those packets that are transmitted in misdetected T_Is are as high as one. Then, Eq. (20) can be formulated as,

$$\begin{aligned}\xi &= \sum_{i=1}^{\infty} \sum_{j=0}^{i-1} i \times (T_I + \Pi) \times \binom{i-1}{j} \times (\Upsilon)^j \times (\Omega)^{i-j} \times (P_e)^{i-j-1} \times (1-P_e)\\ &= \frac{T_I}{N} \times (1+\kappa) \times \left(\sum_{i=1}^{\infty} \sum_{j=0}^{i-1} \binom{i-1}{j} \times i \times (\Upsilon)^j \times (\Omega)^{i-j} \times (P_e)^{i-j-1} \times (1-P_e) \right)\\ &= \frac{T_I}{N} \times \left(\frac{\Omega \times (1-P_e) \times (1+\kappa)}{(\Upsilon + \Omega \times P_e - 1)^2} \right) \text{ (sec)}, \end{aligned} \tag{20}$$

where $\kappa = \Pi / T_I$.

To normalize the average packet delay in terms of T_ps can be expresses as,

$$\xi = \left(\frac{k+N}{N} \right) \left(\frac{\Omega \times (1-P_e) \times (1+\kappa)}{(\Upsilon + \Omega \times P_e - 1)^2} \right) T_p s, \tag{21}$$

where $T_I = (T_p + W_p) \times T_p$ is applied.

5.2. End-to-End packet delay

After mathematically modeling the mean packet delay, now closed-form expressions are derived for the probability mass function (PMF) of E2E packet delay and mean E2E delay. The E2E delay can be defined as the time taken by a packet from its first transmission attempt till its final successful reception at the CH. Based on this definition, the PMF of the proposed scheme is modeled in the following subsection.

5.2.1. Probability mass function

The delay between a packet's first transmission and its successful delivery depends on two factors: 1) erroneous transmission, and 2) occurrence of busy T_Is. For clarity, the PMF for E2E packet delay caused by re-transmissions need to be derived, and then the occurrence of busy T_Is between packet's first transmission and its error-free reception at the CH.

In the first case, when a CH does not detect any busy T_Is between the initial transmission and successful delivery of a packet, then the probability that n T_Is are utilized for the successful delivery of a packet can be formulated as,

$$P_{e2e}(n) = \left(\sum_{j=0}^{n-1} \binom{n-1}{j} \times (P_b \times P_{md})^j \times (P_i(1-P_{\text{fa}}) \times P_e)^{n-j-1} \times (1-P_e)\Omega \right), \text{ where } n = 1, 2, \ldots \tag{22}$$

Eq. (22) can be explained as follows:

- $(\mathrm{P}_b \times \mathrm{M}_d)^j$ describes the probability that j out of $(n-1)$ T_Is are found idle by the CH due to M_d, resulting in erroneous transmission in these T_Is.
- $(P_i \times (1-P_{\text{fa}}) \times P_e)^{n-j-1}$ infers the probability that the rest of $(n-j-1)$ T_Is are accurately detected idle $(1-\mathrm{F}_a)$ by CH. Erroneous transmission in $(n-j-1)$ T_Is is due to the unreliability of the channel.
- Finally, $(1-\mathrm{P}_e) \times \Omega$ shows the probability of final T_I, being idle and is detected correctly, resulting in the successful delivery of packets.

In the second case, when busy T_Is are detected during the transmission of a packet, then Eq. (23) is obtained,

$$\begin{aligned} P_{e2e}(n) = & \sum_{i=0}^{n-2} \sum_{j=0}^{n-i-1} \binom{n-2}{i} \times \binom{n-i-1}{j} \times (P_{busy})^i \\ & \times (P_b \times P_{\text{md}})^j \times (P_i \times (1-P_{\text{fa}}) \times P_e)^{n-i-j-1} \times (1-P_e)\Omega, \text{ where } n = 1, 2, \ldots \end{aligned} \tag{23}$$

In Eq. (22), the term $\binom{n-2}{i} P_{busy}^i$ shows the probability of i T_Is that are detected busy during the initial transmission and successful delivery of a packet. The maximum values i can take are $n-2$ because the first and last T_Is should be idle for initiating and completing the transmission process.

