INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

4ASTI

Réseaux non filaires

Corrections examen avril 2019

Durée : 1h30 – Documents autorisés

Communication radio — 10 points

1 – 6pts 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)*

Le bilan de liaison est :

$20 + (2 - 0.5 - 1 + 2) - 58 - 12 \leq -47.5$ *et* $-47.5 - x \geq 20 \Longrightarrow x \leq -67.5$ *alors on choisit la modulation donnant le débit le plus élevé soit* $54Mbps$ *pour une sensibilité de* $-68dBm$.

FSPL

mur

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 : *(2pts)*

- en version WC, avec une distance « C » de 6m, pour une puissance TX de 20dBm ? de 30dBm ?
  - *en* $20dBm$ *:* $20 + (2 - 0.5 - 1 + 2) - 56 - 20 = -53.5$ *si on veut le même débit alors on a une sensibilité de* $-68dBm$ *ce qui donne une marge de* $-53.5 + 68 = 14.50 < 20 \Longrightarrow$ *l'injection n'est* ***pas possible*** *!*
  - *en* $30dBm$ *: on augmente la marge de* $10dBm \Longrightarrow 24.5 > 20$ *l'injection est* ***possible***.
- en version SA, « salle d'attente », avec une distance « C » de 15m, pour une puissance TX de 20dBm ? de 30dBm ?
  - *en* $20dBm$ *:* $20 + (2 - 0.5 - 1 + 2) - 64 - 20 = -61.5$ *si on veut le même débit alors on a une sensibilité de* $-68dBm$ *ce qui donne une marge de* $-61.5 + 68 = 7.50 < 20 \Longrightarrow$ *l'injection n'est* ***pas possible*** *!*
  - *en* $30dBm$ *: on augmente la marge de* $10dBm \Longrightarrow 17.5 > 20$ *l'injection n'est* ***pas possible***.

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* $20dBm$ *:* $20 + (2 - 0.5 - 1 + 2) - 62 - 32 = -71.5$ *pour recevoir le paquet injecté, il faut pouvoir le démoduler avec le même débit, soit avec une sensibilité de* $-68dBm$ *ce qui donne une marge de* $-71.5 + 68 = -3.5 < 20 \Longrightarrow$ *on ne reçoit rien de démodulable !*
  - *en* $30dBm$ *: on augmente la marge de* $10dBm \Longrightarrow 6.5 > 20$ *la détection n'est* ***pas possible***.
- en version SA et avec une distance « B » de 14m ?
  - *en* $20dBm$ *:* $20 + (2 - 0.5 - 1 + 2) - 63 - 12 = -52.5$ *pour recevoir le paquet injecté, il faut pouvoir le démoduler avec le même débit, soit avec une sensibilité de* $-68dBm$ *ce qui donne une marge de* $-52.5 + 68 = 15.5 < 20 \Longrightarrow$ *on ne reçoit rien de démodulable !*
  - *en* $30dBm$ *: on augmente la marge de* $10dBm \Longrightarrow 25.5 > 20$ *la détection est* ***possible***.

Si oui, est-ce que l'on pourra aussi savoir où se trouve l'attaquant ?

