Cahier Des Charges

Ilyas Barrouhou
Guillaume Valentis
Hugo Chevalier
Mathieu Drillet
Louis Gentil

Table des matières

1 Présentation d'E-protect **3**
- 1.1 Contexte . . . 3
- 1.2 Objet du projet . . . 5

2 Description du système **6**
- 2.1 Périmètre du projet cibles/clientèle . . . 6
- 2.2 Description des besoins fonctionnels . . . 6
- 2.3 Fonctions attendues . . . 6

3 Besoins fonctionnels **7**
- 3.1 Système embarqué . . . 7
  - 3.1.1 Fonctions principales . . . 7
  - 3.1.2 Fonction complémentaires . . . 9
- 3.2 Systéme d'information . . . 10
  - 3.2.1 Besoins fonctionnels en Front Office . . . 10
  - 3.2.2 Besoins fonctionnels en Back Office . . . 10

4 Contraintes **11**
- 4.1 Contraintes SI : . . . 11
  - 4.1.1 Backend . . . 11
  - 4.1.2 Utilisateurs : . . . 11
  - 4.1.3 Serveur : . . . 11
  - 4.1.4 Autres contraintes : . . . 11
- 4.2 Contrainte SE : . . . 11
  - 4.2.1 Environnement : . . . 11
  - 4.2.2 Autonomie : . . . 12
  - 4.2.3 Technologie : . . . 12

5 Prestations attendues **13**
- 5.1 Présentation des préstations attendues . . . 13
- 5.2 Critères de choix . . . 13

Glossaire

Terminologies

Terme	Définition
Time-Out	Désigne le fait qu'une requête informatique dépasse le temps limite de réponse, celle-ci est donc annulée et retirée de la file d'attente
Rasberry Pi	Petit ordinateur monocarte basé sur un processeur ARM qui tourne sous une distribution de Linux
Log	Fichier regroupant un historique de fonctionnement d'un programme
Cloud	cloud computing, principe de partage et stockage de données sur le réseau
Câble RJ45	Câble Ethernet

Acronymes

Acronyme	Signification	Définition
UART	Universal Asynchronous Receiver Transmitter	Communication Série
USART	Universal Synchronous Asynchronous Receiver Transmitter	Communication Série
ASM	Langage assembleur	Programmation très bas niveau
Ajax	Asynchronous JavaScript and XML	permet de rendre une page dynamique, celle-ci n'a pas besoin de se rafraichir pour mettre à jour les données
SE	Système Embarqué	désignation d'un cursus informatique embarqué dans une école d'ingénieurs
SI	Système d'Information	désignation d'un cursus informatique dans une école d'ingénieurs
html	Hypertext Markup Language	Langage de balisage permettant de formater du texte et mettre en forme une page web
css	Cascading Style Sheets	combiné au html permet de réaliser un style pour une page web
PHP	Hypertext Preprocessor	Langage de programmation principalement utilisé pour produire des pages Web dynamiques
SQL	Structured Query Language	Langage servant à exploiter des BDD
BDD	Base De Donnée	Outil permettant de stocker des données

CHAPITRE 1

Présentation d'E-protect

1.1 Contexte

Progression du nombre de cambriolages en France

Selon l'Observatoire national de la délinquance et de la réponse pénale (ONDRP), le nombre des vols commis aux domiciles des particuliers et dans les entrepôts a une nouvelle fois augmenté en 2013, de 7.2% en zone urbaine sur un an.
2013 : hausse de 6.4% (par rapport à 2012) des cambriolages en zone urbaine et de 4.7% en zone rurale. Les cambriolages dans les habitations principales ont respectivement augmenté, dans ces mêmes zones, de 7% et de 1.3% et ceux des résidences secondaires de 10% et 17.7%.
Les cambriolages de résidences principales ont bondi de 11.3% en 2014 dans les secteurs ruraux et périurbains. Soit, 23300 cambriolages de plus en 12 mois !

Il se produit un cambriolage toutes les 1.5 minutes en France, soit près de 985 cambriolages par jour(323000 en 2011 et 359500 en 2012) ; Dopant le business des alarmes et des portes blindées. Le nombre de cambriolages est en hausse constante : sur les 6 prochaines années un Français a 1 chance sur 10 de se faire cambrioler, tout en sachant que cette statistique ne tient pas compte des tentatives ou cambriolages non déclarés.