5.2.2. Average End-to-End packet delay

After obtaining PMF of an E2E packet delay, the mean E2E packet delay can be computed as given in Eq. (24),

$$\begin{aligned} \rho &= \sum_{n=1}^{\infty} n \times P_{e2e}(n), \\ &\approx \sum_{n=1}^{\mathrm{M}_T} n \times P_{e2e}(n), \end{aligned} \tag{24}$$

where ρ is calculated in T_Is and M_T represents the maximum delay that can be considered for ignoring the probability of events having a slim chance of occurrence. For instance, M_T can be selected for quantifying $\sum_{m=1}^{\mathrm{M}_T} P_{e2e}(m) = 1 - 10^{-8}$.

5.3. Throughput

Based on the mean packet delay given in Eq. (20), the throughput of SRC-HARQ scheme is obtained as shown in Eq. (25),

$$\begin{aligned} R_s &= \frac{1}{\xi}, \\ &= \frac{N}{T_I} \times \left(\frac{(\Upsilon + \Omega \times P_e - 1)^2}{\Omega \times (1-P_e) \times (1+\kappa)} \right) \text{ (pkt/sec)}, \\ &= N \times \left(\frac{(\Upsilon + \Omega \times P_e - 1)^2}{\Omega \times (1-P_e) \times (1+\kappa)} \right) \text{ (PPT}_I\text{)}, \\ &= \frac{N}{k+N} \times \left(\frac{(\Upsilon + \Omega \times P_e - 1)^2}{\Omega \times (1-P_e) \times (1+\kappa)} \right) \text{ (PPT}_p\text{)}. \end{aligned} \tag{25}$$

Moreover, let (N_d, K_d) RS code is used, then the throughput can be computed as shown in Eq. (26),

$$R_s = \frac{1}{\xi} \times K_d \times B, \tag{26}$$

where R_s is calculated in bits per second (bps) and B represents the number of bits in a code symbol.

6. Performance results

In this section, the performance of SRC-HARQ scheme is evaluated in terms of mean packet delay, E2E delay, and throughput. It can be demonstrated that P_e, P_b, P_{md}, and P_{fa} have a significant effect on the performance of the proposed scheme. It is essential to mention that in the case of reliable sensing, the values of P_{md} and P_{fa} are zero. The proposed scheme has been designed and implemented using MATLAB, where one hundred thousand packets are transmitted in each case. The simulation begins by sensing the first T_I and ends when N_s packets are sent.

In Fig. 7a, the handshake/authentication time of the proposed scheme is compared to the previous security scheme [21]. It is worth mentioning here that in [21], lightweight sensor nodes were used, and in this paper, powerful multimedia sensor nodes are used. In the proposed scheme, one T_p is enough for authentication and sensing a PU channel, because SRC-HARQ uses a lightweight approach and relies on a 3-way handshake in contrast to the 4-way handshake proposed in [21]. In Fig. 7b, the response time for one-byte of data is shown. This figure makes a comparison among three schemes, i.e., data transmission without security, the SRC-HARQ, and the scheme proposed in [21]. The proposed scheme outperforms the existing schemes in terms of handshake duration and response time due to its lightweight approach, i.e., using a 3-way handshake.

In Fig. 8a, the probabilities of all possible states of a PU or CH in a T_I are illustrated. For example, π_0, π_1, π_2 and π_3 represent P_i, P_{fa}, P_{md} and P_b, respectively, for both cases of unreliable and reliable channel sensing, as given in Eq. (11). It is evident from Fig. 8a that for unreliable sensing, the increase in β causes a significant decrease in $P_i = \pi_0$ and a minimal decrease in $P_{fa} = \pi_1$. This minimal decrease in π_1 is the result of unreliable sensing. On the other hand, an increase in β causes a significant increase in $P_b = \pi_3$. Due to unreliable sensing, the increase in $P_{md} = \pi_2$ is minimal. Similarly, in the case of reliable sensing, there is no change in $P_{md} = \pi_2$, and $P_{fa} = \pi_1$ for any value of β. This is mainly due to the fact that for reliable sensing, $P_{md} = P_{Fa} = 0$. For $P_i = \pi_0$, there is a significant decrease that shows the availability ratio of a channel for CH. On the other hand, for $P_b = \pi_3$, a significant increase shows the transmission of PU over the channel. The analytical results closely match with the simulation results as depicted in Fig. 8a.

