Improved Model for Transmission and Interference Ranges

Arash T. Toyserkani, Erik G. Ström and Arne Svensson

Communication Systems Group
Department of Signals and Systems
Chalmers University of Technology
Göteborg 2007
Abstract

Transmission range ($R_{tx}$), carrier sensing range ($R_{cs}$), and interference range ($R_i$) are three important radio ranges in wireless networks. These parameters are defined in [1] and the authors proposed the first analytical model for the interference range based on which new protocols has been proposed [2–5]. In this paper, we improve on this model by relaxing some of the simplifying assumptions. A new formula for interference range is derived, where noise is not ignored as it was done in [1]. Our formula shows that interference range obtained by ignoring the noise is a good approximation, only for receivers close to the transmitter. While for receivers closer to the transmission range, which suffer from hidden terminal problem, ignoring the noise results in substantially underestimating the interference range.

We also study the effect of physical layer parameters on $R_{tx}$ and $R_i$, by introducing more general definitions for these ranges. Our study indicates that both $R_{tx}$ and $R_i$ are influenced by variations in packet size, modulation, and coding. This implies that RTS/CTS packets may have a different $R_{tx}$ and $R_i$ compared to data packets. Thus, we expect the performance analysis based on the assumption of similar $R_{tx}$ and $R_i$ for RTS/CTS and data packets, to be inaccurate.

Moreover, effects of small-scale fading on $R_{tx}$ and $R_i$ for the case where fading value is constant during a packet investigated. Our case study indicates that Rayleigh fading has a negative effects on both $R_{tx}$ and $R_i$. 
1 Introduction

Carrier Sense Multiple Access (CSMA) is a well-known family of MAC protocols, well-suited for a wireless ad-hoc network. In CSMA protocols, nodes are required to sense the channel prior to transmission. Packet collision is avoided by deferring a transmission whenever the channel is sensed busy. The channel sensing procedure, however, fails for the nodes located outside the carrier sensing range, $R_{cs}$, from the transmitter but close enough to the receiver to interfere with the current packet reception. These nodes are known as hidden terminals [6]. In the presence of hidden terminals, advantages of carrier sensing fade away and throughput of CSMA approaches the throughput of the ALOHA protocol [6].

Numerous protocols have been proposed to combat the hidden terminal problem [6–8]. While these protocols apply different methods, they all strive to compensate the lack of carrier sensing of the hidden terminals. Hence, for these protocols to work efficiently, knowledge of where the hidden nodes are located is crucial. For instance, in the dual busy tone multiple access (DBTMA) protocol [8], the receiver’s busy tone range must be set very cautiously. Unnecessarily powerful busy tone results in a lower network throughput and power efficiency, while a short busy tone fails to stop all the hidden terminals from interfering.

The common assumption in the above-mentioned papers is that hidden terminals are at most located the transmission range away from the receiver. That is, the interference range is constant and equal to the transmission range, regardless of the transmitter-receiver distance ($d_{tx}$). However, as it is shown in [1], the interference range is an increasing function of $d_{tx}$. All the above protocols therefore fail in solving the hidden terminals for the nodes having an interference range larger than transmission range. To the best of our knowledge, the first analytical model proposed to calculate the interference range as a function of $d_{tx}$ and capture threshold is introduced in [1]. The authors of [1] define the transmission and interference ranges as follows:

- **Transmission range** ($R_{tx}$): a range within which a packet is successfully received if there is no interference from other radios.

- **Interference range** ($R_{i}$): a range around a receiver within which an unrelated transmission causes a packet drop.

To obtain the interference range, authors explicitly or implicitly made the following assumptions:
- Packets are received successfully with probability 1 if the signal to noise and interference ratio (SINR) is larger than the capture threshold.
- Multi-path and shadow fading is ignored.
- Path loss is modelled by the two-way ground model.
- Noise is ignored in comparison to the interference.
- Data and interferer packets are completely overlapping, meaning that the SINR is constant during the packet.
- Multiple packet collisions are ignored meaning that this model is only valid for a low and medium network traffic.

