https://doi.org/10.17979/spudc.9788497498081.0863

Control de acceso electrónico de cerraduras de barrera basado en WPA para dispositivos móviles

Miguel Díaz-Cacho Medina[1], Alfonso Trigo Raposo[2], Emma Delgado Romero[1] y Matías García Rivera[1]

[1]Dept.Ing.Sistemas y Automática, Universidad de Vigo, España *
[2]Electronics and ITS Division, Centro Tecnológico del Automóvil (CTAG), Vigo, España **

Resumen

Este trabajo presenta un sistema de acceso mediante llave electrónica instalado en dispositivos móviles como los teléfonos inteligentes, probado sobre un prototipo de barrera de apertura para el acceso de vehículos. El sistema presentado utiliza seguridad basada en WPA y optimización de consumo energético basada en una solución híbrida que combina un detector de presencia, un enlace Bluetooth para la activación del dispositivo móvil y la autenticación a través de Wifi-WPA. Las pruebas realizadas muestran la viabilidad del sistema en lo que a seguridad y minimización del consumo sobre el dispositivo móvil se refiere.

Palabras clave: Apertura electrónica, Llave electrónica, WPA, Wifi, Bluetooth, PIR.

1. Introducción

Este artículo presenta un sistema seguro de apertura automática a distancia para accesos a garages o aparcamientos utilizando seguridad WPA. Aunque el sistema presentado está enfocado a ser implementado sobre vehículos y sistemas de llave/cerradura (o key/lock en inglés) de puertas de garage o barreras, este es lo suficientemente amplio como para poder sustituir a cualquier sistema llave/cerradura en entornos corporativos o domésticos. Las ventajas de un sistema de apertura electrónica, además de la comodidad, está en la seguridad y la gestión. La seguridad viene dada al poder usarse algoritmos de encriptación y transmisión de claves altamente seguros y suficientemente probados. Por otro lado, la gestión permite una administración rápida, sencilla y eficaz de altas, bajas, seguimientos, cesión temporal de llaves y control por dispositivos, posibilidad de definición de perfiles, de grupos de cerraduras, de grupos de usuarios, así como el mantenimiento de históricos y la resolución de problemas de forma remota.

Existen dos líneas básicas de sistemas llave/cerradura electrónica: los sistemas con reconocimiento automático de permiso de acceso (están bastante desarrollados sistemas biométricos por reconocimiento de iris y huella dactilar, o sistemas de reconocimiento automático de matrículas) y los sistemas de llave remota donde el permiso de acceso va asociado a la posesión de una llave electrónica en forma de mando a distancia o tarjeta que transmiten una clave por radiofrecuencia. Pueden destacarse algunas tecnologías actualmente implementadas:

- Apertura por parámetros biométricos. El sistema es muy parecido al sistema de llave mecánica tradicional, con la salvedad de que la llave está incluida en la biología del usuario (huellas dactilares, iris, etc). Su implementación requiere de dispositivos lectores especiales y la seguridad es muy alta, dependiendo de la facilidad de que un intruso pueda falsear o copiar alguno de los parámetros biométricos.

- Apertura por reconocimiento automático de matrículas (Automatic number plate recognition - ANPR) [1] utilizado en accesos a lugares oficiales, puertos o parkings. Su uso requiere la instalación de un dispositivo reconocedor, cada vez mas económico e incluso implementable con tarjetas controladoras como Raspberry Pi o Arduino que incluyan una cámara y un software de tratamiento de imágenes. Estos sistemas no precisan de un soporte físico para la llave. La seguridad es muy baja, pudiendose saltar con una simple falsificación de matrícula.