The throughput of SRC-HARQ scheme is shown in Fig. 8b. Here, the throughput is calculated against P_e and P_b of the PU channel, using Eq. (27).

$$\eta'_S = \frac{N_s}{N_{T_I}} \times \frac{T_p}{S_p + W_p}, \tag{27}$$

where the throughput η'_S is calculated in packets per T_p, N_{T_I} is the number of T_Is used for correctly transmitted N_s packets by MNs. It is obvious from Fig. 8b that throughput is inversely proportional to P_e. Initially, when the channel is highly reliable, i.e., P_e=0, and there is no PU activity over the channel, the throughput is at the peak in reliable sensing as well as in the scenario of unreliable sensing, and gradually goes down when P_e increases. The reason for a low throughput is the unreliability of the channel, which is caused by an increase of P_e. The linear decrease in throughput is due to re-transmission of data packets. Furthermore, another parameter that affects the throughput is P_b. For lower values of P_b, the throughput is high, and vice versa. The throughput drops significantly with an increase of P_b values because the CH takes a longer time to detect an idle T_I. When $P_e = P_b = 0$, the throughput is at the peak and reduces when P_e and/or P_b increases. In Fig. 8b, the throughput for unreliable sensing is lower in comparison to reliable sensing. It is because, unreliable sensing considers P_{md} and P_{fa}, which are essential for attaining reliable sensing in CRNs. In the case of unreliable sensing, the CH may not correctly perform sensing. As a result, a collision occurs, and idle T_Is are wasted due to M_d and P_{fa}. These effects are clearly depicted in Fig. 8b. For example, when $P_{md} = 0.2$ and $P_{fa} = 0.2$, the throughput of SRC-HARQ scheme drops due to the wrong sensing results, as the channel under considerations is unreliable. Moreover, the simulation results and analytical findings of Eq. (21) match with each other, as illustrated in Fig. 8b.

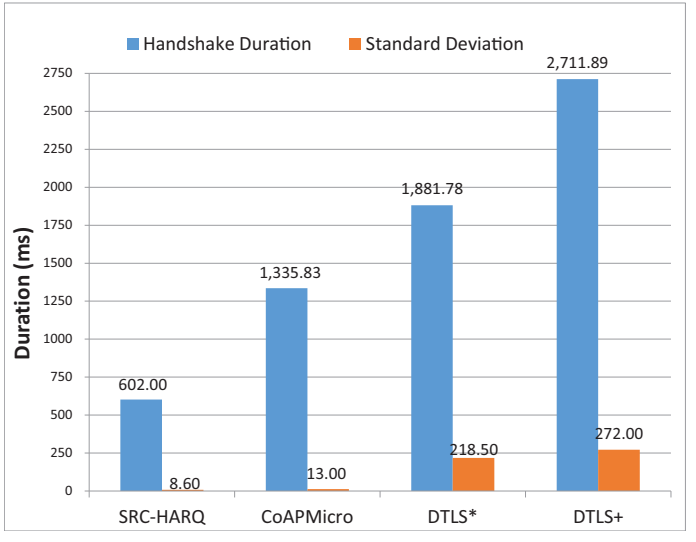
After elaborating the throughput of SRC-HARQ scheme, now delay of the proposed scheme is discussed. The mean packet delay, as depicted in Fig. 9b, is analyzed. It is worth mentioning that the mean packet delay for simulation results is computed using Eq. (28).

$$T_{DS} = \frac{N_{T_I} \times (T_p + W_p)}{N_s} \quad \text{(s)}. \tag{28}$$

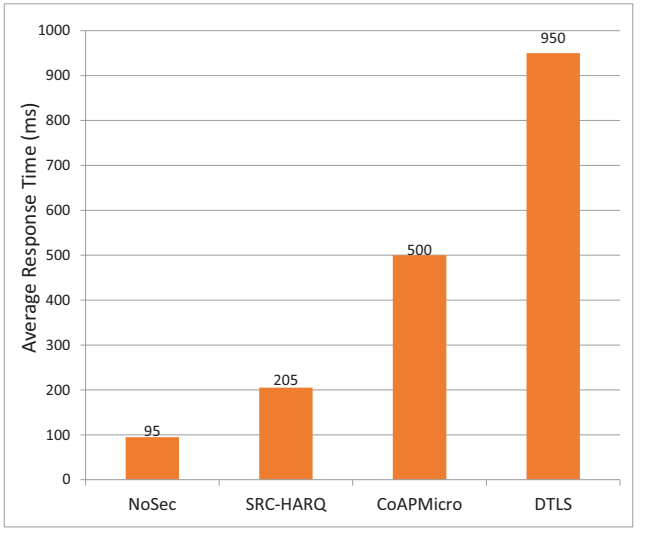
where N_s is the total number of packets successfully transmitted by MNs, and N_{T_I} is the number of T_Is used. Fig. 9b shows results that are normalized by T_p to yield Eq. (29).