Under these assumptions, the interference range was found to be 1.78 times transmitter-receiver distance for 10 dB capture threshold [1]. As a result, the authors show that the interference range becomes larger than the transmission range for the receivers located further than 0.56\(R_{tx}\) away from the transmitter. It was also shown that RTC/CTS fails to prevent all the hidden terminals from interfering, when the interference range is larger than transmission range.

Recently, several authors [2–5] used this model for the interference range. Combining the above interference range model with RTS/CTS handshake in [2], the authors recognize three different medium reservation scenarios, namely underactive, moderate, and overactive. A receiver in the overactive scenario has a noticeably shorter interference range compared to the transmission range. As a result, the RTS/CTS handshake blocks a larger area than required, causing a reduction in the network reuse. An aggressive virtual carrier sensing (AVCS) is proposed in which channel is regarded as busy if both RTS and CTS packets are received, i.e., a node that receives either a RTS or CTS is allowed to initiate a new transmission. This scheme is shown to increase the spatial reuse and throughput. The opposite problem, interference range larger than transmission range, occurs in the underactive case. In this scenario, the RTS/CTS handshake fails to cover all the interference area. To address this problem, the IEEE 802.11 MAC is fused with DBTMA protocol in [3]. A busy tone is used to block the hidden nodes which are out of range of the RTS/CTS handshake. In [4], the same problem is addressed by adjusting the contention window such that the probability of collision from hidden terminals become negligible. In [5], the carrier sensing range is tuned to block the hidden terminals. The above model is only used in this paper to analyze the effect of different carrier sensing ranges.
In this work, we aim at providing a more realistic model for the transmission and interference ranges by relaxing some of the above assumptions. In Section 2, new definitions for transmission and interference ranges are proposed by slightly modifying the definitions in [1]. In Section 3, we show that ignoring noise when calculating the interference range, results in underestimating the interference range, especially for the receivers close to the transmission range. As a result, we argue that protocols using the interference range model introduced in [1], may not achieve their predicted performance.

Effects of physical layer parameters on the transmission and interference ranges are discussed in Section 4. Based on our findings in this section, we argue that RTS/CTS packets generally have a larger transmission range and shorter interference range compared to data packets. To best of our knowledge, this property of RTS/CTS packets has not been considered in the performance analysis of previous protocols based on this handshake. We further show that in the systems with multi-rate physical layers (e.g., IEEE 802.11b) a cross layer design is crucial for the correct performance of the MAC protocol.

In Section 5, we relax the assumption of full overlap between the data packet and the interferer packet as this is an impossible event (zero probability). We show that the interference range is an increasing function of overlap and its variations as a function of overlap are not negligible.

In Section 6, the effect of small-scale fading on transmission and interference ranges for the case of constant fading during the packet is analyzed. The results of this section is therefore only valid when the packet transmission time is smaller than the channel coherence time.

2 New definitions for transmission and interference ranges

In the transmission and interference ranges definitions offered in [1], a packet is received successfully with probability one if the received SINR is above the capture threshold. This is clearly not true in practice. For a given set of physical layer parameters, we will instead assume that the probability of successful reception ($P_s$) of a packet is a function of the SINR during its reception which would be the case if the interference can be modelled as additive Gaussian noise. To take this randomness into account, we modify the above definitions of the transmission and interference ranges as follows:
**Transmission range** ($R_{tx}$): a range within which $P_s$ is above the required threshold ($\mu$) in absence of any interference from other radios. Formally

$$R_{tx} = \max\{d_{tx} : P_s \geq \mu | I = 0\}$$

where $I$ is the interference power. For cases where the SINR can be considered constant during the packet reception, the threshold SINR ($\Theta_{\text{SINR}}$) can be defined as the SINR ($\Gamma$) at which $P_s$ is equal to $\mu$. Then (1) can be simplified to

$$R_{tx} = \max\{d_{tx} : \Gamma \geq \Theta_{\text{SINR}} | I = 0\}$$

which is equivalent to the transmission range definition in [1].

