



Rapport Final E-protect

Ilyas BARROUHO
Guillaume VALENTIS
Hugo CHEVALIER
Mathieu DRILLET
Louis GENTIL

Table des matières

1 Naissance d'E-protect :	2
2 Abstract :	3
3 Resume :	4
4 Introduction :	5
5 Requierments / Opportunity :	6
6 Etat de l'art :	7
6.1 Alarme en France :	7
6.2 Alarme à l'Internationale :	10
7 Solutions proposées :	13
7.1 Innovations majeures :	13
7.1.1 Choix du protocole 6LoWPan allégée 96 octets sur UDP (User Datagram Protocol) :	13
7.1.2 Système de Back-up :	13
7.1.3 Sécurisation des données :	14
7.1.4 Alimentation du système :	14
7.1.5 Gérer la consommation du système :	14
7.2 Système d'information	14
7.2.1 Besoins fonctionnels en Front Office	14
7.2.2 Besoins fonctionnels en Back Office	15
8 Solutions proposées détaillées :	16
8.1 Système embarqué	16
8.1.1 Fonctions principales	16
8.1.2 Fonction complémentaires	18
8.2 Système d'information	19
8.2.1 Besoins fonctionnels en Front Office	19
8.2.2 Besoins fonctionnels en Back Office	19
9 Résultats	20
10 Discussion et Analyse :	22
11 Conclusion :	23

CHAPITRE 1

Naissance d'E-protect :

La création d'E-protect nous est venue lors d'un séminaire au Danemark dans la ville d'Aalborg. Nous étions, le reste de l'équipe et moi-même, enivrés dans la folie des nuits danoises, en train d'écumer les bars et pistes de danse de la vieille ville. Après avoir revu l'ensemble de nos pas, nous décidions d'aller à la rencontre des locaux, c'est à ce moment-là que nous rencontrions Torsten. Le regard vide au milieu d'une bande d'amis bien destinés à lui remonter le moral. Une mission qui après quelque verres nous convenait parfaitement.

Nous nous assayâmes un instant autour de sa table et avant même que nous ayons le temps d'entamer les présentations, il coupa "ce soir je bois pour oublier". Oublier quoi ? Oublier le fait qu'il venait de se faire cambrioler et qu'en attendant les résultats de l'enquête il noyait son dégoût dans des boissons énergétiques.

Le lendemain, nous reprenions notre séminaire et la création d'application android et IOS.

C'est alors apparu comme une évidence : Torsten, les applications, E-protect était né.

Nous commençons alors nos recherches. En 2013 il y a eu 382 000 cambriolages et 263 000 incendies domestiques en France. L'importance de développer des solutions innovantes de protections pour lutter contre ces faits est bien réelle.

Pour information, de nos jours l'achat d'une alarme pour le domicile, entraîne l'intervention d'un technicien et si nous souhaitons apporter des modifications à l'installation un deuxième rendez-vous doit être pris. Perte de temps, surplus financier, le client est dépendant du bon vouloir de l'artisanat.

Il s'agit ici d'une intervention sérieuse, nécessitant une forte part de confiance en l'installateur, un inconnu représentant un risque potentiel.

Voici ce que nous proposons et vous recommandons : Un système d'alarme modulable et installable par le client. Une avancée remarquable dans le domaine de la protection. Avec ses caméras destinées à la prévention et une nouvelle génération de capteurs invisibles révisés par un design innovant, le client pourra imaginer avec l'aide de nos conseillers son installation.

Notre offre se décompose en deux parties :

Une partie Hardware avec une centrale d'alarme, sous forme de cadre numérique munie d'une batterie, connecté au réseau EDF et munie d'un système BACKUP (qui permet d'assurer le fonctionnement de l'alarme le temps de prévenir l'utilisateur via SIGFOX) destinée à gérer un parc de capteurs connectés suivant une topologie meshé (ZigBee/Bluetooth Low Energy/CSRmesh). Celle-ci sera connectée à internet via Ethernet ou WIFI et sera capable de communiquer via un protocole de communication sans fil (ex : SIGFOX).

L'alarme interagira aussi avec une partie software (Sigfox/Ethernet). Une application mobile et un site web permettront de se tenir informé de l'état de fonctionnement de l'installation. De plus et cela à n'importe quel moment et où qu'il soit, le client pourra configurer l'alarme à distance via application Android/iOS/Windows Phone (Javascript/PHP/C#/SQL).