$$\delta' = \frac{\delta}{T_p} \quad (T_p s). \tag{29}$$

The mean packet delay of SRC-HARQ scheme is presented in Fig. 9b. Initially, the mean packet delay is at the lowest level due to channel reliability ($P_e = 0$) where sensing results are perfect, i.e., reliable sensing. It is clear from Fig. 9b, even at $P_e = 0$, there is a delay which is caused by P_b. However, if the values of P_e and/or P_b increase, the average packet delay increases for reliable sensing as well as unreliable sensing. In Fig. 9b, the higher delay of unreliable sensing is due to additional delay from P_{md} and P_{fa}. In both scenarios, the higher mean packet delay is because of the increasing values of P_e. Increase in P_e results in re-transmissions, whereas, an increase in P_b values reduces the chances of transmission for an MN. Moreover, the simulation results and analytical findings obtained from Eq. (29) match with each other as illustrated in Fig. 9b.

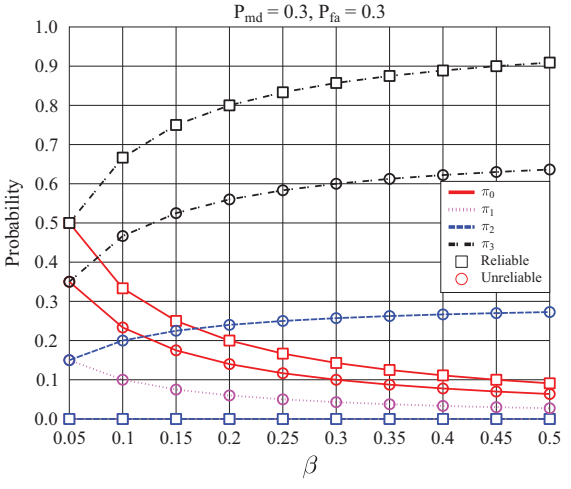


(a) The Handshake Duration

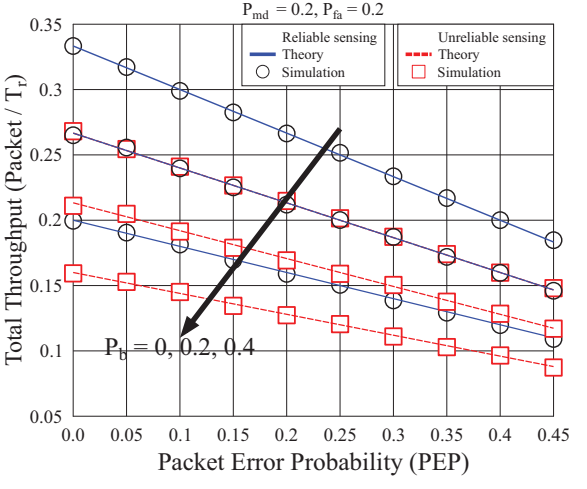


(b) The Response Time at one Byte data

Fig. 7. Handshake duration and response time.

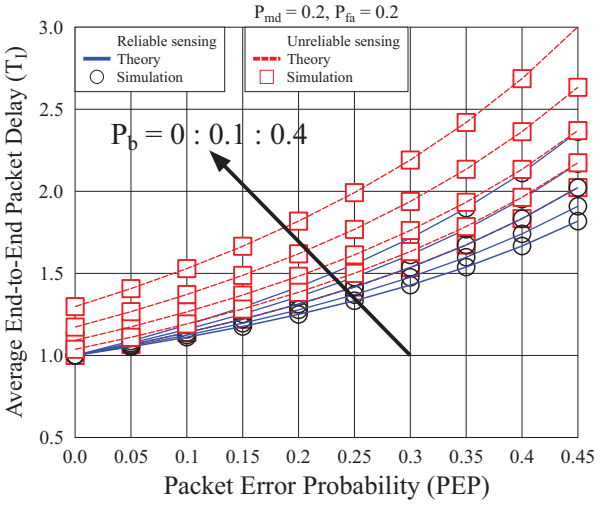


(a) Steady-state probabilities of $[\pi_0; \pi_1; \pi_2; \pi_3]$ seen in ((20) & (21)) with respect to β.