Les chiffres clés

- 8% des foyers français étaient équipés d'une porte blindée en France en 2009
- 95% des cambrioleurs prennent la fuite en cas de déclenchement d'une alarme. Un argument majeur pour s'équiper !
- Les cambriolages représentent 14% des atteintes aux biens.
- 80% des cambriolages ont lieu en ville et 13% seulement sont élucidés.
- 50% des cambriolages concernent les résidences principales, 6% les résidences secondaires et 44% les locaux professionnels.
- 80% des cambrioleurs empruntent la porte, les autres passent par le toit ou les fenêtres.
- 5 minutes : c'est le délai moyen après lequel le monte-en-l'air abandonne son effraction.
- En général, un cambriolage ne dépasse pas une vingtaine de minutes.
- 22% des Français ayant subi un cambriolage n'ont absolument rien fait par la suite pour améliorer leur sécurité !
- 80% des cambriolages ont lieu en plein jour, 55% entre 14 et 17H
- Il y a donc également 20% des cambriolages la nuit pendant le sommeil des propriétaires
- 6500€ : Un cambriolage dans une résidence principale coûte à ses victimes près de 6500 euros.

Récapitulatif

- 382000 en 2013 : +6%
- 359500 en 2012 : +11%
- 323000 en 2011

Cambriolages enregistrés en France métropolitaine	2007	2008	2009	2010	2011	2012
Faits constatés par la Police Nationale	**193 771**	**180 422**	**185 386**	**188 867**	**197 579**	**201 926**
Cambriolages de locaux d'habitations principales	99 745	98 431	105 605	110 651	126 832	132 834
Cambriolages de résidences secondaires	2 234	1 936	2 249	2 442	2 399	2 568
Cambriolages de locaux industriels, commerciaux ou financiers	45 656	38 602	37 588	37 963	33 561	30 346
Cambriolages d'autres lieux	46 136	41 453	39 944	37 811	34 787	36 178
Faits constatés par la Gendarmerie Nationale	**118 613**	**117 751**	**125 914**	**127 217**	**135 759**	**150 700**
Cambriolages de locaux d'habitations principales	50 879	53 306	58 545	61 846	75 166	86 240
Cambriolages de résidences secondaires	12 922	12 577	13 009	11 585	11 874	12 448
Cambriolages de locaux industriels, commerciaux ou financiers	34 911	31 678	33 298	33 426	29 901	29 793
Cambriolages d'autres lieux	19 901	20 190	21 062	20 360	18 818	22 219

FIGURE 1.1 – Cambriolages enregistrés par la police nationale (zone urbaine) ou par la gendarmerie nationale (zone rurale) en France de 2007 à 2012 [1]

En tête du classement on trouve la Guadeloupe. Avec un taux de 6.5 cambriolages pour 1000 habitants, elle précède le Vaucluse (6.4 pour 1000 habitants). De manière générale, les départements d'outre-mer sont parmi les plus exposés au risque de cambriolage. La Guyane affiche ainsi une statistique de 6 pour 1000 habitants. Concernant le France métropolitaine, le sud-est est particulièrement touché par les affaires de cambriolages d'habitations principales.

Six départements ont un taux compris entre 5.4 et 6.5 pour 1000 habitants (les Pyrénées-Orientales, l'Hérault, le Gard, le Vaucluse, les Bouches du Rhône et les Alpes-Maritimes).

L'Île de France que l'on pourrait considérer comme une région très exposée limite la casse et reste dans la moyenne nationale de 2.7/1000 habitants. A l'inverse, le risque de se faire cambrioler est extrêmement faible dans le centre de la France. Les résidents du Cantal peuvent dormir sur leurs deux oreilles avec seulement 0.3 cambriolage pour 1000 habitants département du Cantal. La Haute-Corse connaît la plus forte variation à la hausse avec une augmentation de 71.4%.

L'importance de développer des solutions de protections est bien réelle. De nos jours lorsque l'on achète une alarme pour notre domicile, il faut obligatoirement avoir l'aide d'un technicien pour la poser. Si l'on souhaite installer d'autres capteurs, il faut rappeler un technicien (perte de temps, et obligation de se libérer pour être présent). Du point de vue du client, cela est contraignant car il dépend d'un organisme extérieur. De plus, le fait de faire installer l'alarme par une personne inconnue est un risque potentiel.[2]

1.2 Objet du projet

L'importance de développer des solutions de protections est bien réelle.
La procédure actuelle mobilise beaucoup de temps et représente un investissement financier certain du point de vue client. L'installation ou modifications de système d'alarmes nécessite obligatoirement l'intervention d'un technicien, facturé, dans une plage horaire poussant le client à se libérer de ses activités professionnelles.