CHAPITRE 2

Abstract :

E-protect is a home alarm system connected, easy to install and configure. To propose a least expensive system possible, E-protect is based on the elimination of intermediate and uses a network of smart sensors in a mesh network, playing on the connection of sensors between them. The installation of the E-protect components system is easier than a spun alarm system. No need to punch the walls or install the drivers, which dramatically reduces installation costs.

In Hardware side, an alarm unit manages a fleet of sensors connected with meshed topology (Zig-Bee / Bluetooth Low Energy / CSRMESH). The alarm is deactivated when the customer enters in the house (or through mobile application). The alarm is as unobtrusive as possible and interacted with the software part (SigFox / Ethernet).

A mobile application and website allow to keep the client informed of the alarm's state. In addition the customer can set up the remote alarm (Application Android / iOS / Windows Phone, Javascript / PHP / C # / SQL).

E-protect maintain continuous contact between the client and home.

E-protect system is :

- Smartphone Application to monitor, modify, enable or disable remote system ;
- System Interface ;
- A personalized website with the same Smartphone application function ;
- A backup system in case of failure of the power grid ;
- An innovative and modular sensor design according to customer's will ;
- Very low power consumption, based on a power demand reduced due the use of a meshed network

CHAPITRE 3

Resume :

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 mesh de capteurs intelligent, travaillant sur une portée moins importante jouant ainsi sur la connexion des capteurs entre eux.

L’installation des composants du système E-protect est 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.

Côté Hardware, une centrale d’alarme gère un parc de capteurs connectés suivant une topologie meshé (ZigBee/Bluetooth Low Energy/CSRMesh). L’alarme se désactive lorsque le client entre dans la maison (ou passe par l’application mobile). L’alarme est la plus discrète possible et interagit avec la partie software (Sigfox/Ethernet).

Une application mobile et un site web permettent de se tenir informé de l’état de fonctionnement de l’alarme. De plus le client peut configurer l’alarme à distance (Application Android/iOS/Windows Phone, Javascript/PHP/C#/SQL).

E-protect assure un contact permanent entre le client et le domicile.

Le système E-protect c’est :

- Application Smartphone permettant de surveiller, de modifier, d’activer ou désactiver le système à distance ;
- Interface du système ;
- Un site internet personnalisé au même fonction que l’application Smartphone ;
- 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 meshé

CHAPITRE 4

Introduction :

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. 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 !

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) ; 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.

Certains profitent de cette augmentation d'infractions pour doper le business des alarmes et vendre leur services à des prix exorbitant.

L'importance de développer des solutions de protections défiant les prix actuelles du marché est bien réelle.

La procédure actuelle mobilise beaucoup de temps et représente un investissement financier. 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.[1]

CHAPITRE 5

Requiemments / Opportunity :

En tête du classement des regions les plus touchées par les infractions de domiciles nous retrouvons 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%.^[1]

CHAPITRE 6

Etat de l'art :

6.1 Alarme en France :

Diagral

Diagral, produit de la société Atral, créée en 1985, appartient aujourd'hui au groupe Hager.



FIGURE 6.1 – [2]

Le système Diagral s'appuie sur des alarmes à transmission radio.

Note obtenue dans le comparatif Alarmes de 60 millions de consommateurs : 15.5/20 (site Français spécialiste du marché des alarmes domestiques)

Définition du produit :

- Centrale d'alarme DIAG90AGFK

Différences remarquées en comparaison avec le système E-protect :

- Sirène intégrée
- Annonces vocales
- Division du bâtiment en zone (de 1 à 4) pour adapter les zones à sécuriser
- Communication d'alerte par téléphone en option, via un module de transmission RTC ou GSM

Delta dore



FIGURE 6.2 – [3]

Créée dans les années 70, Delta Dore est une société spécialisée dans les économies d'énergie avant d'élargir son secteur d'activité en intégrant le marché des alarmes sans fils en 2000.

Note obtenue dans le comparatif Alarmes de 60 millions de consommateurs : 12/20 (site Français

spécialiste du marché des alarmes domestiques)

Définition du produit :

- Centrale d’alarme sans fil à transmission radio 868 MHz

Différences remarquées en comparaison avec le système E-protect :

- Sirène intégrée
- Fonctionne sur pile pour éviter les défaut d’alimentation
- Détecteur d’ouverture MICRO COX alimenté par pile
- Module de transmission RTC ou GSM en option

Tag Technologies



FIGURE 6.3 – [4]

PME créée en 2005 à Toulouse, en collaboration avec le CNRS dans le cadre d’un programme de recherche et de développement.