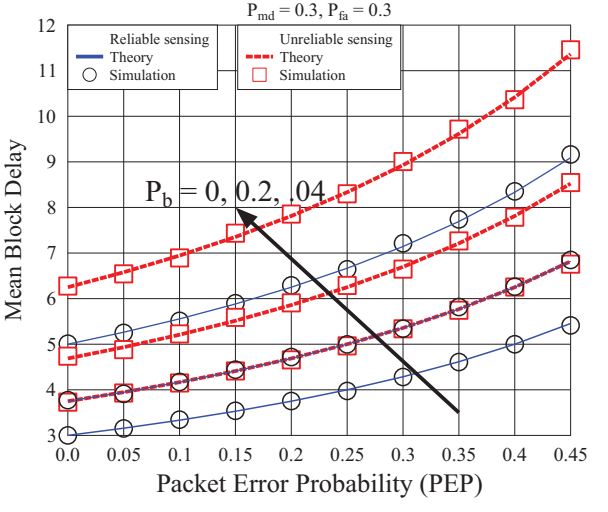


(b) Throughput against P_e, of the SRC-HARQ scheme in terms of various P_b, where $T_p = 1$ and $W_p = 1$ seconds. Average throughput performance is examined for different values of P_e, where results are calculated in terms of T_p.

Fig. 8. Steady-state probabilities and throughout against P_e, for various values of P_b.

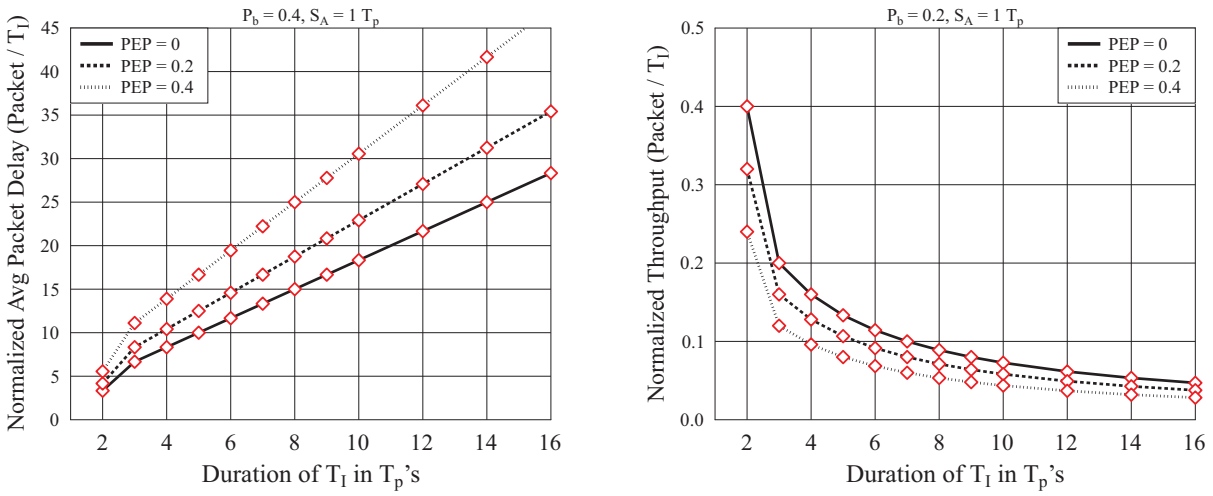


(a) Average E2E delay in reliable sensing scenario and unreliable sensing scenario with ($P_{fa} = 0.2$, $P_{md} = 0.2$) environment for $P_b = \{0, 0.4\}$ and $P_e = \{0.1, 0.4\}$.



(b) Average mean delay of the SRC-HARQ scheme for $P_{md} = 0.3$ and $P_{fa} = 0.3$.

Fig. 9. Average and block delay for different values of P_{md} and P_{fa} against P_e.



(a) Delay with respect to different T_Ps (b) Throughput with respect to different T_Ps

Fig. 10. Delay and throughput with respect to different T_Ps.

