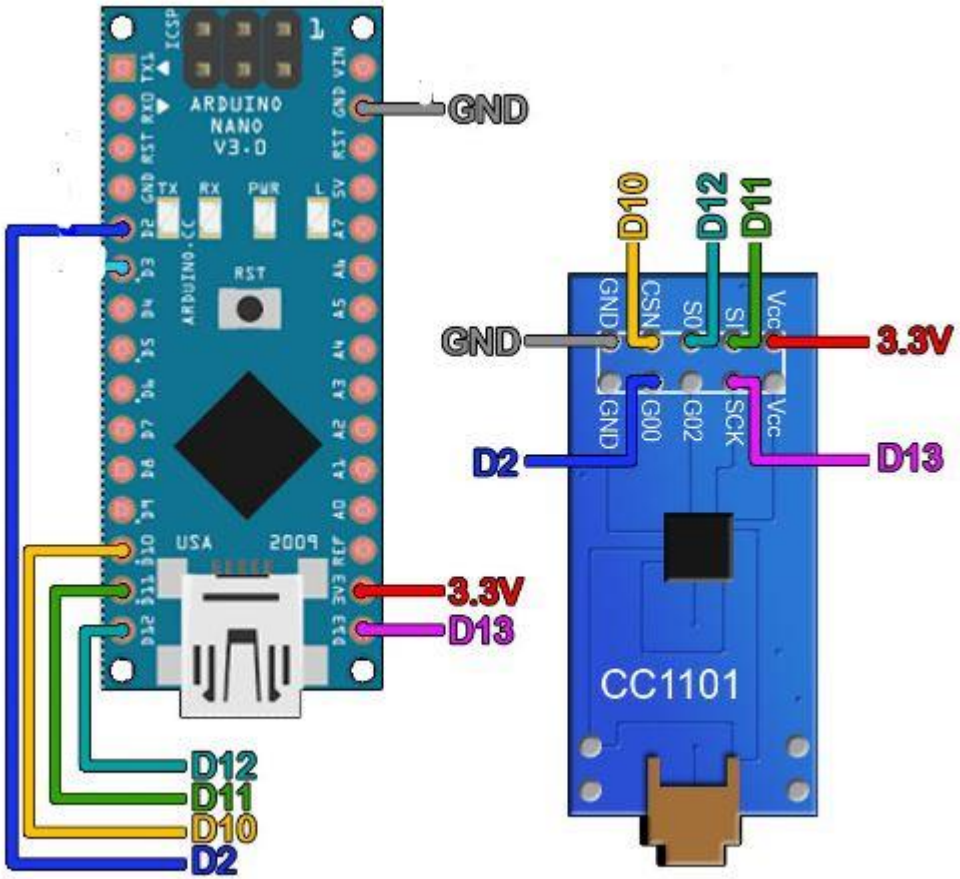
VERISURE PACKET SNIFFER

Structure des paquets

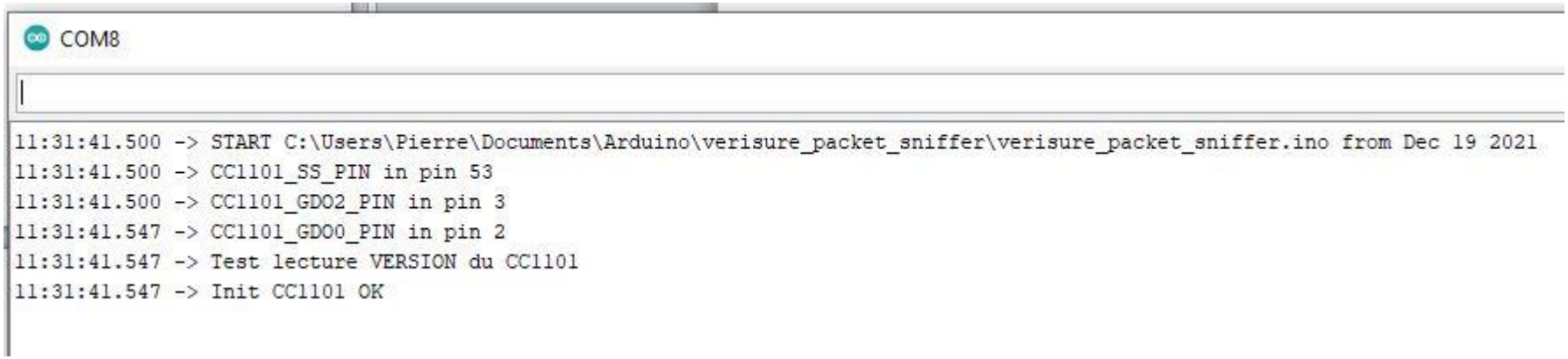
Connexions du CC1101

- Cartes Arduino NANO et UNO
- Pour une carte ATMEGA 2560 remplacer D10 par D53, D11 par D51, D12 par D50 et D13 par D52



Scketch

- Téléverser le sketch verisure_packet_sniffer.ino
- Ouvrir le moniteur série en 57600 bauds
- Si la procédure d'initialisation s'est bien passée on obtient les lignes suivantes



Analyse des échanges

- Relever le contenu des paquets échangés lors des différents évènements : passage devant un détecteur de mouvement, ouverture d'une porte/fenêtre, fermeture d'une porte/fenêtre ….
- Format des paquets reçus (exemple appui sur le bouton central du lecteur de badges)

```
11:31:41.547 -> Init CC1101 OK
11:35:52.820 -> <14> B 67 2F 1A 38 E8 28 0 0 1 B4 B7 42 9B
11:35:52.820 -> Rssi:-41  LQI:155