E-protect libère des ces contraintes, proposant un produit modulable et installable directement par le client, bénéficiant d'un service de conseils gratuit, celui-ci n'a plus à dépendre d'un organisme extérieur.

Le produit proposé est un système d'alarme résidentiel connecté, facile à installer et à configurer. Afin de proposer un système le moins chère possible, E-protect s'appuie sur l'élimination des intermédiaires et utilise un réseau meshe de capteurs intelligent, travaillant sur une portée moins importante et jouant ainsi sur la connexion des capteurs entre eux. L'installation des composants du système E-protect est beaucoup plus simple qu'un système d'alarme filé. Nul besoin de percer les murs et de poser des conducteurs, ce qui réduit considérablement les frais d'installation.

Accessible depuis internet et une application Smartphone, E-protect assure un contact permanent entre le client et le domicile.

Le système E-protect comporte aussi :
- Une connexion avec le poste de police le plus proche ;
- Un système Backup en cas de défaillance du réseau électrique ;
- Un design de capteur innovant et modulable selon la volonté du client ;
- Une consommation énergétique très faible, reposant sur un appel de puissance réduit du fait de l'utilisation d'un réseau meshe.

CHAPITRE 2

Description du système

2.1 Périmètre du projet cibles/clientèle

E-protect assurera la surveillance et la protection des clients résidentiels. Les régions prioritairement ciblées sont la **Guadeloupe** première victime du cambriolage, avec un taux de 6.5 cambriolages pour 1000 habitants, elle précède le **Vaucluse** (6.4 pour 1000 habitants). De manière générale, les départements d'outre-mer sont parmi les plus exposés. La **Guyane** affiche ainsi une statistique de 6 pour 1000 habitants. Concernant le France métropolitaine, le sud-est est particulièrement touché par les affaires de cambriolages d'habitations principales.

De plus, en métropole six départements ont un taux compris entre 5.4 et 6.5 pour 1000 habitants (**les Pyrénées-Orientales, l'Hérault, le Gard, le Vaucluse, les Bouches du Rhône et les Alpes-Maritimes**).

L'Île de France que l'on pourrait considérer comme une région très exposée limite la casse et reste dans la moyenne nationale de 2.7/1000 habitants. A l'inverse, le risque de se faire cambrioler est extrêmement faible dans le centre de la France. Les résidents du Cantal peuvent dormir sur leurs deux oreilles avec seulement 0.3 cambriolage pour 1000 habitants département du Cantal. La **Haute-Corse** connaît la plus forte variation à la hausse avec une augmentation de 71.4%.[2]

2.2 Description des besoins fonctionnels

La solution proposé peut se décomposer en deux parties :
- **Hardware** : une centrale d'alarme va gérer un parc de capteurs connectés suivant une topologie meshé (ZigBee/Bluetooth Low Energy/CSRmesh). L'alarme devra se désactiver lorsque le client entre dans la maison (ou appuies sur un bouton de l'application mobile). L'alarme devra être la plus discrète possible. L'alarme doit pouvoir intéragir avec la partie software (Sigfox/Ethernet) ;
- **Software** : Une application mobile et un site web permettront de se tenir informé de l'état de fonctionnement de l'alarme. De plus le client pourra configurer l'alarme à distance (Application Android/iOS/Windows Phone, Javascript/PHP/C#/SQL).

2.3 Fonctions attendues

Différentes fonctions sont attendues lors du développement d'E-protect :
- Application Smartphone permettant de surveiller, de modifier, d'activer ou désactiver le système à distance ;
- Interface du système ;
- Une connexion avec le poste de police le plus proche ;
- Un système Backup en cas de défaillance du réseau électrique ;
- Un design de capteur innovant et modulable selon la volonté du client ;
- Une consommation énergétique très faible, reposant sur un appel de puissance réduit du fait de l'utilisation d'un réseau meshe ;
- ...