**Interference range** ($R_i$): a range around the receiver within which a single, interfering transmission is enough to result in $P_s$ less than $\mu$. That is, if $d_i$ is the distance between the receiver and the interfering transmitter, then

$$R_i = \max\{d_i : P_s \leq \mu\}$$

If the received SINR is constant during the packet reception and for a given packet length, modulation, and coding, $\Theta_{\text{SINR}}$ can be found such that $P_s$ is equal to $\mu$. Hence, $R_i$ can be expressed as

$$R_i = \max\{d_i : \Gamma \leq \Theta_{\text{SINR}}\}$$

which is the definition used in [1].

As we show in Sections 4-6, using the range definitions given by (1) and (3) instead of (2) and (4), allows us to analyze the effect of physical layer parameters or non-constant received SINR (due to fading or partial collisions), on the transmission and interference ranges.

### 3 Effect of noise on interference range

For given propagation model parameters and in the absence of fading, the received power ($P_r$) at the receiver as a function of transmitter-receiver distance ($d_{tx}$), and transmitted power ($P_{tx}$) can often be modelled as

$$P_r = \frac{CP_{tx}}{d_{tx}^\alpha}$$

where $\alpha$ is the path loss exponent and $C$ is a constant which takes into account other physical parameters such as antenna gains. In
the absence of any interference, the SINR ($\Gamma$) at the receiver is constant and is given by

$$\Gamma = \frac{CP_{tx}}{d_{tx}^\alpha P_N}$$

(6)

where $P_N$ is the noise power. Hence, the transmission range can be found as

$$\Gamma = \Theta_{\text{SINR}} \Rightarrow R_{tx} = \sqrt[\alpha]{\frac{CP_{tx}}{P_N\Theta_{\text{SINR}}}}$$

(7)

To obtain the interference range, we assume, in this section, that all the nodes transmit at the same power level and an interferer packet is fully overlapping with the data packet. If the noise power is ignored, as in [1–4], the SINR at the receiver in case of single packet collision is simply given by

$$\Gamma = \frac{d_i^\alpha}{d_{tx}^\alpha}$$

(8)

where $d_i$ is the interferer-receiver distance. Consequently, the interference range can be estimated as

$$r_i = d_{tx} \sqrt[\alpha]{\Theta_{\text{SINR}}}$$

(9)

where $r_i$ is the interference range estimate without noise consideration, which is similar to the interference range formula used in [1–4]. Now considering the noise, the $\Gamma$ at the receiver in presence of single interferer is given by

$$\Gamma = \frac{Cd_{tx}^\alpha P_{tx}}{Cd_i^{-\alpha} P_{tx} + P_N}$$

(10)

By combining (7), (9), and (10), the exact interference range, $R_i$, can be found as

$$R_i = \frac{r_i}{\sqrt[\alpha]{1 - \left(\frac{d_i}{R_{tx}}\right)^\alpha}}$$

(11)

The difference between $R_i$ and $r_i$ is an extra term in the denominator. We define the relative approximation error in $r_i$ as

$$E_r = \frac{R_i - r_i}{R_i}$$

(12)

Fig. 1 shows $E_r$ as a function of $d_{tx}/R_{tx}$ for different path loss exponents. Keep in mind that the transmission range is different for different path loss exponents.

As it can be seen from Fig. 1, the interference range without noise consideration is a good approximation of the correct interference range only for $d_{tx}$ less than, e.g., 20% of the transmission range. As $d_{tx}$ gets closer to the transmission range, the error grows
Figure 1: The relative approximation error in \( r_i, E_r \), for different path loss exponents.

Figure 2: Hidden nodes are located in the \( A_h \). The transmitter and receiver are denoted by \( tx \) and \( rx \), respectively.

increasingly fast. The \( E_r \) is also larger for a smaller path loss exponent.

