ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) BREVET D'INVENTION

(11) N° de publication :
MA 55847 A1

(51) Cl. internationale :
H04W 12/00

(43) Date de publication :
27.09.2023

(21) N° Dépôt :
55847

(22) Date de Dépôt :
23.02.2022

(71) Demandeur(s) :
- **Ecole Marocaine des sciences de l'Ingenieur EMSI, EMSI, CASABLANCA, 20000 CASABLANCA (MA)**
- **HAMMACH Oussama, massira 1, hay el firdaws, imm 1, app 10, 12020 Temara (MA)**

(72) Inventeur(s) :
Merzouk Safae ; EL BHIRI Brahim ; Charadi Ssadik ; HAMMACH Oussama

(74) Mandataire :
EL Bhiri Brahim

(54) Titre : **Système Intelligent de Prévention contre le Replay Attack SIP-RA**

(57) Abrégé : De nos jours, les objets connectés sont omniprésents et vont forcément nécessiter une attention tout particulière quant à la protection des données personnelles. L'invention que nous présentons ici est un nouveau système de transmission sécurisé pour les dispositifs fonctionnant avec des fréquences (clés de : véhicules, garages, ou autres). Il est Constitué principalement des composantes permettant la synchronisation du périphérique émetteur avec son homologue récepteur. Le système comporte également un module de chiffrage des codes obtenus après la synchronisation. Ces codes chiffrés vont être transmis dans deux canaux sécurisés et seront valables seulement pour une très courte durée bien déterminée, pour éviter toute tentative d'attaque. Après réception du code, il sera comparé suivant les mêmes paramètres faits par le transmetteur pour confirmer ou rejeter sa validation.

Abrégé

De nos jours, les objets connectés sont omniprésents et vont forcément nécessiter une attention tout particulière quant à la protection des données personnelles. L'invention que nous présentons ici est un nouveau système de transmission sécurisé pour les dispositifs fonctionnant avec des fréquences (clés de : véhicules, garages, ou autres). Il est Constitué principalement des composantes permettant la synchronisation du périphérique émetteur avec son homologue récepteur. Le système comporte également un module de chiffrage des codes obtenus après la synchronisation. Ces codes chiffrés vont être transmis dans deux canaux sécurisés et seront valables seulement pour une très courte durée bien déterminée, pour éviter toute tentative d'attaque. Après réception du code, il sera comparé suivant les mêmes paramètres faits par le transmetteur pour confirmer ou rejeter sa validation.

MA 55847A1

Système Intelligent de Prévention contre le Replay Attack « SIP-RA »

1) Domaine de l'invention

Le domaine principal de l'invention est la cybersécurité. Plus précisément, l'invention concerne une solution pour la prévention contre le Replay Attack (l'attaque par rejeu) qui est une forme d'attaque réseau dans laquelle une transmission est répétée d'une manière malicieuse par un agresseur qui a capturé la transmission.

2) État de la technique

Ces dernières années, les systèmes de transmission sont devenus très fréquents dans notre environnement. D'où l'intérêt de protéger un tel système contre toute attaque. Actuellement, plusieurs systèmes de transmission RF sont utilisés à savoir le code fix RF,le Rolling Code, ou encore frequency Hopping. Ces méthodes de transmission présentent plusieurs vulnérabilités permettant aux attaquants d'accéder au code par replay attack. Notre invention exposée ici vient pour corriger les fragilités dans les systèmes existants.

3) Objectifs de l'invention

L'invention que nous proposons ici est une solution visant à protéger les systèmes fonctionnant avec des fréquences de toute les vulnérabilités et les failles qui existent jusqu'à maintenant dans les systèmes de transmission RF.

En utilisant notre technique, chaque signal généré va avoir un code unique qui ne peu jamais se répéter après qu'il soit expiré au bout d'une très courte durée estimée à quelques fractions de seconde. Lorsque l'utilisateur clique sur le bouton d'ouverture, un système implémenté se charge de calculer le temps, le crypter, l'ajouter à un code et l'envoyer sous forme d'un signal unique crypté qui s'expire au bout de quelques fractions de seconde. D'un autre coté le temps va toujours être synchronisé entre le récepteur et l'émetteur pour éviter le décalage temporel.

