

Durée : 1h30 – Documents autorisés

■ ■ ■ Communication radio — 12 points

- 1– Un attaquant essaye d'**injecter** des paquets WiFi malveillants sur l'ordinateur de la victime.

6pts

Il n'a pas accès directement au bureau de la victime, mais il peut accéder librement avec son PC portable, à une autre partie du bâtiment composée de :

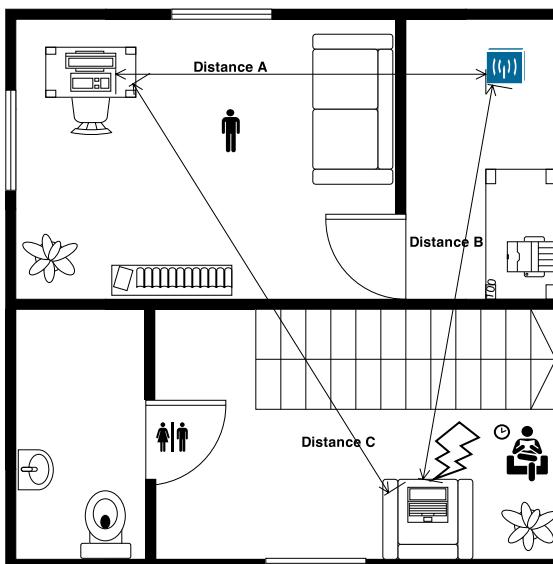
- une salle d'attente avec un fauteuil dans lequel il peut s'installer sans éveiller les soupçons ;
- des toilettes où il peut également séjourner, mais moins longtemps ;

Suivant le placement de l'attaquant, on détermine trois distances :

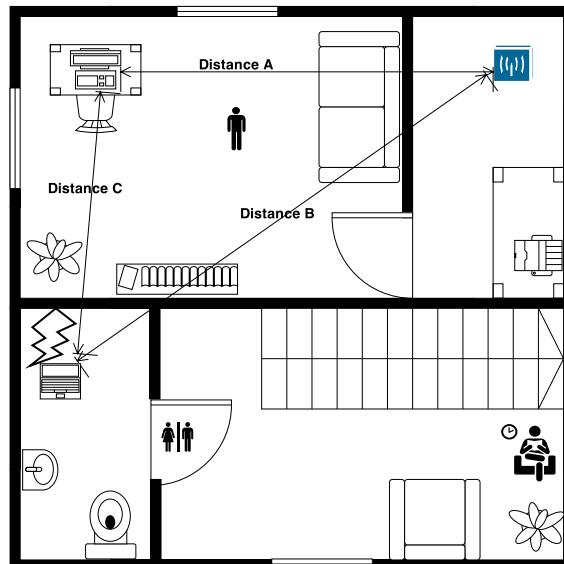
- ▷ distance « A » : du PC de la victime installé sur un bureau au point d'accès WiFi situé dans l'annexe du bureau ;
- ▷ distance « B » : du PC portable de l'attaquant au point d'accès WiFi ;
- ▷ distance « C » : du PC de la victime au PC portable de l'attaquant ;



Voici les deux placements de l'attaquant :



Version « SA »



Version « WC »

Les murs ont les caractéristiques suivantes :

- * celui séparant le PC de la victime du point d'accès induit une atténuation de -12dB ;
- * celui séparant les WC du bureau de la victime induit une atténuation de -20dB à cause du revêtement en carrelage et de la présence de tuyaux en cuivre pour l'alimentation en eau ;
- * celui séparant la salle d'attente du bureau : -12dB.

Les caractéristiques des composants WiFi du PC de la victime et du point d'accès sont les suivantes :

- * la puissance de transmission, « TX Power », est de 20dBm pour les deux ;
- * le gain de l'antenne du PC et du point d'accès est de 2dBi ;
- * la perte due à la connexion de l'antenne est de -0,5dB pour le PC de la victime, et de -1dB pour le point d'accès (son antenne est connectée par un câble) ;

Pour la carte WiFi de l'attaquant :

- * la puissance de transmission est de 20dBm ou 30dBm, son antenne est de 2dBi et son « *cable loss* » est de -0. 5dB.