- Remote keyless system (RKS) es un sistema de cerradura electrónica que controla el acceso a vehículos o edificios sin necesidad de una llave mecánica. Habitualmente está asociado a un dispositivo inalámbrico (llave) que activa por pulsación, entrada de código o por proximidad, un dispositivo fijo asociado a una cerradura. Donde mas se usa es en automóviles. Un RKS dispone de un radio-transmisor de baja potencia (habitualmente en rangos de 5 a 20 metros) que envía un código a un receptor que activa o desactiva una cerradura. La seguridad de estos sistemas puede romperse

*mcacho,emmad,mgrivera@uvigo.es
**alfonso.trigo@ctag.com

con relativa sencillez [2].

- Apertura por RFID (RFID Door Lock) [3]. La tecnología RFID es una de las mas utilizadas en sistemas de llave inteligente, pues funciona como el sistema tradicional de llaves mecánicas, solo que en este caso la tarjeta RFID (Llave) tiene que acercarse a unos 20cm del transmisor RFID de la cerradura produciendo su apertura. La diferencia entre una llave y otra está en el identificador ID incluido en la tarjeta. En algunos casos se utilizan tarjetas RFID activas para que activen la apertura a mayores distancias, como en los sistemas de telepeaje.
- Apertura por Bluetooth (Bluetooth Door Lock) [4]. Estos sistemas utilizan interconectividad Bluetooth para la transmisión de una clave que permite la apertura de la cerradura. La cerradura suele ser el dispositivo servidor y la llave el dispositivo cliente. Este sistema obliga al desarrollo de algoritmos de encriptación y transmisión de claves específicos.

Muchos de estos sistemas llave/cerradura requieren de una tecnología muy específica, como los accesos por reconocimiento de matrículas, los accesos por RFID o sobre todo los accesos por parámetros biométricos. En cualquiera de estos casos, el despliegue generalizado y el mantenimiento de estos sistemas está fuera del alcance de edificios, viviendas o muchos organismos.

El sistema presentado en este artículo utiliza tecnologías abiertas y está enfocado al uso de un dispositivo de telefonía móvil como llave. Se ha encontrado en la literatura algún sistema que ya utiliza los dispositivos móviles para la apertura de puertas [5] [6], pero ninguno de ellos ha buscado la optimización del compromiso entre seguridad y consumo energético utilizando tecnologías ya disponibles.

El sistema se centra en dos aspectos fundamentales: el primero es el de la seguridad y el segundo, surgido a raíz de las tecnologías móviles empleadas, el del consumo energético.

1.1. Seguridad

El sistema de seguridad propuesto es el de transmisión de clave por WPA (Wifi Protected Access) existente en la práctica totalidad de dispositivos con conectividad 802.11 Wifi. Se utilizaría con el modo de operación Wifi *infraestructure*, donde la cerradura implementa el AP y la llave el cliente. WPA permite la transmisión de una clave estática (Personal Mode) o de una clave dinámica (Enterprise Mode), aunque para este último se requiere de un servidor RADIUS, por lo que se mostrará el procedimiento del Personal Mode.

La autenticación mediante WPA en tecnologías inalámbricas 802.11 ha demostrado una alta fiabilidad y seguridad, avalada por cientos de millones de dispositivos que la usan. WPA usa una palabra clave precompartida (WPA Pre-Shared Key, o WPA-PSK) de entre 8 y 63 caracteres para autenticación y una vez que un dispositivo se ha autenticado en el punto de acceso o en el servidor de autenticación RADIUS, implementa el protocolo TKIP que emplea claves dinámicas diferentes en cada trama de datos enviada. La palabra clave se convierte en una clave de autenticación de 256 bits mediante una función de derivación llamada *Password-Based Key Derivation Function 2* e implementada en varios lenguajes de programación.

$$PSK = PBKDF2(PalClav, SSID, LSSID, N, S) \quad (1)$$

Básicamente consiste en utilizar una palabra clave ($PalClav$), el identificador de red ($SSID$) y su longitud ($LSSID$) para crear una clave PSK de S bits. Los parámetros N y S indican las veces que se pasa el algoritmo sobre la palabra clave y el tamaño final de la clave PSK respectivamente (los valores habituales son 4096 y 256 para ambos parámetros).

