УКРАЇНА

(19) UA (11) 110241 (13) U

(51) МПК (2016.01)
B60R 25/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: u 2016 05940

(22) Дата подання заявки: 01.06.2016

(24) Дата, з якої є чинними права на корисну модель: 26.09.2016

(46) Публікація відомостей про видачу патенту: 26.09.2016, Бюл.№ 18

(72) Винахідник(и):
Черниш Сергій Кимович (UA)

(73) Власник(и):
Черниш Сергій Кимович,
вул. Семінарська, 143, м. Харків, 61039 (UA)

(54) ДІАЛОГОВИЙ СПОСІБ ІДЕНТИФІКАЦІЇ БРЕЛОКА ДВОСТОРОННЬОЮ АВТОМОБІЛЬНОЮ ОХОРОННОЮ СИСТЕМОЮ "SL"

(57) Реферат:

Діалоговий спосіб ідентифікації брелока двосторонньою автомобільною охоронною системою включає двосторонній зв'язок брелока із системним блоком, під час якого, натискаючи на одну з кнопок брелока, відправляють повідомлення у закодованому вигляді із заданою командою до системного блока на визначеній частоті передачі, де за допомогою системи виконують дії по його декодуванню. При успішному декодуванні повідомлення, перевіряють правильність надісланої відповіді, якщо відповідь правильна, ідентифікують брелок як "свій" та виконують відповідну команду, про що відправляють повідомлення брелоку, де ініціюють виконання команди на дисплеї брелока. Якщо відповідь неправильна, ідентифікують брелок як "чужий" і процес діалогу припиняють. Також у випадку неможливості декодування повідомлення процес діалогу припиняють. Натискають на одну з кнопок брелока, направляють на частоті передачі, заданої випадковим чином з 512 можливих варіантів у дозволеному діапазоні 433,05-433,79 МГц, до системного блока повідомлення із запитанням та відповідною командою, яке кодують, використовуючи генератор випадкових чисел. У системному блоці повідомлення декодують і при успішному декодуванні створюють випадкову композицію із згаданим повідомленням на брелок, де його декодують і виконують хешування за попередньо визначеною формулою із застосуванням 128-битного ключа шифрування. Отриманий результат повертають системі на одній із щонайменше трьох частот дозволеного діапазону, заданих випадковим чином. На двох інших частотах відправляють результат хешування з похибкою із збереженням розрядності, де його декодують. При успішному декодуванні повідомлення перевіряють правильність відповіді шляхом порівнювання з одночасно виконуваним у системі хешуванням із застосуванням 128-битного ключа шифрування. Якщо відповідь вірна - результати обчислень у системі і у брелоку співпадають, - ідентифікують брелок, як "свій" і виконують відповідну команду, про що відправляють повідомлення брелоку, який ініціює виконання команди на своєму дисплеї, а при неможливості декодування повідомлення процес діалогу між брелоком і системою припиняють.

UA 110241 U

Корисна модель належить до техніки захисту транспортних засобів від несанкціонованого використання і може бути застосована для захисту від електронного злому двосторонніх автомобільних охоронних систем.

Найближчим аналогом до корисної моделі є діалоговий спосіб ідентифікації брелока двосторонньою автомобільною охоронною системою, що включає двосторонній зв'язок брелока із системним блоком, під час якого, натискаючи на одну з кнопок брелока, відправляють повідомлення у закодованому вигляді із заданою командою до системного блока на визначеній частоті передачі, де за допомогою системи виконують дії по його декодуванню, при успішному декодуванні повідомлення, перевіряють правильність надісланої відповіді, якщо відповідь правильна, ідентифікують брелок як "свій" та виконують відповідну команду, про що відправляють повідомлення брелоку, де ініціюють виконання команди на дисплеї брелока, якщо відповідь неправильна, ідентифікують брелок як "чужий" і процес діалогу припиняють, також у випадку неможливості декодування повідомлення процес діалогу припиняють [Патент на корисну модель № 48425, Україна, МПК (2009) B60R 25/00, опубліковано 10.03.2010, бюл. № 5/2010].