The E2E packet delay of SRC-HARQ scheme for reliable and unreliable sensing is shown in Fig. 9a. The E2E delay may be computed as,

$$E2E = \frac{\mathbb{F}_{\mathbb{T}} - \mathbb{F}_{\mathbb{R}}}{N_S}. \tag{30}$$

where $\mathbb{F}_{\mathbb{T}}$ is the time of first transmission, $\mathbb{F}_{\mathbb{R}}$ is the time of final reception, and N_s is the total number of packets. To mathematically model the E2E delay, let a vector $\boldsymbol{w}$ of size N_s is assumed for storing the delay experienced by each packet from its first transmission attempt to its final successful reception. For example, the $\boldsymbol{w}(k)$ symbolizes the E2E delay of a kth packet, and the PMF (P_{dist}) of E2E delay depicted in Fig. 9a, can be computed as follow,

$$\boldsymbol{P}_d(m) = \frac{\sum_{k=1}^{N_s}, \delta \times (\boldsymbol{w}(i) - m)}{N_s}, \text{ where } \quad 1 \leq m \leq \max(\boldsymbol{w}). \tag{31}$$

The δ function in Eq. (31) finds total T_ps taken by a packet. For instance, if 200, 160, 120 packets are successfully recieved in 1, 2, and 3 T_ps respectively; then the distribution may be written as $\boldsymbol{P}_d(m) = [200/N_s,\ 160/N_s,\ 120/N_s,\ \ldots]$.

The E2E delay for reliable sensing and unreliable sensing is represented in Fig. 9a. It is obvious from Fig. 9a, that for unreliable sensing, i.e., when $P_{fa} = 0.2$ and $P_{md} = 0.2$, 84% data packets are successfully transmitted with an E2E delay of one T_I for $P_e = 0.1$. Furthermore, 8.8% packets are successfully transmitted with an E2E delay of two T_Is, and 3.7% packets take an E2E delay of three T_Is, as presented in Fig. 9a. In comparison, for reliable sensing, i.e., when $P_{fa} = 0$, and $P_{md} = 0$, 90% packets are successfully transmitted with an E2E delay of one T_I, 7.2% packets are successfully transmitted with an E2E delay of two T_Is, the number of packets with an E2E delay of 3 T_Is is decreased to 2% only, for $P_e = 0.1$. Similarly, for P_e=0.4, the E2E delay of one T_I is 54% for unreliable sensing and 60% for reliable sensing.

Moreover, T_I of different T_ps (2T_ps to 16 T_ps) are used, and the effect of this increase is illustrated in Fig. 10a and b. When the number of T_ps increases, the delay is higher because after transmitting a packet the remaining T_ps go wasted due to the stop-and-wait nature of the proposed scheme. Similarly, in Fig. 10b, the increase in the number of T_ps causes low throughput because the MN waits for the feedback from the CH which is received at the end of a T_I.

7. Conclusion

In this paper, the performance of SRC-HARQ scheme for both reliable and unreliable sensing in a smart city application is evaluated. By evaluating the 4-state Markov Chain and the use of a probabilistic approach, closed-form expressions for steady states and performance metrics are obtained, which are then verified through simulation. One hundred thousands Monte Carlo simulations are performed to achieve the performance metrics of throughput, mean packet delay, and E2E mean delay. The performance results show that throughput and delay of the SRC-HARQ scheme are significantly affected by the quality of channel (P_e), channel availability (P_b), and/or CH sensing. As a result, when the channel is free from the PU, the throughput is higher and delay is lower, and vice versa. Similarly, when the sensing process is reliable, then the proposed system performs exceptionally well. Therefore, it is essential to investigate the optimal values of these metrics to achieve better results. It will be interesting to assess the performance of SRC-HARQ by transmitting several packets in a time-slot to reduce the waiting time.

Declaration of Competing Interest

The authors declare no conflict of interest.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2019.106502.