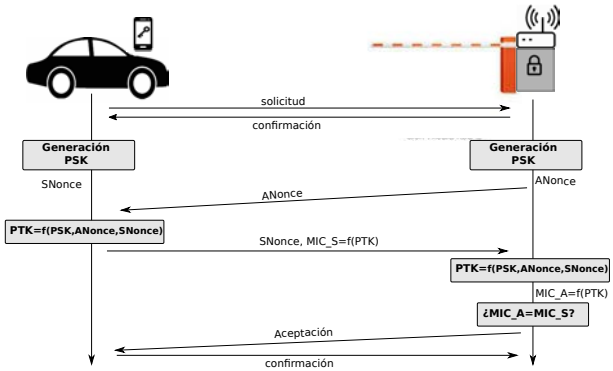

Figura 1: Seguridad WPA

El cliente (la llave) envía una solicitud de acceso y el AP (la cerradura) le envía un número aleatorio llamado *ANonce*. El cliente genera otro número aleatorio *SNonce* y envía un mensaje de autenticación compuesto por el *SNonce* y un hash (llamado *MIC* y del cual no puede deducirse la palabra clave) generado con el *ANonce* y la clave PSK. En ambos extremos se genera una clave transitoria llamada PTK (Pairwise Transient Key) que está compuesta por una función del *ANonce*, el *SNonce* y el *MIC*, y esta clave debe coincidir en ambos

Cuadro 1: Comparativa Bluetooth vs Wifi

	Bluetooth	**Wifi(WPA)**
Alcance	Corto (10m)	Largo (100m)
Tasa de transferencia	Baja	Alta
Consumo energético	Bajo	Alto
Nivel de seguridad	Bajo	Alto

extremos para finalizar la autenticación. Es importante resaltar que la clave PSK no se envía nunca al otro extremo, por lo que no puede ser capturada por un atacante, y además, cada cliente genera una PTK diferente, pues para ello se utilizan números aleatorios.

Este sistema se repite para cada solicitud de autenticación, por lo que aunque un atacante capture las tramas de intercambio no podrá autenticarse si no tiene la palabra clave correcta y ningún cliente puede autenticarse si no lo solicita primero y le es enviado un nuevo *ANonce*. La figura 1 representa el proceso descrito.

1.2. Problemática de consumo energético

El uso de WPA como algoritmia de seguridad implica la utilización de tecnología Wifi para el establecimiento de enlace entre la llave y la cerradura. Intuitivamente, el sistema de enlace entre llave y cerradura se produce porque la llave (el cliente Wifi) escanea continuamente para conocer si hay cerraduras (APs) disponibles. Este procedimiento requiere de un alto consumo energético en el cliente y provocaría una pérdida rápida de carga de batería en el dispositivo móvil que lo implementase [7], [8], [9].

Como alternativa, podrían utilizarse otras tecnologías de enlace inalámbricas disponibles en los dispositivos móviles como Bluetooth, con menos requerimientos de consumo, pero esta adolece de mas problemas de seguridad. La tabla 1 presenta una comparativa entre ambas tecnologías.

Por ello ha habido que diseñar un sistema híbrido de establecimiento de enlace mas eficaz (energéticamente hablando) que el simple enlace Wifi en modo Infraestructure. Este sistema de establecimiento de enlace se presenta en la sección 2.

2. Sistema de control de apertura/cierre

El sistema consiste en una apertura de barrera conectada a través de una controladora Raspberry Pi 2 a una aplicación Android para dispositivos móviles como smartphones o tablets. La figura 2 muestra una arquitectura del sistema.