Найближчий аналог не забезпечує достатньо надійного захисту від несанкціонованого перехвату з можливістю наступного кодування-декодування отриманих чужою системою (грабером) даних через застосування у згаданій системі лише одного частотного каналу для прийому-передачі даних.

В основу корисної моделі поставлена задача створення такого способу ідентифікації брелока двосторонньою автомобільною охоронною системою, який би дозволив підвищити її захищеність від несанкціонованого перехвату за рахунок застосування одночасно щонайменше трьох каналів, один з яких призначений для передачі повідомлення з певною командою, а два інших - для передачі інформації з похибкою, що суттєво зменшує вірогідність злому двосторонньої автомобільної охоронної системи.

Поставлена задача вирішується тим, що діалоговий спосіб ідентифікації брелока двосторонньою автомобільною охоронною системою, включає двосторонній зв'язок брелока із системним блоком, під час якого, натискаючи на одну з кнопок брелока, відправляють повідомлення у закодованому вигляді із заданою командою до системного блока на визначеній частоті передачі, де за допомогою системи виконують дії по його декодуванню. При успішному декодуванні повідомлення, перевіряють правильність надісланої відповіді. Якщо відповідь правильна, ідентифікують брелок як "свій" та виконують відповідну команду, про що відправляють повідомлення брелоку, де ініціюють виконання команди на дисплеї брелока. Якщо відповідь неправильна, ідентифікують брелок як "чужий" і процес діалогу припиняють. Також у випадку неможливості декодування повідомлення процес діалогу припиняють, згідно з корисною моделлю, натискають на одну з кнопок брелока, направляють на частоті передачі, заданої випадковим чином з 512 можливих варіантів у дозволеному діапазоні 433,05-433,79 МГц, до системного блока повідомлення із запитанням та відповідною командою, яке кодують, використовуючи генератор випадкових чисел. У системному блоці повідомлення декодують і при успішному декодуванні створюють випадкову композицію із згаданим повідомленням на брелок, де його декодують і виконують хешування за попередньо визначеною формулою із застосуванням 128-битного ключа шифрування. Отриманий результат повертають системі на одній із щонайменше з трьох частот дозволеного діапазону, заданих випадковим чином, а на двох інших частотах відправляють результат хешування з похибкою із збереженням розрядності, де його декодують і при успішному декодуванні повідомлення перевіряють правильність відповіді шляхом порівнювання з одночасно виконуваним у системі хешуванням із застосуванням 128-битного ключа шифрування. Якщо відповідь вірна - результати обчислень у системі і у брелоку співпадають, - ідентифікують брелок, як "свій" і виконують відповідну команду, про що відправляють повідомлення брелоку, який ініціює виконання команди на своєму дисплеї. При неможливості декодування повідомлення процес діалогу між брелоком і системою припиняють.

Корисна модель дозволяє збільшити можливості для використання сучасних інформаційних технологій для підвищення ефективності боротьби із спробами несанкціонованого використання транспортних засобів за рахунок створення умов для застосування одночасно щонайменше трьох каналів, один з яких призначений для передачі повідомлення з певною командою, а два інших - для передачі інформації з похибкою.

Застосуванням саме 128-битного ключа шифрування обумовлене "спробою оптимально підвищити рівень захисту та врівноважити швидкість відклику системи на запити".

Частоту передачі задають випадковим чином з 512 можливих варіантів, для уникнення закономірності, що ускладнює процес незаконного перехвату даних.

Приклад.

Двостороння автомобільна охоронна система "SL", складається з двох основних модулів - системного процесорного стаціонарного блока, який встановлений у транспортному засобі, та мобільного модуля керування - брелока, призначеного для зберігання у водія транспортного засобу. Як системний процесорний стаціонарний блок може бути використаний центральний блок сигналізації на базі ARM - процесора. Як брелок використали брелок на базі ARM - процесора. Зв'язок між цими пристроями здійснюється по радіоканалу, який забезпечує двосторонній зв'язок брелока із системним блоком. Система може включати гальванічно з'єднані модуль управління; прийомопередаючу антену двостороннього зв'язку з функцією подання виклику на брелок-передавач зі світлодіодним індикатором стану; брелок-передавач з визначеним кодом; перемикач та реле блокування. Брелок-передавач має функції, визначені відповідними кнопками - постановки системи на охорону; зняття системи з охорони; управління програмованим каналом; включення режиму "пошук автомобіля"; перевірки стану автомобіля.