Enfin, les contraintes pour le WiFi sont les suivantes :

- * on considère qu'une valeur de « *link margin* » supérieure à 20dB est nécessaire pour assurer un échange correct de paquet ;
- * suivant le débit que l'on veut obtenir, et la modulation nécessaire pour l'atteindre, la sensibilité du récepteur varie suivant le tableau suivant :

Débit (Mbps)	54	48	36	24	18	12
Sensibilité (dBm)	-68	-68	-75	-79	-82	-84

Distance (m)	6	8	13	14	15
FSPL (dB)	-56	-58	-62	-63	-64

Questions :

- a. Sachant que la distance « A » est de 8m, quel débit maximum peut être atteint entre le PC de la victime et le point d'accès ? (1pt)
- b. Si l'attaquant essaye d'injecter des paquets vers le PC de la victime **avec le même débit que la victime partage avec le point d'accès**, est-ce qu'il peut le faire :
 - ◊ en version WC, avec une distance « C » de 6m, pour une puissance TX de 20dBm ? de 30dBm ?
 - ◊ en version SA, « salle d'attente », avec une distance « C » de 15m, pour une puissance TX de 20dBm ? de 30dBm ?
- c. Un **outil de détection des injections** a été installé sur le point d'accès. (2pts)
Est-ce qu'il pourra détecter une attaque :
 - ◊ en version WC et avec une distance « B » de 13m ?
 - ◊ en version SA et avec une distance « B » de 14m ?

Si oui, est-ce que l'on pourra aussi savoir où se trouve l'attaquant ?
- d. Est-ce que l'emploi d'une **antenne directionnelle** « yagi » d'un gain de 14dBi permettrait de découvrir toutes les attaques ainsi que l'emplacement des attaquants ? (1pt)

2– a. Pourquoi la **distance** entre deux radios modifie-t-elle le **débit** de la liaison ? (1pt)

2pts b. Pourquoi parle-t-on « *d'étalement de spectre* » ? (1pt)

■ ■ ■ Système embarqué — 2 points

3– a. Qu'est-ce qui **garantie** le bon fonctionnement logiciel d'un système embarqué dans la durée ? (1pt)

2pts b. Quel(s) avantage(s) apporte(nt) une meilleure **batterie** et/ou une meilleure **antenne** ? (1pt)

■ ■ ■ IoT et Sécurité — 6 points

4– a. En quoi l'intégration d'un IoT dans un réseau personnel est-elle plus « *risquée* » que celle de l'ordinateur portable de l'utilisateur ? (2pts)

b. Est-ce que le déploiement d'un IoT chez un utilisateur peut créer un risque pour l'entreprise qui l'a vendu ? (2pts)

c. Est-ce qu'une architecture de PKI est adaptée au contexte de l'IoT ? (2pts)

Vous discuterez de ces avantages et de ces inconvénients, et vous donnerez votre avis en conclusion.

■ ■ ■ Communication radio — 12 points (suite et fin)

5— Réseaux de capteurs avec LoRa :

4pts On utilise un « SF » de 11 avec une bande passante de 250kHz sur tous les capteurs.

Pour un capteur :