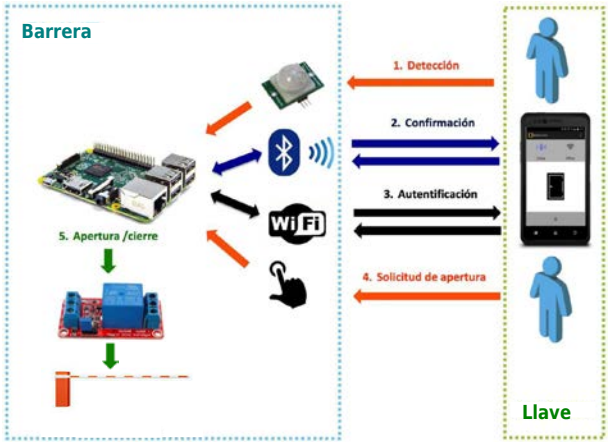

Figura 2: Arquitectura general del sistema

La barrera es un prototipo de Micro-Log modificado para dar estabilidad mecánica al sistema y permitir mejor conectividad y control hacia controladores externos al prototipo. A él se ha añadido un miniordenador RaspberryPi 2 (RBPi2) que hace de controladora y que permite gracias a su universalidad, capacidad de cómputo y conectividad de entrada/salida implementar soluciones de prototipado de alto nivel. A la controladora RBPi2 se le han añadido una tarjeta wifi Edimax y una tarjeta Bluetooth a través de los puertos USB. Asímismo se ha incluido un sensor de presencia por infrarrojos PIR conectado por uno de los pins de entrada/salida de propósito general (GPIO) [10]. La controladora RBPi2 activa, a través de dos GPIO, sendos relés para permitir alimentar en uno u otro sentido el motor de la barrera. La barrera dispone de un final de carrera en cada extremo angular de su rango de movimiento. La figura 3 muestra el prototipo y la controladora.

La llave puede ser cualquier dispositivo móvil con sistema operativo Android y conectividad Wifi y Bluetooth. El software implementado permite seleccionar entre diferentes modelos de apertura, así como la activación automática de escaneado de redes Wifi y la conexión a las mismas. La figura 4 muestra la pantalla principal de la aplicación Llave en Android.

La necesidad de la aplicación Android, viene determinada por la opción de activar o no la apertura de la barrera a voluntad, así como para reactivar la apertura tras un comienzo de cierre indeseado pero programado por un temporizador. No obstante, bastaría con una aplicación mas sencilla que estuviese monitorizando la conectividad bluetooth en modo servidor (de bajo consumo energético) y que

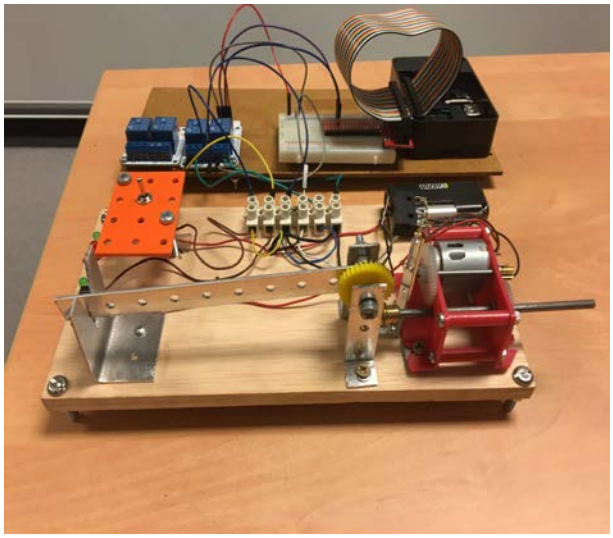

Figura 3: Prototipo de cierre de barrera controlado por Raspberry Pi

activase la búsqueda de redes Wifi para la localización de la cerradura y comenzar el proceso de autenticación WPA.

El proceso técnico de apertura está basado en el uso de relés activados por la controladora, que a su vez comprueba la autenticación de un dispositivo móvil via WPA para accionar el relé.