La société est un acteur innovant sur le marché de l’alarme sans fil à travers ses marques Domotag et My-Fox.

Note obtenue dans le comparatif Alarmes de 60 millions de consommateurs : non noté.

Définition du produit :

- Centrale qui se relie à une ligne RTC pour délivrer ses alertes par le réseau IP sous forme d’emails.

Différences remarquées en comparaison avec le système E-protect :

- Télécommande 4 boutons pour piloter le système à distance

mhouse



FIGURE 6.4 – [5]

Filiale du groupe Italien Nice, mhouse propose des systèmes d’alarmes qui se distingue par leur facilité d’installation et d’utilisation grâce à des interfaces intuitives.

Note obtenue dans le comparatif Alarmes de 60 millions de consommateurs : non noté.

Définition du produit :

- Centrale d’alarme avec sirène, synthèse vocale et transmetteur RTC/GSM intégrés.

Différences remarquées en comparaison avec le système E-protect :

- Relié au secteur avec Batterie intégrée
- Communication radio sur les canaux 433 et 868MHz
- Detecteur d'ouverture
- Commande vocale
- Badge transpondeur MAB1

Daitem



FIGURE 6.5 – [6]

Autre marque de la société Atal, marque d'alarme haute gamme, onéreuse, vendu exclusivement auprès d'installateurs. Pas de pack proposé au particulier.

Somfy



FIGURE 6.6 – [7]

Créée dans les années 60 et aujourd'hui cotée en bourse, Somfy est le leader mondial des systèmes d'automatismes d'ouvertures et de fermetures des stores, volets roulant, etc...

Somfy propose aussi des système d'alarme NFA2P.

Note obtenue dans le comparatif Alarmes de 60 millions de consommateurs : 9.5/20.

Définition du produit :

- Centrale d'alarme sans fil.

Différences remarquées en comparaison avec le système E-protect :

- Sirène intégrée
- Ne dispose pas nativement d'éléments de communication
- Module RTC ou GSM en option
- Detecteur d'ouverture à contact magnétique
- Télécommande marche/arrêt

6.2 Alarme à l'Internationale :

Visionic



FIGURE 6.7 – [8]

Société israélienne créée en 1973 faisant aujourd'hui partie du groupe Suisse TYCO, leader mondial des solutions de protections et de sécurité. Seulement disponible auprès de grossiste et des revendeurs spécialisés.

Définition du produit :

- Centrale d'alarme sans fil.

Différences remarquées en comparaison avec le système E-protect :

- Central doté de la technologie PowerG qui simplifie les installations, les économies d'énergie et une liaison sans fil fiable
- Cryptage de type AES

Jablotron



FIGURE 6.8 – [9]

Société Tchèque peu commercialisé en France.

Définition du produit :

- Centrale d'alarme sans fil.

Différences remarquées en comparaison avec le système E-protect :

- Central qui intègre divers protocoles : RTC, GPRS, LAN

Honeywell



FIGURE 6.9 – [10]

Créée dans les années 90, Honeywell conçoit et commercialise aux travers de ses marques Domonial et Ademco des systèmes d'alarme ant-intrusion.
Commercialisation très discrète en France.

Chuanggo



FIGURE 6.10 – [11]

Société Chinoise créée en 2001, Chuango est un des leaders mondial de l'alarme.
Produits peu commercialisés en France.

Définition du produit :

- Centrale d'alarme GSM G5.

Différences remarquées en comparaison avec le système E-protect :

- Aucune fonctions supplémentaires.

Hager



FIGURE 6.11 – [12]

Hager Group a été créée en 1955 intervenant dans l'ingénierie électrique. La firme s'est depuis diversifié et a étendu son activité dans les alarmes pour domicile.

Définition du produit :

- Centrale d'alarme Logisty Serenity.

Différences remarquées en comparaison avec le système E-protect :

- Communication centrale/capteurs assurée par la technologies Twinband
- Pas de fonction de communication téléphonique
- L'ajout d'un module prévoit la transmission d'image

Alarme paradoxe

Société créée en 1989 qui bénéficie d'un large réseau de distributeurs répartis dans une centaine de pays.

Définition du produit :



FIGURE 6.12 – [13]

- Centrale d’alarme Magellan 6250.