CHAPITRE 3

Besoins fonctionnels

3.1 Système embarqué

3.1.1 Fonctions principales

Communiquer

Communication inter-capteurs Une centrale d'alarme contrôle un parc de capteurs connectés suivant une topologie meshé (ZigBee/Bluetooth Low Energy/CSRmesh).
Les données perçues par les capteurs sont transmises avec le protocole 6lowPan.
Le protocole 6LoWPan appartient au standard IEEE 802.15.4. Celui-ci présente :

- Des ressources limitées avec un coût faible
- Basse consommation et détection de l'énergie
- Faible porté et courtes distances
- Interconnecter des unités embarqués avec peu de ressources comme des capteurs
- Les unités sont en sommeil la plupart du temps

Protocole 6LoWPan
A la volonté du client, pour toute modification de configuration du système d'alarme, 6LoWPan permet à une machine nouvellement connéctée au réseau de s'autoconfigurer soit déterminer son adresse lien local et vérifier son unicité. De plus ce protocole présente des avantages certains concernant l'intéropérabilité extensive (wifi, ethernet, GPRS, ATM), la sécurité (authentification, pare-feux), les services réseaux de haut niveau (équilibrage de la charge, cache, mobilité, NAT), l'adressage et le routage, les services applicatifs de haut niveaux (HTTP,XML,SOAP,REST) ainsi qu'au niveau des outils de supervision réseaux.[3]

Le choix du protocole 6LoWPan se définis autour de plusiseurs points clés.
E-protect travail sur un réseau meshé interne qui ne necessite pas énormément de données mais suffisament pour transmettre les données issues des caméras de surveillance. Nous obtons donc pour la technologie 6LoWPan allégée 96 octets sur UDP (User Datagram Protocol).

Modalité de routage
Le 6LoWPan utilisé utilise un routage Mesh Under.
La décision de routage se faisant au niveau du 6 LoWPan et seulement avec les fragments du paquets IPv6 reconstitué uniquement dans l'équipement destinataire permet un délai de transmission plus court.[3]

Communication serveur

La connexion serveur est assuré par le protocole TCP, protocole plus orienté « connexion » afin de répondre aux exigences de sécurités de transmission des données.
Répondant à l'ensemble des options du protocole UDP, le protocole TCP vérifie que le destinataire soit prêt à réceptionner les données et témoigne de la bonne réception par un accusé de réception. Pour cela les paquets importants de données sont transmis en somme de plus petit paquets pour

que l'IP les accepte.
Le contrôle des données s'effectue par le biais du contrôle CRC. Le CRC vérifie l'intégralité des données transmises, permettant dans le cas où les données reçues sont corrompues, aux destinataires de demander à l'émetteur de renvoyer les données corrompues.[3]

Communication utilisateur Une application mobile et un site web permet de tenir le client informé de l'état de fonctionnement de l'ensemble du système et lui permettront de le configurer à distance (Application Android/iOS/Windows Phone, Javascript/PHP/C#/SQL).

- Application mobile avec notification push
- Interface mobile : écran de contrôle (modification du système, mise en veille, activation/désactivation, contrôle de la connexion UNB...)
- Accés à une page internet personnalisée en connexion constante avec le système E-protect

Backup

Alimentation secondaire E-protect assure le fonctionnement du système en cas de coupure de courant en basculant l'instalation en fonctionnement Back-up.
L'ensemble du système se place en fonctionnement basse consommation. Seules les fonctions principales restent actives (écran et rasberry se désactivent). Le client garde le contrôle de l'installation (activation/désactivation de l'ensemble du système de sécurité) par le biais d'une carte de contôle.
L'alimentation générale se fait par déchargement de batterie assurant le fonctionnement de l'ensemble du système 48h durant. Branché au secteur, la batterie untilisée se charge en fonctionnement normal.
Communication secondaire La communication SigFox permet d'alerter le client en cas de coupure d'électricité ou de connexion internet. Ce protocole est intégré à la base. SIGFOX utilise UNB (Ultra Narrow Band) basé sur une technologie radio pour connecter des périphériques à son réseau mondial.
Le réseau fonctionne dans les bandes ISM (bandes de fréquences sans licence) disponibles mondialement et coexistent sur ces fréquences avec d'autres technologies radio, mais sans aucun risque de collision ou de problèmes de capacité. SIGFOX utilise actuellement la bande européenne ISL la plus populaire sur 868MHz (telle que définie par l'ETSI et CEPT).

Un avantage important fourni par l'utilisation de la technologie à bande étroite est la flexibilité liée au choix de l'antenne.

Le protocole SIGFOX est compatible avec les émetteurs-récepteurs existants et activement transféré vers un nombre de plateformes techniques.
[4]

Auto-monitoring

Dans un souci de surveillance informatique, E-protect assurera une communication permanente entre les capteurs et la base.
Ce monitoring s'articule autour d'un échange de données (protocole 6LoWPan) des capteurs à la base (RAS) sur un pas de temps d'une minute. En cas de non réception de message provenant d'un des capteurs, la base sonde le capteur en question et communique au client l'état du système (protocole SigFox).