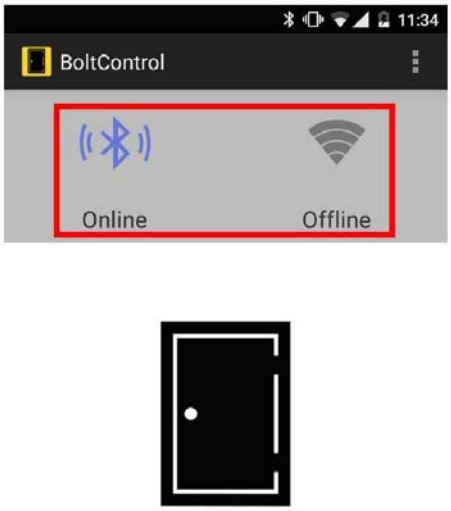

Figura 4: Pantalla principal de la aplicación Llave en Android

3. Modelo de apertura

El modelo de apertura consta de dos partes diferenciadas, las operaciones de enlace y autenticación, y las operaciones de apertura/cierre. Las primeras se encargan de establecer un enlace de datos entre la llave y la cerradura, y las segundas de la decisión y acción de apertura.

3.1. Operaciones de enlace/autenticación

Para la operación de enlace se ha diseñado un sistema híbrido que permite primero la detección por parte de la cerradura de un vehículo o individuo en un radio muy cercano a la cerradura, para seguidamente localizar un servicio Bluetooth operativo en el dispositivo móvil y enviar a este una solicitud de autenticación contra el AP de la cerradura. Cuando el dispositivo móvil detecta el establecimiento de un enlace Bluetooth y recibe la solicitud de autenticación, activa el driver Wifi y se conecta al punto de acceso de la cerradura. Si el dispositivo móvil está autorizado y dispone de la palabra clave correcta la cerradura se abre.

De forma sintetizada, el control básico de proximidad por parte de la cerradura se realiza mediante un detector de presencia y el establecimiento de radioenlace Bluetooth. El control de acceso se realiza mediante enlace 802.11 y encriptación WPA. Intuitivamente puede explicarse mediante la existencia de una zona de presencia, una zona de activación y finalmente una zona de autenticación. Los rangos de establecimiento de enlace pueden verse en la figura 5, donde se muestran las áreas de cobertura estándar del detector PIR, del enlace Bluetooth y de la autenticación WPA a través de enlaces 802.11 Wifi. En particular, el área de cobertura de un detector PIR es de un radio de 6 metros, el de un enlace Bluetooth es de aproximadamente 10 metros para los dispositivos móviles (Bluetooth tipo 2) y el de un enlace WIFI de unos 100 metros en exteriores.

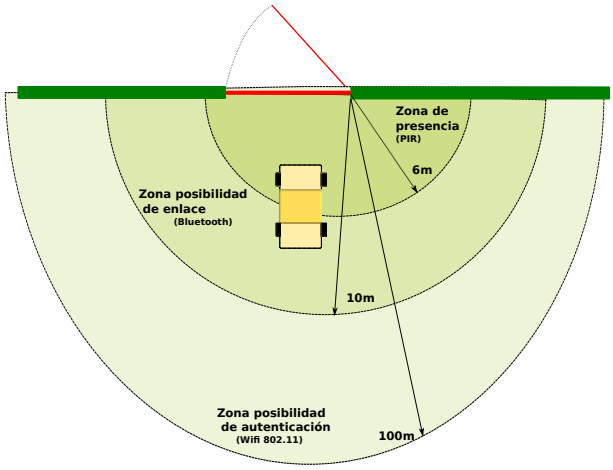

Figura 5: Cobertura PIR, Bluetooth y Wifi

El uso de estas zonas de enlace permite ahorros de consumo en los dispositivos móviles superiores al 90 % además de disminuir sustancialmente falsas solicitudes de apertura cuando un dispositivo

móvil se acerca a la zona de autenticación sin voluntad de apertura.