Nevertheless, incorrect knowledge of the interference range, results in deficient operation of hidden terminal avoidance methods like RTS/CTS or busy tone. To elaborate more on this point, let us consider an ad-hoc network where nodes are uniformly distributed in an area. As mentioned before, hidden terminals are nodes located outside the carrier sensing range of a transmitter but in the interference range of a receiver. This corresponds to the area \( A_h \) in
3 Effect of noise on interference range

Fig. 2. Assuming uniformly distributed nodes, the average number of nodes in an area is proportional to the area. The average number of hidden nodes is given by

\[ n_h = d_n A_h \]  

(13)

where \( d_n \) is the node density. A larger \( A_h \) results in higher average number of hidden terminals and consequently, a higher risk of packet collision caused by them.

Fig. 3 demonstrates \( A_h \) as a function of \( d_{tx}/R_{tx} \) for carrier sensing ranges of \( 1.5R_{tx} \) and \( 2R_{tx} \). It is evident from this figure that there are no hidden terminals for a receiver close to the transmitter, as all the nodes in its interference range are able to detect the ongoing reception.

![Figure 3: \( A_h \) as a function of \( d_{tx}/R_{tx} \) for \( r_i \) and \( R_i \) with two different \( R_{cs} \).](image)

Values of \( d_{tx} \) at which \( A_h \) becomes non-zero for different \( R_{cs} \) and \( \alpha \) are shown in Table 1.

<table>
<thead>
<tr>
<th>( R_{cs} )</th>
<th>( \alpha = 3 )</th>
<th>( \alpha = 4 )</th>
<th>( \alpha = 5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1.5 R_{tx} )</td>
<td>0.47</td>
<td>0.53</td>
<td>0.58</td>
</tr>
<tr>
<td>( 2 R_{tx} )</td>
<td>0.60</td>
<td>0.69</td>
<td>0.75</td>
</tr>
</tbody>
</table>

Comparing Table 1 with Fig. 1, we can see that the interference range without noise considerations is indeed inaccurate for the range of \( d_{tx} \) within which, a receiver would suffer from the hidden
terminal problem (non-zero $A_h$). As a result adjusting busy tone range in protocols like DBTMA [8], FPDBT [3], or VPDBT [3] according to the interference range without considering noise, would not succeed in resolving the hidden terminal problem.

To verify our model, a simulation experiment is performed in OPNET Modeler [9]. An ideal MAC protocol is assumed such that a receiver always successfully blocks all the nodes inside a range $R$ from the receiver. As a result, all the nodes inside the range $R$ of the receiver can be ignored. To simulate a single, fully overlapped packet collision, a constantly transmitting interferer is located outside the range $R$. The topology of this simulation experiment is shown in Fig. 4.

![Topology of simulation experiment](image)

**Figure 4:** Topology of simulation experiment.

The result of this simulation experiment is demonstrated in Fig. 5. Every simulation point is an average of 5 different simulation runs of approximately 30,000 packet transmissions. As we predicted, for $R = r_i$, the target success rate is missed as $d_{tx}$ approaches the transmission range. On the contrary, it is achieved within the simulation accuracy when $R = R_i$.

4 **Effect of physical layer parameters on transmission and interference ranges**

In this section, we analyze the effect of packet length, modulation, and coding on the transmission and interference range. We ignore fading and assume that all the nodes transmit at a same transmit
Effect of physical layer parameters on transmission and interference ranges

Figure 5: The probability of successful reception, \( P_s \), for interference range with and without noise consideration. The success threshold, \( \mu \), is 0.99.

For given packet length and modulation, the exact formula for \( P_s \) depends on the coding and decoding method used. For the sake of simplicity in this paper, we assume that perfect block codes decoded using hard-decision, maximum likelihood (ML) decoding are used. While we are aware that perfect block codes do not exist for all considered code rates and number of correctable errors, for simplicity we ignore this fact. This assumption allows us to derive \( P_s \) as

\[
P_s = \sum_{i=0}^{\tau} \binom{N}{i} P_b^i (1 - P_b)^{N-i}
\]

where \( \tau \) is the number of correctable errors, \( N \) is the packet length, and \( P_b \) is the coded bit error probability. The effect of the modulation on \( P_s \) is represented by \( P_b \). Hence, any change in the packet size, coding, or modulation results in different required SINR.