Sécuriser les données

6LoWPan
Le 6LoWPan permet de garantir la sécurité (confidentialité et intégrité) des données et la disponibilité du réseau.
Afin de répondre aux attaques externes actives tel que la paralysation du réseau par brouillage du signal radio, E-protect renforce la sécurités de ses données par l'optimisation du cryptage.
Pour cela l'algorithme AES 128 est utilisé pour sécuriser la couche liaison (MAC). Cet algorithme a été conçu de manière à rendre des méthodes de brouillage classique tels que la cryptanalyse linéaire ou différentielle extremement difficile.[3]

SigFox
La communication sur SIGFOX est sécurisée à bien des égards, y compris la protection anti-rejeu, message de brouillage, séquençage, etc. Cependant, l'aspect le plus important de la sécurité de transmission est le fait que seuls les fournisseurs de périphérique comprennent les données échangées entre le périphérique et les systèmes informatiques. SIGFOX agit seulement comme un canal de transport, poussant les données vers le système informatique du client.[4]

3.1.2 Fonction complémentaires

Alimenter le système

Le système E-protect propose deux systèmes d'alimentations electriques **Utilisation du secteur** Branchement de la base au secteur. **Utilisation de Witricity, modèle WIT-5000**
Cette méthode repose sur la conversion d'énergie de radiations microondes directionnelles, limitant les risques sur la santé et la sécurité, en énergie électrique continue.
Il s'agit d'un système de filtrage et d'un redresseur, basé sur l'association originale d'un système passif d'adaptation d'impédance optimisé et d'un convertisseur spécifique.
Ce système à une durée de vie illimité.
Le transmetteur et le récepteur ont des antennes à boucle magnétique synchronisé à la même fréquence. le système fonctionne dans un champs magnétique, identique au champ magnétique de la bobine Tesla mais utilise une énergie considérablement plus basse et sécuritaire grâce à la technologie des champs rapprochés qui donne un bon pouvoir de transmission.
Le WIT-5000 est conçu avec la spécification Rezence pour l'électronique grand public, de l'Alliance pour l'électricité sans fil (A4WP). Il fonctionne à 6,78 MHz, une fréquence de fonctionnement qui est adoptée pour les applications électronique grand public et largement utilisé dans les applications industrielles, médicales et scientifiques. A cette fréquence, le système de recharge sans fil a une interaction minimale avec des corps étrangers métalliques, et a été conçu pour respecter les limites applicables d'exposition humaine. L'utilisation de Bluetooth LE pour le contrôle du système, permet au Wit-5000 de tirer parti de l'infrastructure de communication existante qui peut déjà être en place dans les dispositifs de consommateurs (smartphones, tablettes, ordinateurs personnels).[5]

Gérer la consommation

Reposant sur un réseau meshé et une technologie de capteur innovante, le système E-protect travaille sur des communications (capteurs/capteur, capteur/base) de faibles portées. Une économie d'énergie consommée conséquente est réalisée par diminution d'appelles de puissance.

Design

Le réseau E-protect s'articule autour de deux types de capteurs à différentes fonctions, les dissuasifs et les camouflés.

Dissuasif

Fidèle à sa fonction première les capteurs dissuasifs sont installés de sorte à ce que l'intru potentiel puisse les voir à l'interieur (fenètre, porte vitrée, etc...) comme à l'exterieur du domicile et renonce à donner suite à ses intentions.

Camouflé

Les capteurs camouflés ont une fonction propre à chaque clients, de taille plus petite et installable sur n'importe quel support.

3.2 Systéme d'information

3.2.1 Besoins fonctionnels en Front Office

Notre site web à pour objectif d'être consulté par l'utilisateur afin qu'il puisse avoir un état des capteurs qui sont chez lui. Dans ce but il faut qu'en cas d'alerte il puisse se connecter de n'importe quel périphérique, portable , tablette ou ordinateur, nous avons donc besoin d'un site web adaptatif (responsive design).

Nous optons pour le framework css/html bootstrap. Dans le but de rendre le site le plus simple possible pour l'utilisateur se traduisant par la présence de toutes les actions sur la page utilisateur.

3.2.2 Besoins fonctionnels en Back Office

Pour la communication entre les bases et le serveur nous utilisons la technologie des socket qui représente l'avantage de ne pas être à sens unique et qui permet de savoir quand la connexion est perdu, contrairement aux simples requetes http.