11:35:52.913 -> <14> B 67 2F 1A 38 E8 28 0 0 1 B4 B7 42 9C
11:35:52.913 -> Rssi:-41  LQI:156
11:35:53.710 -> <14> B 67 2F 1A 38 E8 28 0 0 1 B4 B7 45 9B
11:35:53.710 -> Rssi:-40  LQI:155
```

NB : le même paquet est envoyé 3 fois car ce lecteur n'est pas enregistré sur la centrale (il n'y a pas d'accusé de réception de la centrale).

Analyse des échanges

<14> B 67 2F 1A 38 E8 28 0 0 1 B4 B7 42 9B

Nombre d'octets lus dans le RX FIFO (en décimal)

Nombre d'octets envoyés par le capteur (en hexadécimal)

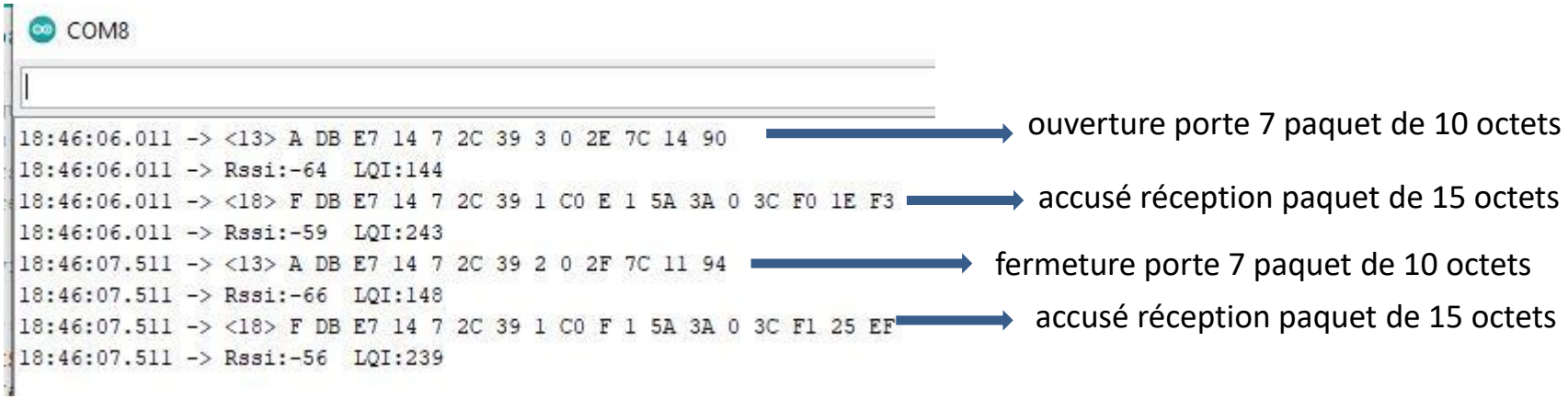
Données envoyées par le capteur (hexadécimal). Soit ici 11 octets

* Données ajoutées par le CC1101 lors de la réception (hexadécimal)

* 2 octets sont ajoutés dans le RX FIFO par le CC1101 lors de la réception. Le premier octet est le RSSI (force du signal) et le second est le LQI (qualité de la liaison) ainsi que le bit de CRC.