These variations in SINR can be translated to variations in transmission range as

\[
\Phi = \frac{R_{tx}(2)}{R_{tx}(1)} = \sqrt[\Delta]{\frac{\Theta_{\text{SINR}}(1)}{\Theta_{\text{SINR}}(2)}} = 10^{\frac{\Delta}{10}}
\]

where \( \Phi \) is the ratio of transmission ranges and \( \Delta \) is the variations of \( \Theta_{\text{SINR}} \) in dB and is defined as

\[
\Delta = \Theta_{\text{SINR}}(2)[dB] - \Theta_{\text{SINR}}(1)[dB]
\]

Fig. 6 shows \( \Phi \) as a function of \( \Delta \) for three different \( \alpha \). As expected, the reduction in the required SINR to achieve \( \mu \) results in a longer transmission range.
To demonstrate that variations in the transmission range are indeed noteworthy, we consider four different scenarios where a 100 byte or 1 Kbyte packet is transmitted using BPSK or 16-QAM. The packet is assumed to be coded using a $\tau$-error correcting perfect block code. The coded bits are then mapped to modulation constellation using a Gray code. Fig. 7 demonstrates the variations in $\Theta_{\text{SINR}}$ and $\Phi$ as a function of $\Delta$, for $\mu = 0.99$. To calculate $\Phi$, $R_{tx}(1)$ is assumed to be the transmission range in case of 1 Kbyte packet with 16-QAM modulation and no coding. It can be observed from these figures that the transmission range can be considerably influenced by changing the packet length, modulation, or coding.

It can also be seen from these figures that while a stronger code increases the transmission range, this gain saturates as $\tau$ increases. Additionally, it is evident from these figures that packet length and modulation have a big impact on the transmission range. For instance, the transmission range can be increased by 20% if a BPSK modulation is used instead of 16-QAM to transmit a 100 byte packet with 10 bit error correction.

One important conclusion of this observation is that RTS, CTS, and data packets experience different transmission range. According to the 802.11 standard [10], the RTS packet is 44 byte and CTS or ACK packets are 38 bytes. In most practical applications, however, data packets are in the order of several hundreds of bytes. As a result, the RTS/CTS/ACK packets are expected to have different (mainly larger) transmission ranges compared to the data packet. For example, an RTS packet transmitted using BPSK with no error correction has about 12% larger transmission range compared to a
1Kbyte packet transmitted using 16-QAM with $\tau = 10$ code. To the best of our knowledge, this difference between the transmission ranges of RTS/CTS/ACK packets and data packets has never been considered in evaluations of protocols based on RTS/CTS/ACK handshake.

To observe the impact of physical layer parameters on the interference range, (11) is rearranged as

$$R_i = \frac{K}{\sqrt{\left(\frac{B_{tx}}{4}\right)^\alpha - 1}}$$

where $K = \sqrt{\frac{CP}{P_N}}$. In the absence of power control and fading, $K$ is constant. In this case, a larger transmission range results in shorter interference range.

To demonstrate the effect of packet size, modulation, and coding on the interference range, we consider two cases. In the first case,
we consider a 100 byte packet transmitted using BPSK modulation with a block code capable of 10 bit error correction. In the second case, a 1000 byte packet is transmitted using 16-QAM with no error correction capability. In both cases, $\mu$ is 99 percent. The resulting interference range as a function of $d_{tx}/R_{tx}$ is demonstrated in Fig. 8. The vertical dotted lines in each case represent the transmission ranges for the corresponding case.

![Graph](image)

**Figure 8:** The interference range as a function of $d_{tx}$ for case 1 (BPSK, 100 byte packets, $\tau = 10$) and case 2 (16-QAM, 1000 byte packets, no error correction).

It can be seen from this figure that the interference range is also affected by variations in packet length, modulation, and coding. Consequently, it is expected that RTS/CTS packets also experience different interference ranges compared to the data packet. Thus, assuming similar ranges for the RTS/CTS and data packet, results in inaccurate analysis of the MAC performance.