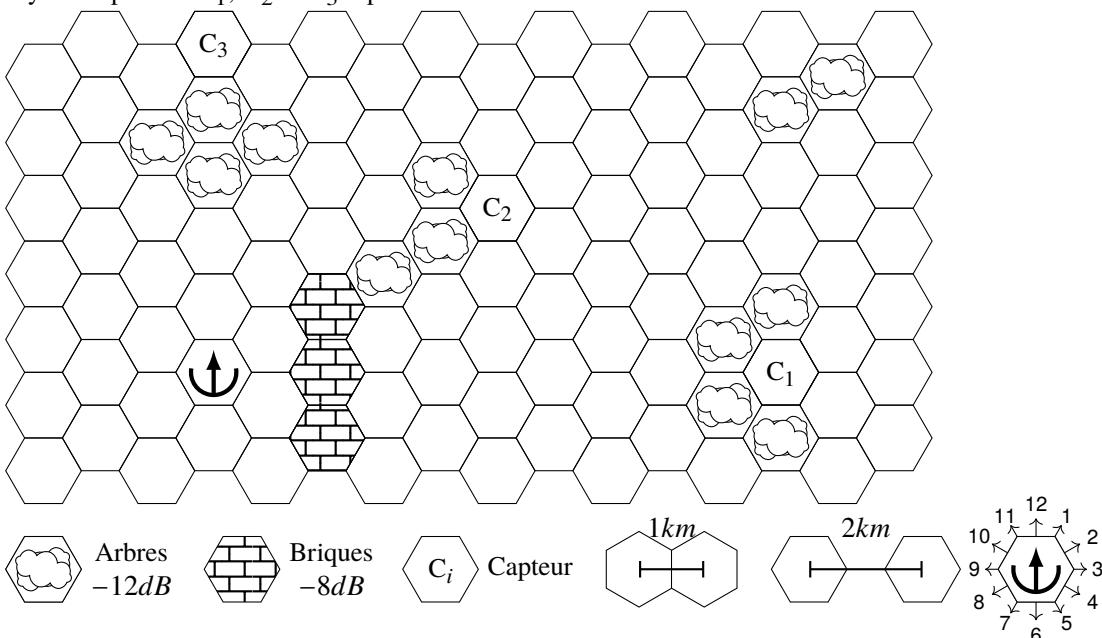
- ◊ l'antenne a un gain de 2dBi ;
- ◊ la puissance d'émission est de 14dBm ;
- ◊ la perte dans le câble et le connecteur de connexion est de -3dB .

La passerelle LoRa possède une antenne directionnelle : son gain est de 6dBi dans la direction vers laquelle elle pointe et de 2dBi dans les autres directions.

La perte dans le câble et le connecteur de connexion est de -3dB .

L'antenne de la passerelle  *est initialement orientée vers 12h.*

Il y a 3 capteurs : C_1 , C_2 et C_3 répartis sur le terrain suivant :



Le passage par une case « Arbres » enlève -12dB et par une case « Briques » -8dB .

Chaque passage d'une case à l'autre étends la distance de 1km .

Exemple : la distance entre la passerelle et le capteur C_1 est de 10km .

Questions :

a. Vérifiez si chacun des capteurs est capable de communiquer avec la passerelle. (2pts)

On considère que la marge de liaison doit être supérieure ou égale à 10dB pour que la liaison fonctionne.

b. Dans le cas où un, ou des liens, ne fonctionne(nt) pas, est-ce que la **réorientation** de l'antenne de la passerelle peut résoudre le problème ? (1pt)

c. Si on ne peut pas changer la direction de l'antenne, que peut-on faire **varier** pour résoudre le problème ? (1pt)
Vous indiquerez si les modifications apportées entraînent des problèmes sur la pérennité du réseau de capteurs.

LoRa	Sensibilité									
	bandwidth	7800	10400	15600	20800	31200	41700	62500	125000	250000
SF6	-132	-131	-129	-128	-125	-124	-121	-118	-115	-112
SF7	-135	-134	-132	-131	-129	-128	-126	-123	-120	-117
SF8	-139	-138	-136	-135	-133	-131	-129	-126	-123	-120
SF9	-142	-141	-139	-138	-136	-134	-132	-129	-126	-123
SF10	-145	-143	-142	-140	-138	-137	-135	-132	-129	-126
SF11	-147	-145	-144	-142	-141	-139	-138	-135	-132	-129
SF12	-149	-148	-146	-145	-143	-142	-140	-137	-134	-131