Натискаючи на одну з кнопок брелока, направляють на частоті передачі, заданої випадковим чином з 512 можливих варіантів у дозволеному діапазоні 433,05-433,79 МГц, до системного блока повідомлення із запитанням та відповідною командою. Згадане повідомлення кодують, використовуючи генератор випадкових чисел, що входить до складу системного процесорного стаціонарного блока. Як генератор випадкових чисел може бути використаний фізичний генератор випадкових чисел на основі істинних чисел. Повідомлення з брелока у кодованому вигляді надходить до системного блока, де його декодують, і при успішному декодуванні створюють випадкову композицію із згаданим повідомленням на брелок. У системі може бути використане динамічне кодування. У брелоку випадкову композицію із згаданим повідомленням декодують і виконують хешування за попередньо визначеною формулою із застосуванням 128-битного ключа шифрування. Отриманий результат повертають системі на одній із трьох частот, що входять до дозволеного діапазону, заданих випадковим чином, а на двох інших частотах відправляють результат хешування з похибкою із збереженням розрядності. Згадане повідомлення (результат хешування з похибкою) декодують у системі і при успішному декодуванні повідомлення перевіряють правильність відповіді шляхом порівнювання з одночасно виконуваним у системі хешуванням із застосуванням 128-битного ключа шифрування. Якщо відповідь вірна - результати обчислень у системі і у брелоку співпадають і брелок ідентифікують як "свій" та виконують відповідну команду, про що відправляють повідомлення брелоку. При цьому брелок ініціює виконання команди на своєму дисплеї. У випадку неможливості декодування повідомлення процес діалогу між брелоком і системою припиняють. Завдяки використанню трьох каналів, один з яких призначений для передачі повідомлення з певною командою, а два інших - для передачі інформації з похибкою, пропонований спосіб дозволив суттєво зменшити вірогідність злому двосторонньої автомобільної охоронної системи.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Діалоговий спосіб ідентифікації брелока двосторонньою автомобільною охоронною системою, що включає двосторонній зв'язок брелока із системним блоком, під час якого, натискаючи на одну з кнопок брелока, відправляють повідомлення у закодованому вигляді із заданою командою до системного блока на визначеній частоті передачі, де за допомогою системи виконують дії по його декодуванню, при успішному декодуванні повідомлення, перевіряють правильність надісланої відповіді, якщо відповідь правильна, ідентифікують брелок як "свій" та виконують відповідну команду, про що відправляють повідомлення брелоку, де ініціюють виконання команди на дисплеї брелока, якщо відповідь неправильна, ідентифікують брелок як "чужий" і процес діалогу припиняють, також у випадку неможливості декодування повідомлення процес діалогу припиняють, який **відрізняється** тим, що натискають на одну з кнопок брелока, направляють на частоті передачі, заданої випадковим чином з 512 можливих варіантів у дозволеному діапазоні 433,05-433,79 МГц, до системного блока повідомлення із запитанням та відповідною командою, яке кодують, використовуючи генератор випадкових чисел, а у системному блоці повідомлення декодують і при успішному декодуванні створюють випадкову композицію із згаданим повідомленням на брелок, де його декодують і виконують хешування за попередньо визначеною формулою із застосуванням 128-битного ключа шифрування, отриманий результат повертають системі на одній із щонайменше з трьох частот дозволеного діапазону, заданих випадковим чином, а на двох інших частотах відправляють результат хешування з похибкою із збереженням розрядності, де його декодують і при успішному декодуванні повідомлення перевіряють правильність відповіді шляхом порівнювання з

одночасно виконуваним у системі хешуванням із застосуванням 128-битного ключа шифрування, якщо відповідь вірна - результати обчислень у системі і у брелоку співпадають, - ідентифікують брелок, як "свій" і виконують відповідну команду, про що відправляють повідомлення брелоку, який ініціює виконання команди на своєму дисплеї, а при неможливості декодування повідомлення процес діалогу між брелоком і системою припиняють.

Комп'ютерна верстка Д. Шеверун

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601