El flujo de procesos de enlace/autenticación en la cerradura puede verse en la figura 6

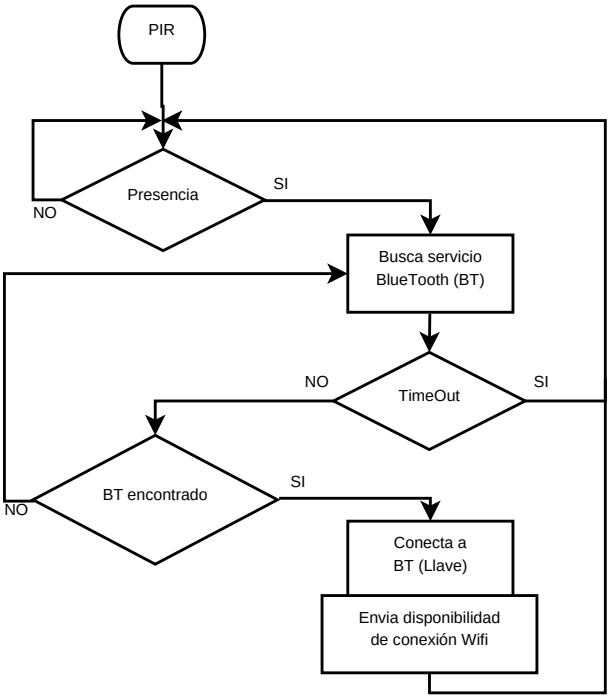

Figura 6: Flujo de procesos de enlace en la cerradura

Es importante resaltar que estas operaciones pueden complementarse con sistemas de autorización por MAC, que permitirían autorizar o no la apertura en función de la dirección MAC del dispositivo Wifi de la llave.

3.2. Operaciones de apertura

Se han diseñado tres tipos de operaciones de apertura: de forma automática, por solicitud y mediante el envío de un código de apertura independiente de la autenticación WPA.

- Automática: la cerradura se abre una vez finalizada correctamente la operación de enlace/autenticación. Esta operación es la mas sencilla y rápida, pero requeriría de un nuevo proceso de enlace/autenticación en el caso en que el usuario no haya podido acceder al edificio antes del cierre temporizado de la cerradura.

- Por solicitud: la cerradura se abre si el usuario envia una solicitud (pulsa la pantalla o un botón del dispositivo móvil) tras la finalización correcta de la operación de enlace/autenticación. Esta operación se asemeja a los sistemas de mando a distancia, pudiendo solventar el problema de nueva solicitud de apertura si no se ha podido acceder al entorno cerrado antes del comienzo de cierre.

- Por código: la cerradura se abre si el usuario introduce un código de cuatro dígitos en un cuadro de dialogo del dispositivo móvil, tras la finalización correcta de la operación de enlace/autenticación. Esta operación permite una doble seguridad.

4. Pruebas

Para la realización de las pruebas y poder comparar diferentes consumos energéticos en el dispositivo móvil se ha empleado un terminal LG Nexus 4 con una batería e 2100 mAh totalmente cargada, en los siguientes escenarios:

- Llave + Bluetooth: la aplicación instalada en el dispositivo móvil está activa, ofreciendo el servicio Bluetooth que permite que sea detectada por la cerradura.

- Servicio Bluetooth: la aplicación instalada en el dispositivo móvil está apagada, pero la radio Bluetooth está encendida aunque ociosa, puesto que ninguna aplicación la emplea.

- Reposo: el dispositivo móvil no ejecuta ninguna aplicación ni tiene habilitado el servicio Bluetooth.

Se estudió el consumo en miliamperios del dispositivo móvil en los tres escenarios descritos. Para ello se emplearon las estadísticas del sistemas generadas por Android. Dado que las estadísticas del sistema proporcionan información muy detallada, ha sido posible reducir considerablemente la duración de los muestreos.

Se realizaron muestreos de una hora de duración para cada uno de los escenarios, extrayéndose datos de consumo de la aplicación, consumo de la radio Bluetooth y consumo total (que incluye el consumo de la pantalla del dispositivo).

La tabla 2 muestra un resumen de los resultados.