Différences remarquées en comparaison avec le système E-protect :

- Central gérant les protocoles GPRS, GSM, RTC et d’un module double SIM
- Communication sans fil fait sur les canaux 868 ou 433MHz

CHAPITRE 7

Solutions proposées :

7.1 Innovations majeures :

7.1.1 Choix du protocole 6LoWPan allégée 96 octets sur UDP (User Datagram Protocol) :

- E-protect travail sur un réseau meshé interne qui ne nécessite pas énormément de données mais suffisamment pour transmettre les données issues des caméras de surveillance.
- Pour toute modification de configuration du système d'alarme, 6LoWPan permet à une machine nouvellement connectée 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'interopérabilité extensive (wifi, ethernet, GPRS, ATM)
 - La sécurité (authentification, pare-feux)
 - Les services réseaux de haut niveau (équilibre de la charge, cache, mobilité, NAT)
 - L'adressage et routage
 - Les services applicatifs de haut niveaux (HTTP,XML,SOAP,REST)
 - Les outils de supervision réseaux
 - Délai de transmission plus court, du à l'utilisation d'un routage Mesh Under (décision de routage fait au niveau du 6 LoWPan et seulement avec les fragments du paquets IPv6 reconstitué uniquement dans l'équipement destinataire)[14]

7.1.2 Système de Back-up :

E-protect assure le fonctionnement du système en cas de coupure de courant en basculant l'installation en fonctionnement Back-up.

Alimentation

L'ensemble du système se place en fonctionnement basse consommation. Seules les fonctions principales restent actives (écran et raspberry se désactivent).

L'alimentation générale se fait par déchargement de batterie assurant le fonctionnement de l'ensemble du système 48h durant. Branché au secteur, la batterie utilisée se charge en fonctionnement normal.

Communication

Utilisation de la communication SigFox (protocole intégré à la base) : permet d'alerter le client en cas de coupure d'électricité ou de connexion internet.

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.

Avantage de ce protocole : SIGFOX est compatible avec les émetteurs-récepteurs existants et activement transféré vers un nombre de plateformes techniques.[15]

7.1.3 Sécurisation des données :

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 sécurité de ses données par l'optimisation du cryptage.

Pour cela l'algorithme AES 128 est utilisé pour sécuriser la couche liaison (MAC). Cet algorithme rend des méthodes de brouillage classique tels que la cryptanalyse linéaire ou différentielle extrêmement difficile.

7.1.4 Alimentation du système :

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 illimitée.
- Conçu avec la spécification Rezenca pour l'électronique grand public. Il fonctionne à 6,78 MHz, une fréquence de fonctionnement qui est adoptée pour les applications électronique grand public. A cette fréquence, conçu pour respecter les limites applicables d'exposition humaine, l'interaction avec des corps étrangers métalliques est minimale.
- 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).[16]

7.1.5 Gérer la consommation du système :

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'appels de puissance.

7.2 Système d'information

7.2.1 Besoins fonctionnels en Front Office

Notre site web a 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.

7.2.2 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 perdue, contrairement aux simples requêtes http.

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

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

CHAPITRE 8

Solutions proposées détaillées :

8.1 Système embarqué

8.1.1 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 connectée 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'interopérabilité extensive (wifi, ethernet, GPRS, ATM), la sécurité (authentification, pare-feux), les services réseaux de haut niveau (équilibre 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.[?]

Le choix du protocole 6LoWPan se définit autour de plusieurs points clés.

E-protect travaille sur un réseau meshé interne qui ne nécessite pas énormément de données mais suffisamment pour transmettre les données issues des caméras de surveillance. Nous obtenons 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.[?]

Communication serveur

La connexion serveur est assurée par le protocole TCP, protocole plus orienté « connexion » afin de répondre aux exigences de sécurité 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 petits 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.[?]

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...)
- Accès 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'installation en fonctionnement Back-up.

L'ensemble du système se place en fonctionnement basse consommation. Seules les fonctions principales restent actives (écran et raspberry 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 contrôle. L'alimentation générale se fait par déchargement de batterie assurant le fonctionnement de l'ensemble du système 48h durant. Branché au secteur, la batterie utilisée 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 ISM 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.[15]

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 sécurité 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 extrêmement difficile.[?]

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.[15]

8.1.2 Fonction complémentaires

Alimenter le système

Le système E-protect propose deux systèmes d'alimentations électriques **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 a une durée de vie illimitée.

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).[16]

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'appels 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'intrus potentiel puisse les voir à l'intérieur (fenêtre, porte vitrée, etc...) comme à l'extérieur 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.

8.2 Système d'information

8.2.1 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.