As we demonstrated above, the transmission and interference ranges are significantly influenced by the variations in packet length, modulation or coding. This observation opens up a new door for designing an intelligent MAC protocols that combines a classical hidden terminal avoidance methods (like RTS/CTS or busy tone) with an appropriate choice of physical layer parameters and even position information to mitigate the hidden terminal problem more efficiently. As an example, we consider the scenario in Fig. 9 where node A transmits a 1 Kbyte packet to node B with required successful delivery of 99%. Assume that topology information is available to node A. If the packet is transmitted using 16-QAM modulation, the interference range is $R_2$. As a result nodes C and D are located...
inside the interference range and can potentially create a collision. On the other hand, if BPSK modulation is used instead, the interference range can be reduced to $R_1$ and the hidden terminal problem is solved.

![Figure 9: Hidden terminal avoidance by modifying the modulation parameters.](image)

Another interesting conclusion is that in systems with multi-rate physical layers (e.g., IEEE 802.11b), where the data rate is changed by modifying the modulation and/or coding, these ranges are also varying depending on the data rate. Since MAC protocols can only perform correctly if they are aware of correct ranges, cross-layer interaction between the physical layer and the MAC layer seems necessary.

5 Interference range variation with the overlap percentage

In the interference range calculation, it was assumed that the interfering packet is completely overlapping with the data packet. In reality, however, there is a zero probability that data and interference packets completely overlap, and the data packet is therefore always only partially corrupted by an interferer packet. Note that in our assumptions, multiple packet collisions are ignored.

Intuitively it is conceivable that if a portion of a packet is col-
Collision free, the rest of the packet can endure higher interference level compared to the case of a fully overlapping collision. Thus, it is expected that the interference range shrinks when there is less overlap between the data and interference packet. Therefore, the interference range obtained in case of complete overlap is an upper bound to the interference range.

For a partially collided data packet, the SINR in the collision free part \((\Gamma)\) and collided part \((\Gamma_C)\) of the packet is given by (6) and (10) respectively. We can rewrite (10) as

\[
\Gamma_C = \frac{1}{(\frac{d_{tx}}{d_{tx}})^\alpha + \Gamma}
\]  

(18)

In a partially collided packet, there are two SINRs, and consequently, two bit error rates. To calculate \(P_s\) for a packet with variable bit error rates, we use a similar method as in [11]. We define \(P(m, n)\) as the probability of having \(m\) errors out of \(n\) coded bits. Then \(P(m, n)\) can be recursively written as

\[
P(0, 0) = 1
\]

\[
P(0, n) = \prod_{i=1}^{n}(1 - P_b(i))
\]

\[
P(m, n) = 0 \text{ for } m > n
\]

\[
P(m, n) = (1 - P_b(n))P(m, n - 1) + P_b(n)P(m - 1, n - 1)
\]

where \(P_b(n)\) is the bit error rate at bit \(n\). Using \(P(m, n)\), \(P_s\) for a perfect block code with \(\tau\) error correction capability is given by

\[
P_s = \sum_{m=0}^{\tau} P(m, N)
\]  

(19)

where \(N\) is the packet size. The bit error rate of each bit can be found knowing the modulation and SINR. Depending on whether the bit is in the collision or collision-free part of the packet, the SINR of the bit is given by \(\Gamma_C\) or \(\Gamma\). If \(\Gamma\) and \(\Gamma_C\) can be found such that \(P_s\) is equal to \(\mu\), the interference range, using (18), can be determined as follows

\[
R_i = d_{tx} \sqrt[\alpha]{\frac{\Gamma_C^{\Gamma}}{\Gamma - \Gamma_C}}
\]  

(20)

Thus, the following procedure is employed to obtain \(R_i\):

1. \(\Gamma\) is determined according to (6).

2. The bit error rate of collision-free part of the packet is calculated using \(\Gamma\) and the modulation method.
3. By numerical methods and for a given packet length and coding, the maximum bit error rate of the collided part of the packet is determined such that $P_s = \mu$.