4) Exposé de l'invention

L'invention est capable de réaliser les objectifs cités précédemment à travers deux composants essentiels à savoir un système émetteur et un système récepteur. Ceci est via un protocole respectant trois étapes. Premièrement, la synchronisation du temps et le cryptage du code à envoyer par l'émetteur. Deuxièmement, la transmission du signal via deux canaux sécurisés de l'émetteur vers le récepteur. La dernière étape c'est la comparaison du temps et du code transmis entre émetteur et récepteur.

5) Liste des figures

Figure 1 : Protocole général de la solution SIP-RA

Figure 2 : Etape de synchronisation et de chiffrage

Figure 3 : Etape de transmission du code/temps

Figure 4 : Etape de comparaison et vérification du code/temps transmis

6) Description détaillée

6.1. Synchronisation et chiffrage

Notre dispositif émetteur est équipé d'une horloge temps réel (HTR) permettant un décompte très précis du temps d'une manière qu'il soit synchronisé avec le dispositif récepteur. Chacun des dispositifs est doté d'un propre code d'une taille précise auquel s'ajoute le temps réel

synchronisé auparavant. La combinaison entre le temps synchronisé et le code du système, donne naissance à un code final qui va être chiffré par la suite suivant une fonction de hachage. (Figure2)

6.2.transmission du code/temps

Le code chiffré obtenu par le dispositif émetteur, sera converti en format adéquat pour qu'il puisse être envoyé selon une fréquence bien déterminée en utilisant des canaux de transmission. Les bits constituant le code seront divisés sur les canaux selon un protocole spécifié. Le dispositif récepteur va recevoir le code du même format de l'envoi en provenance des canaux, puis il va les rassembler pour avoir un seul code qui sera converti pour obtenir le code original chiffré qui a été calculé précédemment par le dispositif émetteur. (Figure 3)

6.3.comparaison et vérification du code/temps transmis

Le code final chiffré et envoyé par le dispositif émetteur va être vérifié et comparé par le dispositif récepteur avec le code recalculé par le dispositif récepteur, suivant les mêmes paramètres utilisés dans la première étape par le dispositif émetteur.

Le code obtenu est considéré obsolète si le résultat de la comparaison indique que les deux codes sont différents. Chaque code envoyé par le dispositif émetteur s'expire au bout de quelques fractions de seconde, après le code devient obsolète et inutile.

Revendications

1- Le système inventé est une solution intelligente constitué de deux dispositifs émetteur/récepteur connectés sans fil ou par autres moyens de connexion via des canaux fiables et sécurisés, permettant la prévention contre le Replay Attack ou autres. Ce système peut être exploité par tout dispositif fonctionnant avec des fréquences et utilisé par des particuliers ou des organismes du domaine (Figure 1).

2- Système selon la revendication 1, est caractérisé de ce qu'il est constitué d'un dispositif émetteur contenant une horloge temps réel pour la synchronisation avec le récepteur afin de créer un code propre et unique s'ajoutant à un code du système afin de former un code final qui va être chiffré.

3- Système, selon les revendications 1 et 2, est caractérisé de ce qu'il est constitué d'un système de transmission fiable et sécurisé via des canaux selon un protocole spécifié afin de permettre une communication sécurisée entre les dispositifs émetteur et récepteur.

4- Système suivant les revendications 1 ,2 et 3 est caractérisé en ce qu'il est constitué d'un dispositif récepteur capable de reconnaitre le code envoyé et chiffré suivant le même protocole adopté par l'émetteur.

5- Système suivant les revendications 1 et 4 est caractérisé en ce qu'il est capable de comparer les codes de l'émetteur et du récepteur via un système adéquat, de rejeter ou accepter la communication.

6- Système suivant la revendication 5 est caractérisé de ce qu'il est capable de considérer obsolète tout code non authentique.

7- Système suivant la revendication 5 est caractérisé de ce qu'il est capable de considérer obsolète tout code non utilisé au bout de quelques fractions de secondes via un système de contrôle adéquat afin de prévenir toutes tentatives d'accès au code, réception du code, modification non autorisé du code ou autres.