8.2.2 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 perdue, contrairement aux simples requetes http.

Le framework, sailsjs, ne pouvant pas gérer les sockets tcp (ceux utilisé par la raspberrypi) nous obtenons 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 téléphonique.

CHAPITRE 9

Résultats

Après avoir analysé et pris en compte les critères suivant :

- 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.
- Nécessité 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)
- Délai de réponse des capteur à la base (5 minutes : c'est le délai moyen après lequel l'intrus abandonne son effraction).

Nous avons créé un système E-protect décomposable en deux parties, Hardware et Software assurant à ce jour les fonctions suivantes :

- Interactions de différents type de capteurs, de chocs, de mouvements et caméra géré par une base ;
- 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.
- Accès à une page internet personnalisée en connexion constante avec le système E-protect

Du coté Hardware la centrale assure la communication inter-capteur par le protocole 6LoWPan allégé 96 octets du standard IEEE 802.15.4. présentant les avantages suivant :

- 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

) Dans un souci de surveillance informatique, E-protect assure une communication permanente entre les capteurs et la base.

Ce monitoring s'articule autour du protocole 6LoWPan dans un échange de données 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).

Comme dit précédemment elle-ci interagit avec la partie Software en s'appuyant sur le protocole Sigfox, assurant la communication utilisateur et présentant un gage de sécurité supplémentaire. 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 sécurité de ses données par l'optimisation du cryptage. Pour cela l'algorithme AES 128 est utilisé pour sécuriser la couche liaison (MAC).

Le base E-protect se branche simplement au secteur respectant les normes Européenne.

CHAPITRE 10

Discussion et Analyse :

“La liberté au service de l’innovation”

Le choix de la valorisation concours répond à différentes envies de notre part. Le fait de pouvoir challenger notre travail nous pousse à être meilleur, à créer, innover, à trouver ce qui peut faire la différence.

La voie choisie fut l’innovation. Nous avons compris que nous ne pourrions pas rivaliser avec les industriels bien en place sur le marché et sur des techniques et architectures utilisés concernant leur produit. Pour exister il fallait apporter quelque chose de nouveau, c’est ce qui nous poussa à choisir cette valorisation.

Le concours nous permet de réinventer totalement les produits en place, les repenser, repartir à zéro et laisser place à une imagination totale. Contrairement aux autres valorisations, notre marge de manoeuvre est totale, nous sommes seul maître de notre projet et pouvons lui donner quand bon nous semble la direction que nous souhaitons. Nous fixons les priorités et la marche à suivre. Cette ambiance de travail est jouissive et permet à l’ensemble de l’équipe de participer et de s’épanouir pleinement.

CHAPITRE 11

Conclusion :

Après 2 mois de travaux, notre système répond entièrement au cahier des charges. De nombreux test ont été réalisé, le produit est finis et peut dès à présent être commercialisé. De part son architecture, la topologie, l'hardware, le software utilisé et son coût E-protect défie toute concurrence sur le marché de la sécurité de domicile.

- [1] ONDRP. Observatoire national de la délinquance et de la réponse pénale, 2014. <http://www.ondrp.fr>.
- [2] Diagral. Diagral logo, 2015. <http://www.diagral.fr>.
- [3] Deltadore. Deltadore logo, 2015. <http://www.deltadore.fr>.
- [4] Tag. Tag logo, 2015. <http://www.tag.fr>.
- [5] mhouse. mhouse logo, 2015. <http://www.mhouse.fr>.
- [6] Daitem. Daitem logo, 2015. <http://www.daitem.fr>.
- [7] Somfy. Somfy logo, 2015. <http://www.somfy.fr>.
- [8] Visionic. Visionic logo, 2015. <http://www.visionic.com>.
- [9] Jablotron. Jablotron logo, 2015. <http://www.jablotron.com>.
- [10] Honeywell. Honeywell logo, 2015. <http://www.honeywell.com>.
- [11] Chuango. Chuango, 2015. <http://www.chuango.com>.
- [12] Hager. Hager logo, 2015. <http://www.hagerlogo>.
- [13] Alarme Paradoxe. Alarme paradoxe logo, 2015. <http://www.alarmeparadoxe.com>.
- [14] Contiki. Contiki, 2015. <http://www.contiki-os.org>.
- [15] A propos de Sigfox. Sigfox, 2015. <http://www.sigfox.com/fr>.
- [16] Site officiel de Witricity. Witricity, 2015. <http://www.witricity.com>.