Le framework, sailsjs, ne pouvant pas gérer les sockets tcp (ceux utilisé par la raspberrypi) nous obtons pour un bridge via un serveur node qui communique à la fois avec la raspberrypi et le serveur web en utilisant socketio. Nous nous imposons d'utiliser une base de donnée NoSQL et avons choisi MongoDb.

Afin de notifier l'utilisateur, l'utilisation de l'API Twilio permet d'envoyer une alerte par message telephonique.

CHAPITRE 4

Contraintes

4.1 Contraintes SI :

4.1.1 Backend

– Technologies : Nous nous sommes imposé comme contrainte de faire le backend en node.js, nous avons choisi le framework sailsjs, qui présente une architecture MVC et prends en charge nativement les websockets (avec socket.io) et s'adapte à n'importe quel framework frontend. Le raspberry communique avec le serveur en tcp, sailsjs cependant ne supporte pas les sockets tcp il faut donc que l'on fasse un bridge en node qui ouvrira un socket en tcp avec la raspberrypi d'un côté et un websocket avec l'application web de l'autre.

4.1.2 Utilisateurs :

L'utilisateur doit pouvoir :
– Pouvoir créer un compte ;
– Pouvoir connecter une base existante mais non lié à un utilisateur ;
– Pouvoir renommer les devices ;
– Pouvoir monitorer en temps réel l'activité des bases et devices.

4.1.3 Serveur :

Le serveur doit répondre aux actions suivantes :
– Connecter des devices aux bases (via websocket) ;
– Rajouter une base (via requete url sigfox).

4.1.4 Autres contraintes :

– Les Comptes admin doivent pouvoir gérer les utilisateurs ;
– Possibilité de logger l'activité des devices.

4.2 Contrainte SE :

4.2.1 Environnement :

– La base doit être camouflé et prendre la forme d'un objet courant ;
– La base nécessite une prise de courant à proximité ;
– Nécessite un port Ethernet proche ;
– Les capteurs destinés à l'intérieur de la maison doivent être le plus discret possible.

4.2.2 Autonomie :

- La base doit pouvoir communiquer pendant au moins 48h après une coupure de courant ;
- La base doit éteindre l'écran numérique lors d'une coupure de courant ;
- Les capteurs doivent avoir une autonomie de 1 an en fonctionnement normal.

4.2.3 Technologie :

- La base doit pouvoir gérer le réseaux local de capteurs (6lowpan IPV6) ;
- La base doit communiquer avec le serveur distant en IPV4 ;
- En cas de coupure de courant, la base doit communiquer grâce au modem sigFox.
- Les capteurs doivent communiquer en 6lowPan

CHAPITRE 5

Prestations attendues

5.1 Présentation des préstations attendues

E-protect assurera :
- Interactions de différents type de capteurs, de chocs, de mouvements et caméra.
- Application Smartphone permettant de surveiller, de modifier, d'activer ou désactiver le système à distance.
- Interface mobile : écran de contrôle (modification du système, mise en veille, activation/désactivation, contrôle de la connexion UNB...).
- Systeme Back-up assurant le bon fonctionnement du système en cas de coupure de courant.
- Accés à une page internet personnalisée en connexion constante avec le système E-protect
- Service de conseils d'installation et de suivi du produit gratuit.

5.2 Critères de choix

Critères pris en compte :
- Facilité et gain de temps dans l'installation du parc de capteur.
- Proposition d'un produit modulable.
- Diminution du coût d'installation pour rivaliser sur le marché.
- Elimination de tout intermédiaire.
- Necessité d'interaction avec les réseaux existants.
- Accessibilité constante du système par toute forme de support smart (smartphone, ordinateur, tablette)
- Installation d'une alarme (95% des cambrioleurs prennent la fuite en cas de déclenchement d'une alarme).
- Localisation des conseils de pose de capteur (80% des cambrioleurs empruntent la porte, les autres passent par le toit ou les fenêtres)
- Delai de réponse des capteur à la base (5 minutes : c'est le délai moyen après lequel l'intru abandonne son effraction).

Bibliographie

[1] DCpj. Traitement ondrp, 2012. http://www.dcpj.fr.

[2] ONDRP. Observatoire national de la délinquance et de la réponse pénale, 2014. http://www.ondrp.fr.

[3] contiki. Contiki, 2015. http://www.contiki-os.org.

[4] A propos de Sigfox. Sigfox, 2015. http://www.sigfox.com/fr.

[5] Witricity. site officiel de witricity, 2015. http://www.witricity.com.