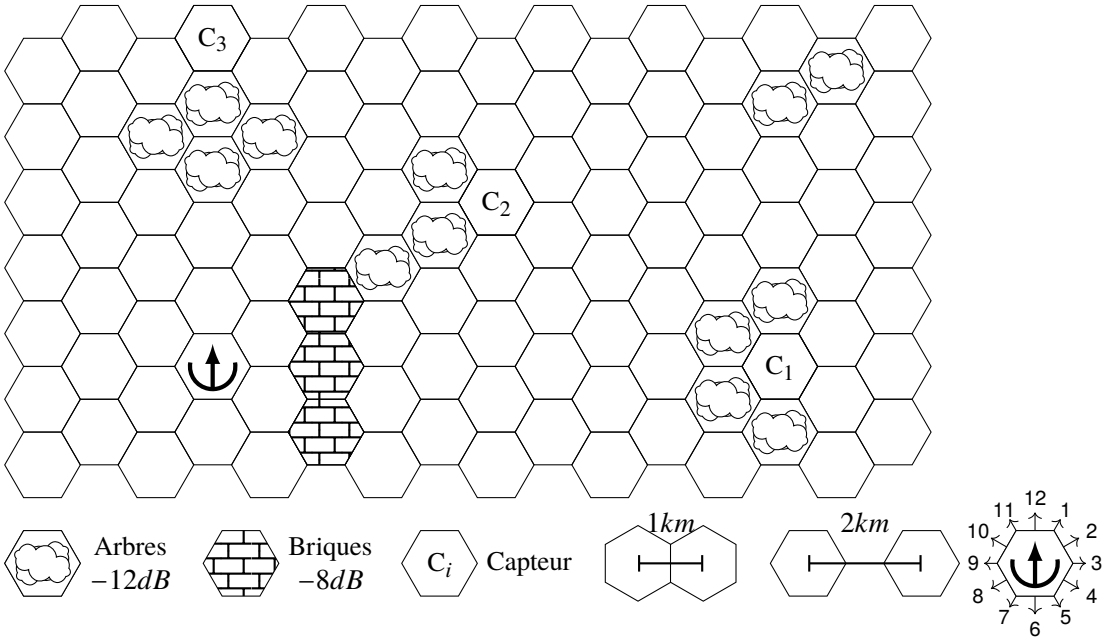
Si on connait les différents endroits possibles où peut se trouver l'attaquant sachant que le débit est maximale, seule la salle d'attente le permet ; mais l'injection n'étant pas possible depuis cette position, l'outil de surveillance ne verra pas l'injection réalisée depuis les WC.

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)*
Oui depuis la Salle d'Attente et depuis les WC.

Communication radio — 10 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.*

	Tx	Cable	Antenne	FSPL	Obstacles	Antenne	Cable	Sensibilité	marge	Comm?
C_1	14	-3	2	-111.22	-20	2	-3	-132	12.78	ok!
C_2	14	-3	2	-105.2	-32	2	-3	-132	6.8	nok!
C_3	14	-3	2	-105.2	-24	6	-3	-132	18.8	ok!

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)*

On peut tourner l'antenne vers « 2h *» et on obtient :*

	Tx	*Cable*	*Antenne*	*FSPL*	*Obstacles*	*Antenne*	*Cable*	*Sensibilité*	*marge*	*Comm?*
C_1	*14*	*-3*	*2*	*-111.22*	*-20*	*2*	*-3*	*-132*	*12.78*	*ok!*
C_2	*14*	*-3*	*2*	*-105.2*	*-32*	*6*	*-3*	*-132*	*10.8*	*ok!*
C_3	*14*	*-3*	*2*	*-105.2*	*-24*	*2*	*-3*	*-132*	*14.8*	*ok!*

$\Longrightarrow$ *On résout le problème.*

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 entrainent des problèmes sur la pérennité du réseau de capteurs.

Pour corriger le problème sur C_2 *il faut* $3.2dB$ *en plus, ce qui s'obtient avec :*

- ◇ *un changement de «* SF *» : pas possible, en passant à «* $SF = 12$ *» on ne gagne que* $2dB$ *;*
- ◇ *un changement de bande passante : en passant à* $250kHz$ *on a un gain de* $3dB$ *mais on pert en débit et c'est insuffisant ;*
- ◇ *un changement de bande passante à* $250kHz$ *et avec un* $SF = 12$*, alors on a un gain de* $5dB$ *ce qui marche mais on augmente le temps de transmission ce qui peut vider la batterie du capteur* C_2 *plus rapidement ;*
- ◇ *on peut changer l'antenne de* C_2 *vers une antenne de gain* $6dBi$*, soit un gain de* $4dB$*, ce qui résout le problème sans affecter le reste.*

LoRa	Sensibilité									
bandwidth	7800	10400	15600	20800	31200	41700	62500	125000	250000	500000
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