Analyse des échanges

- La longueur des paquets dépend du type de capteur et si la centrale est en service ou non.
- Lorsque la centrale est en service on observe des accusés de réception venant de la centrale et à destination des capteurs.
- Exemple ouverture porte 7 puis fermeture porte 7



Analyse des échanges

- Demande d'état (appui sur le bouton central du lecteur de badges)

```
18:59:53.207 -> <14> B DB E7 14 38 5C 28 0 0 17 B4 67 7 82
18:59:53.207 -> Rssi:-71  LQI:130
18:59:53.207 -> <19> 10 DB E7 14 38 5C 28 0 0 16 A7 0 2 2 23 40 C5 1C E7
18:59:53.207 -> Rssi:-60  LQI:231
```

Demande d'état paquet de 11 octets

Réponse de la centrale paquet de 16 octets

- Passage devant le détecteur de mouvement n°2

```
18:59:46.222 -> <13> A DB E7 14 2 9F 26 10 0 E5 9B 6 A9
18:59:46.222 -> Rssi:-71  LQI:169
18:59:46.222 -> <18> F DB E7 14 2 9F 26 0 0 15 1 4D FF 0 3C 49 1E F4
18:59:46.222 -> Rssi:-59  LQI:244
```

Détection mouvement paquet de 10 octets

Accusé réception paquet de 15 octets

Analyse des échanges

- Passage d'un badge devant le lecteur

```
20:34:08.654 -> <27> 18 DB E7 14 38 5C 28 0 0 1F B5 FF FF 4 98 B2 A6 FA EA 2C 80 BC BF FD 77 E 82
20:34:08.654 -> Rssi:-67  LQI:130
20:34:08.654 -> <27> 18 DB E7 14 38 5C 28 0 0 14 B8 FF FF 4 98 B2 A6 FA EA 2C 80 2 0 1 FA 21 E3
20:34:08.654 -> Rssi:-58  LQI:227
20:34:18.968 -> <21> 12 DB E7 14 0 5C 5 0 0 15 50 2 4 0 0 0 0 0 B3 2C D7
20:34:18.968 -> Rssi:-52  LQI:215
20:34:19.906 -> <21> 12 DB E7 14 0 5C 5 0 0 15 50 2 4 0 0 0 0 0 B3 2F D6
20:34:19.906 -> Rssi:-51  LQI:214
20:34:20.890 -> <21> 12 DB E7 14 0 5C 5 0 0 15 50 2 4 0 0 0 0 0 B3 30 D7
20:34:20.890 -> Rssi:-50  LQI:215
```

24 octets envoyés par le lecteur

Accusé réception 24 octets

Infos envoyées par la centrale 18 octets (3 fois)

- Activation du mode nuit (depuis le lecteur de badges)

```
19:55:06.925 -> <14> B DB E7 14 38 5C 28 0 0 1B B3 6A B 84
19:55:06.972 -> Rssi:-69  LQI:132
19:55:06.972 -> <19> 10 DB E7 14 38 5C 28 0 0 3 A7 1E 1 3D 40 0 E7 22 E5
19:55:06.972 -> Rssi:-57  LQI:229
19:55:08.332 -> <21> 12 DB E7 14 0 5C 5 0 0 4 50 4 4 1E 0 0 0 0 C2 30 D9
19:55:08.332 -> Rssi:-50  LQI:217
19:55:09.270 -> <21> 12 DB E7 14 0 5C 5 0 0 4 50 4 4 1E 0 0 0 0 C2 33 D9
19:55:09.270 -> Rssi:-49  LQI:217
19:55:10.207 -> <21> 12 DB E7 14 0 5C 5 0 0 4 50 4 4 1E 0 0 0 0 C2 31 D9
19:55:10.207 -> Rssi:-50  LQI:217
19:55:37.118 -> <21> 12 DB E7 14 0 5C 5 0 0 5 50 1 4 0 0 0 0 0 A2 2F DB
19:55:37.165 -> Rssi:-51  LQI:219
19:55:38.103 -> <21> 12 DB E7 14 0 5C 5 0 0 5 50 1 4 0 0 0 0 0 A2 2F DB
19:55:38.103 -> Rssi:-51  LQI:219
19:55:39.041 -> <21> 12 DB E7 14 0 5C 5 0 0 5 50 1 4 0 0 0 0 0 A2 2F DC
19:55:39.041 -> Rssi:-51  LQI:220
```