References

[1] Babar M, Khan F, Iqbal W, Yahya A, Arif F, Tan Z, et al. A secured data management scheme for smart societies in industrial internet of things environment. IEEE Access 2018;6:43088–99. doi:10.1109/ACCESS.2018.2861421.
[2] Akhtar F, Rehmani MH, Reisslein M. White space: definitional perspectives and their role in exploiting spectrum opportunities. Telecomm Policy 2016;40(4):319–31.
[3] IEEE recommended practice for information technology-telecommunications and information exchange between systems wireless regional area networks (WRAN)-specific requirements-part 22.2: Installation and deployment of IEEE 802.22 systems. IEEE; 2012. p. 1–44. Std 802222-2012
[4] Zaheer K, Othman M, Rehmani MH, Perumal T. A survey of decision-theoretic models for cognitive internet of things (ciot). IEEE Access 2018;6:22489–512.
[5] Rehman AU, Thomas VA, Yang LL, Hanzo L. Performance of cognitive selective-repeat hybrid automatic repeat request. IEEE Access 2016;4:9828–46.
[6] Khan F, Nakagawa K. Comparative study of spectrum sensing techniques in cognitive radio networks. In: World congress on computer and information technology (WCCIT), 2013; 2013. p. 1–8.
[7] Ta D-T, Nguyen-Thanh N, Maillé P, Nguyen V-T. Strategic surveillance against primary user emulation attacks in cognitive radio networks. IEEE Trans Cognit Commun Networking 2018;4(3):582–96.
[8] Liang W, Nguyen HV, Ng SX, Hanzo L. Adaptive-TTCM-aided near-instantaneously adaptive dynamic network coding for cooperative cognitive radio networks. IEEE Trans Veh Technol 2016;65(3):1314–25.
[9] Jain S, Hussain M, Garimella RM. Primary user authentication in cognitive radio network using authentication tag. In: Recent advances and innovations in engineering (ICRAIE), 2016 international conference on. IEEE; 2016. p. 1–5.
[10] Salameh HAB, Almajali S, Ayyash M, Elgala H. Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks. IEEE Internet Things J 2018;5(3):1904–13.
[11] Qian Y, Chen M, Chen J, Hossain MS, Alamri A. Secure enforcement in cognitive internet of vehicles. IEEE Internet Things J 2018;5(2):1242–50.
[12] Zhu J, Song Y, Jiang D, Song H. A new deep-q-learning-based transmission scheduling mechanism for the cognitive internet of things. IEEE Internet Things J 2018;5(4):2375–85.
[13] Song H, Fink GA, Jeschke S. Security and privacy in cyber-physical systems: foundations, principles, and applications. John Wiley & Sons; 2017.
[14] Azmat F, Chen Y, Stocks N. Analysis of spectrum occupancy using machine learning algorithms. IEEE Trans Veh Technol 2016;65(9):6853–60.
[15] Eltom H, Kandeepan S, Liang Y-C, Evans RJ. Cooperative soft fusion for hmm-based spectrum occupancy prediction. IEEE Commun Lett 2018;22(10):2144–7.
[16] Liu B, Li Z, Si J, Zhou F. Optimal sensing interval in cognitive radio networks with imperfect spectrum sensing. IET Commun 2016;10(2):189–98.
[17] Rehman AU, Yang L-L, Hanzo L. Performance of cognitive hybrid automatic repeat request: Go-back-n. In: 2016 IEEE 83rd vehicular technology conference (VTC Spring). IEEE; 2016. p. 1–5.
[18] Khan F, Ur Rehman A, Usman M, Tan Z, Puthal D. Performance of cognitive radio sensor networks using hybrid automatic repeat request: stop-and-wait. Mob Netw Appl 2018;23:479–88.
[19] Horn RA, Johnson CR. Matrix analysis. Cambridge University press; 2012.
[20] Mitchell G. Investigation of hamming, reed-solomon, and turbo fec codes. Tech. Rep. DTIC Document; 2009.
[21] Jan MA, Khan F, Alam M, Usman M. A payload-based mutual authentication scheme for internet of things. Future Gen Comput Syst 2019;92:1028–39.

Fazlullah Khan is an Assistant Professor in Abdul Wali Khan University Mardan, Pakistan. He got gold medal in B.S. degree and completed higher studies from Japan on MEXT scholarship. His research interests are security, privacy, and performance analysis of adhoc networks. He has published more than 10 papers in IEEE and ACM/Springer journals, with two edited books to his name.

Ateeq ur Rehman is an Assistant Professor at the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. He obtained Ph.D. from Southampton University, UK. He is currently working in IoT, cognitive radio, 5G, and adhoc networks.

Mian Ahmad Jan is an Assistant Professor at the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. He got Ph.D. degree from University of Technology Sydney, Australia. His research interests include security, privacy and energy-efficient routing in Internet of Things. He has published his research work in various IEEE Transactions and Elsevier Journals.