4. Knowing the modulation method, this bit error rate is translated back to $\Gamma_C$.

5. $R_i$ is determined using (20)

As an example, we consider a receiver node located at $d_{tx} = 0.9R_{tx}$.

The interference range as a function of overlap percentage in three different scenarios were obtained and are shown in Fig. 10. The different parameters used in these scenarios are shown in Table 2.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Packet length</th>
<th>Modulation</th>
<th>$\tau$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1000 Bytes</td>
<td>16-QAM</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1000 Bytes</td>
<td>BPSK</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>100 Bytes</td>
<td>BPSK</td>
<td>10</td>
</tr>
</tbody>
</table>

In Fig. 10, for each curve, the interference range is normalized by its maximum interference range (full overlap). It can be seen from this figure that as expected, the interference range indeed grows as a function of the overlap percentage. Additionally, these variations are not negligible and assuming a full overlap results in a pessimistic interference range calculation. It also appears that the interference range is more sensitive to the amount of overlap when each bit in the packet is more strongly protected.

Receiver busy tone in DBTMA [8] or other similar protocols can be adjusted more efficiently based on this observation. Receivers send out a busy tone in the beginning of reception to block all the hidden nodes according to the maximum interference range. The busy tone range can be reduced if no collision is detected after some portion of packet is received. This reduction in busy tone range, may result in a better spectral reuse, throughput and power efficiency.

6 Small-scale fading

The effect of small-scale fading on the transmission and interference range is considered in this section. We focus our attention to the case where the fading value is constant during the packet reception,
i.e., the packet transmission time is smaller than the coherence time of the channel. With this assumption and in the absence of interference, the SNR and consequently bit error rate is constant during the packet reception, while it randomly varies from one packet to another. A packet’s SNR for a receiver at $d_{tx}$ is given by

$$\Gamma = \frac{\kappa_{tx} CP_{tx}}{d_{tx}^2 P_N}$$  \hspace{1cm} (21)$$

where $\kappa_{tx}$ is a random variable accounting for the effect of the small-scale fading on the SNR.

As given in (14), the probability of successful reception of a packet for a given SNR, $\Gamma$, assuming hard-decision, ML decoding of a perfect block code is given by

$$P_k(\Gamma) = \sum_{i=0}^{\infty} P_b(\Gamma)^i(1 - P_b(\Gamma))^{N-i}$$  \hspace{1cm} (22)$$

where $P_b(\Gamma)$ is the bit error rate. Using (22), $P_s$ can be obtained by averaging over the probability distribution function (pdf) of $\Gamma$, $f_\Gamma(\Gamma)$, as

$$P_s = \int_0^\infty P_k(x)f_\Gamma(x)dx$$  \hspace{1cm} (23)$$

As an example, $\Gamma$ in a Rayleigh fading channel is exponentially distributed and its pdf is given by

$$f_\Gamma(x) = \frac{\exp^{-x/\gamma}}{\gamma}$$  \hspace{1cm} (24)$$

where $\gamma = \frac{CP_{tx}}{d_{tx}^2 P_N}$ is the average SNR. Combining (23) with transmission range definition in (1), $R_{tx}$ is obtained by finding $d_{tx}$ such that $P_s$ is $\mu$. 

![Figure 10: Normalized interference range as a function of overlap percentage for three different scenarios.](image)
For the sake of simplicity, here we assume a full overlap between the interferer packet and the data packet. To find the interference range for the partial overlap case, a similar procedure as in Sec. 5 should be employed. Using a full overlap assumption, a packet’s SINR becomes constant and $a$ can be written as

$$
\Gamma = \frac{\kappa_{tx} CP_{tx} d_{tx}^{-\alpha}}{\kappa_i CP_{tx} d_i^{-\alpha} + PN}
$$

(25)

where $\kappa_{tx}$ and $\kappa_i$ are random variables corresponding to the power gain of the fading channel for the transmitter-receiver and interferer-receiver pairs, respectively. In the Rayleigh fading channel, $\kappa_{tx}$ and $\kappa_i$ are exponentially distributed. Similarly, $P_s$ can be found by

$$
P_s = \int_{0}^{\infty} P_k(x)f(x)dx
$$

(26)

Instead of deriving the pdf for $\Gamma$, the integration can be performed over the pdfs of $\kappa_{tx}$ and $\kappa_i$ which are assumed to be independent random variables. Thus (26) can be rewritten as

$$
P_s = \int_{0}^{\infty} \int_{0}^{\infty} P_k(\kappa_1, \kappa_2)f(\kappa_1)f(\kappa_2)d\kappa_1d\kappa_2
$$

(27)

The interference range for a node at $d_{tx}$ is obtained by finding $d_i$ such that $P_s$ is equal to $\mu$.