Appui mode nuit, paquet de 11 octets

Accusé réception centrale paquet de 16 octets

Décompte pour temporisation de sortie (6 paquets envoyés par la centrale)

Résumé paquets capteurs

- Les paquets envoyés par les détecteurs d'ouverture ou de mouvement ont toujours 10 octets.
- Les accusés de réception de la centrale vers les détecteurs ont toujours 15 octets.
- L'appui sur un des 5 boutons du lecteur de badge envoie des paquets de 11 octets
- L'accusé de réception de la demande du lecteur est composé de 16 octets.
- Le passage d'un badge devant le lecteur de badge envoie des paquets de 24 octets.

Structure des paquets des détecteurs (10 octets)

- Synthèse d'analyse des données sur 3 détecteurs d'ouverture (SW4, SW7, SW8) et un détecteur de mouvement (SW2)

Switch	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
SW4 O	0xDB	0xE7	0x14	0x04	0x7C	0x39	0x03	0x00	0x91	0x2C
SW4 F	0xDB	0xE7	0x14	0x04	0x7C	0x39	0x02	0x00	0x92	0x2C
SW7 O	0xDB	0xE7	0x14	0x07	0x2C	0x39	0x03	0x00	0x22	0x70
SW7 F	0xDB	0xE7	0x14	0x07	0x2C	0x39	0x02	0x00	0x23	0x70
SW8 O	0xDB	0xE7	0x14	0x08	0x38	0x39	0x03	0x00	0x31	0x8C
SW8 F	0xDB	0xE7	0x14	0x08	0x38	0x39	0x02	0x00	0x32	0x8C
SW2 D	0xDB	0xE7	0x14	0x02	0x9F	0x26	0x10	0x00	0xD2	0x88

Déduction de la signification des différents champs (byte 1 à 10)
Tous les capteurs enregistrés sur la centrale possèdent le même ID réseau (3 premiers octets).

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10
0xDB ID réseau	**0xE7** ID réseau	**0x14** ID réseau	**N° capteur** Numéro du capteur	Identification capteur ?	Type capteur ?	**ETAT** 0x03=ouvert 0x02=fermé 0x10=détecté	Toujours à 0	Compteur poids faible	Compteur poids fort

Structure des paquets des boutons du lecteur de badge (11 octets)

Bouton	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11
Centre	0x67	0x2F	0x1A	0x38	0xE8	0x28	0x00	0x00	0x24	0xB4	0xDA
Nuit	0x67	0x2F	0x1A	0x38	0xE8	0x28	0x00	0x00	0x02	0xB3	0xB7
Jour	0x67	0x2F	0x1A	0x38	0xE8	0x28	0x00	0x00	0x03	0xB2	0xB7
Total	0x67	0x2F	0x1A	0x38	0xE8	0x28	0x00	0x00	0x04	0xA0	0xA6
Silent	0x67	0x2F	0x1A	0x38	0xE8	0x28	0x00	0x00	0x05	0xB1	0xB8
Centre *	0xDB	0xE7	0x14	0x38	0x5C	0x28	0x00	0x00	0x34	0xB4	0x84
Nuit *	0xDB	0xE7	0x14	0x38	0x5C	0x28	0x00	0x00	0x35	0xB3	0x84

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10	Byte 11
0xDB ID réseau	**0xE7** ID réseau	**0x14** ID réseau	**0x38** Type de capteur	0x5C Identification capteur ?	0x28 Identification capteur ?	Toujours à 0	Toujours à 0	Compteur	**ID bouton** 0xB4=centre 0xB3=nuit 0xB2=jour 0xA0=total 0xB1=silent	Compteur ou CRC ?