Asímismo, los retardos medidos desde la detección de presencia por parte de la cerradura hasta la apertura de la misma han sido de entre menos de 1 segundo y 2 segundos, que a nivel operativo para este tipo de sistemas son satisfactorios.

5. Conclusiones y Líneas Futuras

Se ha desarrollado un sistema de apertura de cerraduras utilizando como llaves dispositivos móviles basados en Android que incluyen conectividad

Cuadro 2: Comparativa de consumos en miliamperios

	Llave+BT	**BT**	**Reposo**
Consumo Aplicación	0.0019 mA		
Consumo BT	0.019 mA	0.0178	
Consumo total	5.241 mA	4.683 mA	4.57 mA

inalámbrica con tecnologías Wifi 802.11 y Bluetooth. El sistema desarrollado aprovecha los estándares de seguridad WPA como sistema de autenticación e implementa un servicio Bluetooth en la llave para evitar escaneos contínuos de redes Wifi y localizar cerraduras. Este forma híbrida de localización de cerraduras por parte del dispositivo móvil permite un ahorro energético notable y habilita que el sistema sea funcional para teléfonos u otros dispositivos móviles. Las pruebas realizadas sobre un prototipo de cerradura en forma de barrera y un teléfono móvil comercial han mostrado la viabilidad del sistema sin necesidad de desarrollar nuevas tecnologías, y permiten diseñar estrategias de integración masivas.

El sistema podría extenderse a otros entornos donde se requiera seguridad en accesos físicos, e incluso a la apertura de los propios vehículos, con niveles de seguridad muy superiores a los que ofrecen actualmente los RKS.

Las líneas futuras pasan por la mejora del sistema en lo que se refiere a la gestión de accesos y el desarrollo de un entorno de gestión. Asímismo se trabaja en la implementación del sistema en entornos reales y la realización de comparativas respecto a los sistemas tradicionales y pruebas de satisfacción de usuarios.

Agradecimientos

Este trabajo ha sido parcialmente subvencionado por el Ministerio Español de Ciencia y Tecnología en el proyecto DPI2013-47100-C2-2-P.

Referencias

[1] S. Du, M. Ibrahim, M. Shehata, and W. Badawy, "Automatic license plate recognition (alpr): A state-of-the-art review," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 2, pp. 311–325, Feb 2013.

[2] S. Kamkar, "New attacks and tools to wirelessly steal cars," Website, 2015.

[3] R. Ting and M. Keane. (2014) Rfid door lock. Website.

[4] N. H. Ismail, Z. Tukiran, N. N. Shamsuddin, and E. I. S. Saadon, "Android-based home door locks application via bluetooth for disabled people," in *Control System, Computing and Engineering (ICCSCE), 2014 IEEE International Conference on*, Nov 2014, pp. 227–231.

[5] I. 802.15, "Ieee 802.15 wpan task group 1," Website, 2002, http://www.ieee802.org/15/pub/TG1.html.

[6] M. K. M. W. Ashish Jadhav, "Feasibility study of implementation of cell phone controlled, password protected door locking system.." *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 6, p. 7, 2013.

[7] N. Vallina-Rodriguez and J. Crowcroft, "Energy management techniques in modern mobile handsets," *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 179–198, First 2013.

[8] S. Chakkor, E. A. Cheikh, M. Baghouri, and A. Hajraoui, "Comparative performance analysis of wireless communication protocols for intelligent sensors and their applications," *CoRR*, vol. abs/1409.6884, 2014. [Online]. Available: http://arxiv.org/abs/1409.6884

[9] C. A. Siebra, P. H. Costa, F. Q. da Silva, R. C. Miranda, and A. L. Santos, "Energy management in wireless networks from the mobile devices perspective."

[10] M. Schwartz, "Control a relay from anywhere using the raspberry pi," Website, 2013. [Online]. Available: https://www.openhomeautomation.net/control-a-relay-from-anywhere-using-the-raspberry-pi/