Figure 11: The effect of Rayleigh fading channel on $R_{tx}$ and $R_i$.

As an example, we consider a packet of 100 bytes transmitted using BPSK modulation over both an AWGN and a Rayleigh fading channel. For each channel, two separate cases of uncoded packets and coded packets with a perfect block code capable of correcting 10 errors are considered. The transmission and interference ranges as
Improved Model for Transmission and Interference Ranges

a function of transmitter-receiver distance is shown in Fig. 11. The transmission range, $d_{tx}$, is normalized by the transmission range of the case when a packet is transmitted without any coding in an AWGN channel. It can be seen from this figure that small-scale fading has a significant negative effect on both transmission and interference ranges. We can see from Fig. 11 that the transmission range in a fading channel is less than half of transmission range in an AWGN channel. As for the interference range, we can observe that the interference range in Rayleigh fading channel grows at a considerably higher rate compared to the AWGN channel. Consequently, the number of hidden terminals increases substantially in the Rayleigh fading channel.

Comparing the coded case with the uncoded one over the Rayleigh fading channel, we observe that the coding gain is not significant. One reason for this is that, in the absence of interleaving, burst errors, caused by deep fading, can not be corrected.

7 Conclusion

In this paper, we discussed some of the shortcomings of the interference range model introduced in [1] caused by simplifying assumptions. As a first step, we introduced a more general definition for the transmission and interference range in Sec. 2 by taking the probability of successful packet reception into account. Moreover, we demonstrated in Sec. 3 that ignoring the noise compared to the interference results in an approximation error in the interference range calculation, especially for nodes close to the transmission range. Considering that these nodes, very often, are troubled by the hidden terminal problem, we argued that different methods of hidden terminal avoidance based on an inaccurate interference range calculation would not successfully eliminate hidden terminals.

In Section 5, we relaxed the assumption of having a complete overlap between the data and interferer packet as this is a zero-probability event. Our case study indicated that a smaller overlap results in noticeably shorter interference range. Therefore, we speculate that the full-overlap assumption may result in overestimating the interference range.

Effects of physical layer parameters on transmission and interference ranges were studied in Sec. 4 and as our examples indicated, variations in packet length, coding and modulation, clearly influence the transmission and interference ranges. There are two main consequences of this observation. First, as RTS/CTS packets have different size, modulation, or coding compared to data pack-
ets, they might have a different transmission and interference ranges compared to data packets. This fact, to the best of our knowledge, has never been considered in the analysis of protocols based on RTS/CTS handshake. Secondly, as different bit rates at physical layer is often obtained by changing modulation and/or coding, different transmission and interference ranges might exist in networks with physical layer having several bit rates options. This, we believe, might have a negative influence on the performance of the MAC protocol and as a results network performance may be improved if a cross-layer design between physical and MAC layer is employed.

The last section of this paper is devoted to a brief study of the effect of small-scale fading on the transmission and interference ranges. Only the case of constant fading value during the packet is considered. It was shown that a Rayleigh fading channel has destructive effects on both transmission and interference range. While the transmission range is reduced substantially, the interference range was shown to grow at a much faster rate in Rayleigh fading channel compared to AWGN channel. Adding these two effects, we conclude that the hidden terminal problem is even more serious in the Rayleigh fading channel.

References


[5] Jing Deng, Ben Liang, and P. K. Varshney, “Tuning the carrier sensing range of IEEE 802.11 MAC,” *IEEE Global Telecommu-