Utilisation de 2 lecteurs de badges pour l'analyse. Le lecteur enregistré est repéré par * (même ID réseau que les capteurs)

Structure des paquets du passage du badge (24 octets)

- Passage du badge 1 (2 fois)

DB E7 14 38 5C 28 0 0 42 B5 FF FF 4 98 B2 A6 FA EA 2C 80 BC BF FD 9A

DB E7 14 38 5C 28 0 0 43 B5 FF FF 4 98 B2 A6 FA EA 2C 80 BC BF FD 9B

- Passage du badge 2 (2 fois)

DB E7 14 38 5C 28 0 0 3C B5 FF FF 4 27 44 EF 82 E9 2C 80 C7 3A A6 B4

DB E7 14 38 5C 28 0 0 44 B5 FF FF 4 27 44 EF 82 E9 2C 80 C7 3A A6 BC

Structure des paquets de passage en mode activation de l'alarme

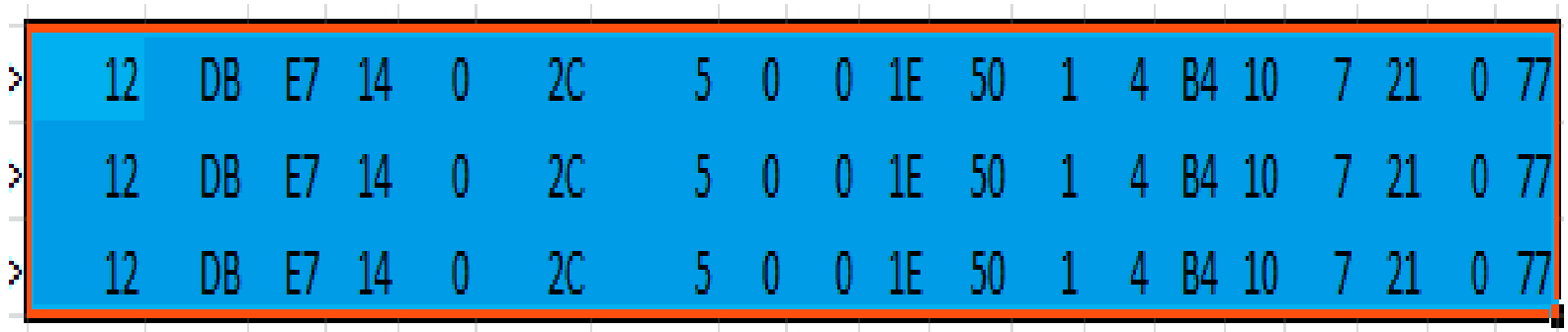
- Passage en mode nuit à partir du lecteur de badges ou du clavier de la centrale.
- Réponses de la centrale à la demande d'activation (18 octets)

12	DB	E7	14	0	5C	5	0	0	8	50	4	4	1E	0	0	0	C6
12	DB	E7	14	0	5C	5	0	0	8	50	4	4	1E	0	0	0	C6
12	DB	E7	14	0	5C	5	0	0	8	50	4	4	1E	0	0	0	C6
12	DB	E7	14	0	5C	5	0	0	9	50	1	4	0	0	0	0	A6
12	DB	E7	14	0	5C	5	0	0	9	50	1	4	0	0	0	0	A6
12	DB	E7	14	0	5C	5	0	0	9	50	1	4	0	0	0	0	A6

- 3 paquets espacés d'une seconde pendant le décompte de la temporisation de sortie puis 30 secondes plus tard 3 paquets identiques pour confirmer l'activation.
- Champ 11=4 activation en cours (tempo de sortie)
- Champ11= 1 activation effective
- Champ 12=4 mode nuit

Structure des paquets lors de la détection d'intrusion

- Déclenchement de la sirène (18 octets)



>	12	DB	E7	14	0	2C	5	0	0	1E	50	1	4	B4	10	7	21	0	77
>	12	DB	E7	14	0	2C	5	0	0	1E	50	1	4	B4	10	7	21	0	77
>	12	DB	E7	14	0	2C	5	0	0	1E	50	1	4	B4	10	7	21	0	77

- Hypothèse champ 14 avec la valeur 0x10