Figures

Figure 1

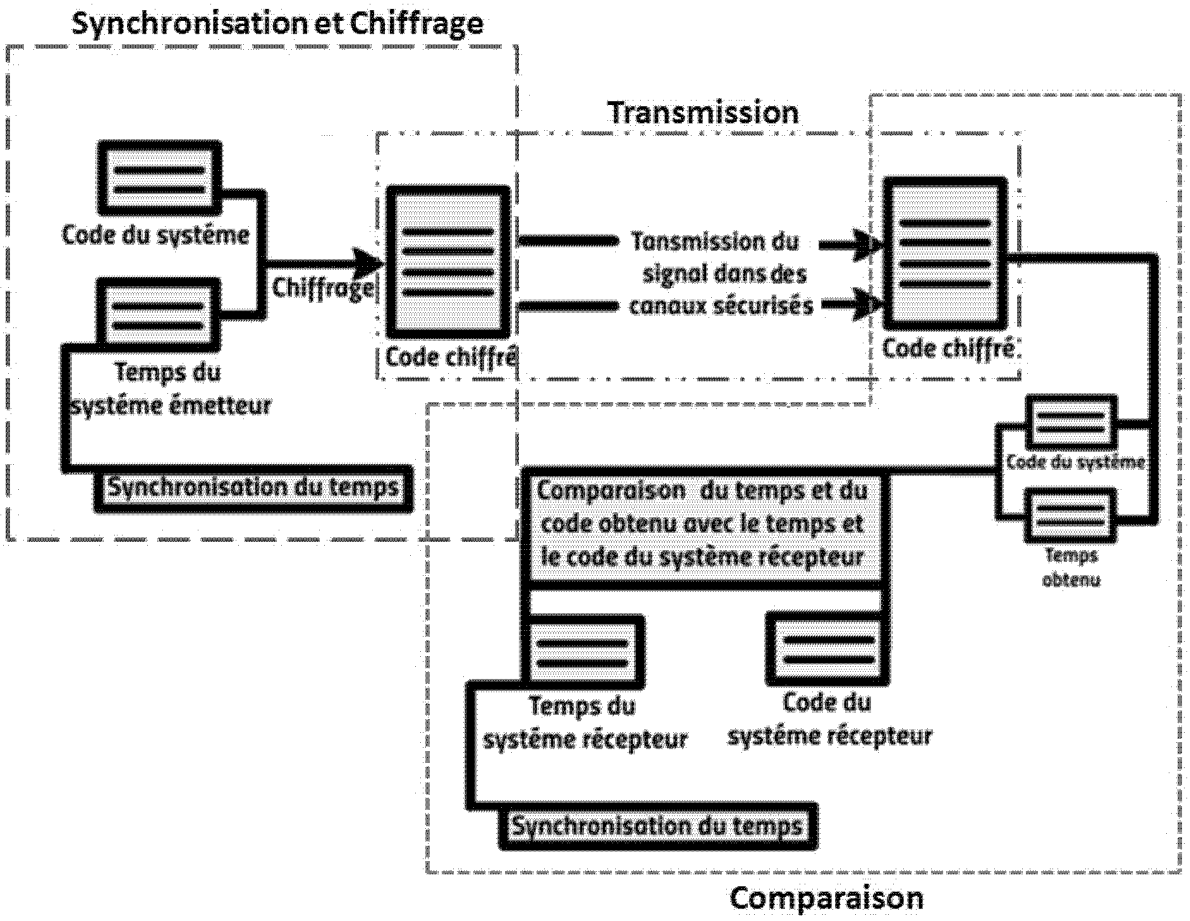


Figure 2

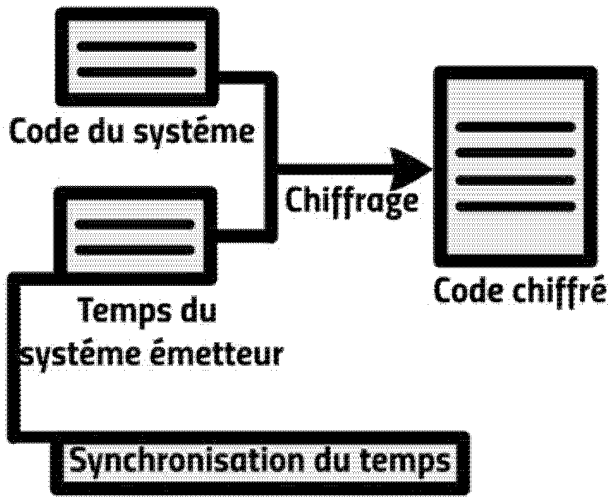
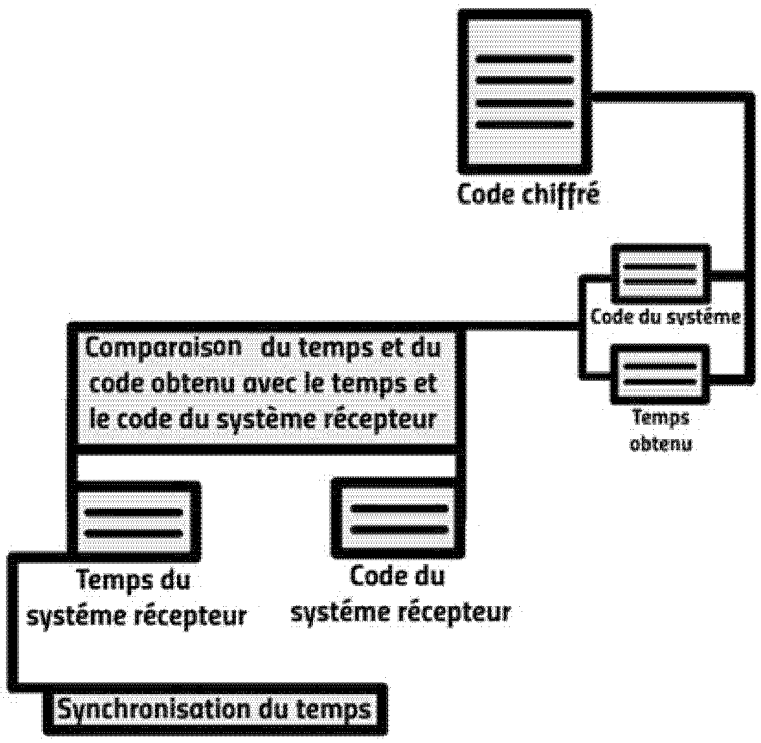


Figure 3

Figure 4


Code chiffré
Code du système
Temps obtenu
Comparaison du temps et du code obtenu avec le temps et le code du système récepteur
Temps du système récepteur
Code du système récepteur
Synchronisation du temps

MA 55847A1

ROYAUME DU MAROC
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE

OMPIC

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 55847	Date de dépôt : 23/02/2022
Déposant : Ecole Marocaine des sciences de l'Ingénieur EMSI et HAMMACH Oussama	
Intitulé de l'invention : Système Intelligent de Prévention contre le Replay Attack SIP-RA	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 05/09/2022
Téléphone: 212 5 22 58 64 14/00	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  8 Pages
- Revendications
  1-7
- Planches de dessin
  3 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04W12/00
CPC : H04W12/00

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, IEEE, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	US8615265B2 ; Assets Net LLC ; 24/12/2013	1-7
X	CN102739659B ; South China Normal University GCI Science and Technology Co Ltd ; 08/07/2015	1-7

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de forme et de clarté

La revendication 1 n'est pas rédigée en deux partie, de sortie que le préambule spécifie l'état de la technique le plus proche, et la partie caractérisante indique les caractéristiques distinctives de la présente invention.

La revendication 1 ne contient pas toutes les caractéristiques essentielles à la définition de l'invention.

Par conséquent, l'objet des revendications 1-7 manque de clarté au sens de l'article 35 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications aucune Revendications 1-7	Oui Non
Activité inventive	Revendications aucune Revendications 1-7	Oui Non
Application Industrielle	Revendications 1-7 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : US8615265B2

1. Nouveauté

Le document D1 divulgue un système constitué de deux dispositifs émetteur/récepteur sans fils permettant la prévention contre le Replay Attack, caractérisé en ce que le dispositif émetteur contient une horloge temps réel pour la synchronisation avec la réception afin de créer un code propre et unique s'ajoutant à un code du système afin de former un code final qui va être chiffré.

L'objet des revendications 1-7 manque de nouveauté au sens de l'article 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. Activité inventive

L'objet des revendications 1-7 n'est pas nouveau et n'implique donc pas une activité inventive au sens de l'article 28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. Application industrielle

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.