# STRAP: Secure TRansfer of Association Protocol (STRAP: Secure TRansfer of Association Protocol)

**Abstracto:**

Cuando se requiere instalar varios dispositivos de Internet de las cosas en una casa inteligente, se requiere un esfuerzo considerable para proporcionar a cada dispositivo la información de asociación para el enrutador inalámbrico de la casa. Diseñamos y construimos un nuevo protocolo llamado Protocolo seguro de transferencia de asociación (STRAP), que inicia de forma segura la conectividad entre un conjunto de dispositivos WiFi implementados y el enrutador inalámbrico de un hogar. Mostramos que STRAP funciona en una variedad de entornos y es más rápido que los métodos convencionales para conectar dispositivos WiFi a enrutadores inalámbricos domésticos.

**Publicado en:**[27a Conferencia Internacional de 2018 sobre Comunicación y Redes de Computadoras (ICCCN)](https://ieeexplore.ieee.org/xpl/conhome/8486798/proceeding)

**Fecha de la conferencia:** 30 de julio al 2 de agosto de 2018

**Fecha añadida a IEEE *Xplore* :** 11 de octubre de 2018

**Información del ISBN:**

**Impresión bajo demanda (PoD) ISSN:** 1095-2055

**Número de acceso de INSPEC:** 18164097

**DOI:**[10.1109 / ICCCN.2018.8487333](https://doi.org/10.1109/ICCCN.2018.8487333)

**Editorial:**IEEE

**Lugar de la conferencia:** Hangzhou, China

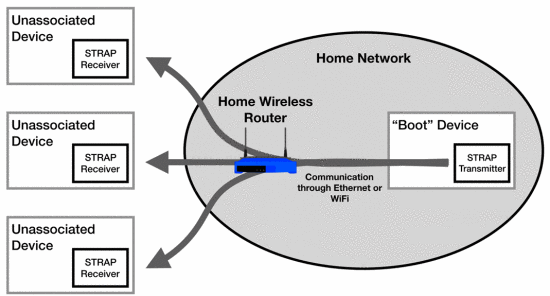
**SECCIÓN I.**

## **Introducción**

Internet de bajo costo (IoT) y dispositivos de "hogar inteligente" tienen aplicaciones en seguridad en el hogar, cuidado de la salud en el hogar, envejecimiento en el lugar y eficiencia energética. Es posible que sea necesario instalar varios sensores y actuadores al mismo tiempo en un hogar para habilitar una de estas aplicaciones. Por ejemplo, un sistema de envejecimiento en el lugar puede usar múltiples sensores de movimiento, sensores de silla o cama y un dispensador de pastillas inteligente. Como otro ejemplo, un sistema de control inteligente de HVAC puede usar sensores de movimiento, sensores de temperatura, termostato, sensores de CO 2 y sensores de contaminación del aire. En este documento, nos motiva específicamente una aplicación en la que se instalan sensores en cada una de las decenas de miles de hogares para recopilar datos de exposición a la contaminación del aire en grandes estudios de sujetos humanos para la investigación epidemiológica del asma y otras enfermedades [1]. Un instalador puede traer y conectar estos dispositivos, o, alternativamente, un kit puede enviarse por correo al residente con instrucciones de autoinstalación. Es fundamental que la instalación sea rápida y con el menor número de pasos posible. El tiempo de un instalador es costoso, y un residente no capacitado puede desanimarse o confundirse por un proceso de instalación largo o complicado.

La mayoría de los dispositivos IoT usan el WiFi del hogar para conectarse a Internet. Por lo general, estos dispositivos no tienen teclado o pantalla, por lo que es mucho más difícil proporcionarle información para acceder a la red WiFi encriptada existente en el hogar. Además, muchos de estos dispositivos económicos, como es el caso de nuestros sensores de calidad del aire, tienen una interfaz de red WiFi pero ninguna otra interfaz de red. Por lo tanto, no se puede acceder a estos dispositivos utilizando ninguna otra red (por ejemplo, Bluetooth) para instalar el nombre y la contraseña de la red WiFi del hogar para permitirles acceder a la red WiFi del hogar.

Un enfoque existente para lidiar con nuestro problema de seguridad de "arranque" es que el dispositivo IoT actúe como un punto de acceso temporal y solicite al usuario que se conecte a él y le proporcione el nombre y la contraseña de la red WiFi doméstica. Este es un enfoque común que utilizan muchos dispositivos comerciales. Si bien este enfoque funciona bien cuando se conecta un nuevo dispositivo, es el momento de conectarsenorte dispositivos escala linealmente con norte. Tener que ingresar el nombre de red y la contraseña en cada dispositivo es engorroso, requiere mucho tiempo y es propenso a errores, especialmente cuando se instalan decenas de dispositivos en cada hogar. A medida que los dispositivos IoT se vuelven más populares, esperamos que aumente la cantidad de dispositivos que deben instalarse, lo que empeora este problema. Otro enfoque existente que utiliza soluciones de seguridad WiFi empresarial (discutido en la Sección V ) generalmente no es compatible con los puntos de acceso de los consumidores o las redes domésticas.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-1-source-large.gif)

**Figura 1:**

Descripción general de los componentes STRAP. El dispositivo de arranque envía de forma segura el nombre y la contraseña de la red fuera de la red doméstica a los dispositivos no asociados.

[Ver todo](https://ieeexplore.ieee.org/document/8487333/all-figures)

En este documento, abordamos el problema anterior de instalación rápida y fácil de dispositivos IoT sin utilizar otra interfaz de red. Básicamente, aquí hay un problema de "huevo y gallina", ya que necesitamos transferir de forma segura la información de asociación a los dispositivos, pero para poder hacer esa transferencia a través de WiFi estándar, cada dispositivo ya debe tener la información de asociación y estar conectado a la red Creamos un protocolo novedoso que permite un dispositivo ya conectado (el dispositivo de "arranque" en la Figura 1), ya sea a través de Ethernet o WiFi, para transmitir datos de forma segura a un grupo de dispositivos no autenticados. Utilizamos esta capacidad para transmitir la información de asociación WiFi, permitiendo que los dispositivos no conectados se autentiquen y se conecten a la red. Utilizamos información clave sobre cómo los marcos de Ethernet y 802.11 son encapsulados, encriptados y transmitidos por enrutadores inalámbricos para codificar las credenciales en los campos de dirección de origen y destino de Ethernet. Nuestro protocolo proporciona comunicación simple a dispositivos inalámbricos no asociados al sobrecargar las direcciones de origen y destino de las tramas Ethernet y 802.11, sin requerir modificaciones al enrutador inalámbrico.

Figura 1muestra los componentes de alto nivel de nuestro protocolo. Hay tres componentes: un grupo de dispositivos WiFi no asociados que esperan recibir las credenciales de autenticación, el enrutador inalámbrico del hogar y un dispositivo ya conectado, el arranque, que transmite las credenciales de autenticación. El dispositivo de arranque ya debe estar conectado a través de Ethernet o WiFi para que pueda enviar tramas en la red. La región sombreada representa la red doméstica segura. Nuestro enfoque funciona de la siguiente manera: un instalador ingresa la información de asociación en el dispositivo de arranque. Como el dispositivo ya está conectado, puede enviar tramas Ethernet a la red. El arranque encripta la información de asociación e inserta estos datos en las direcciones de origen y destino de múltiples tramas Ethernet, sobrecargando el propósito de estos campos. No asociado,

Nuestro protocolo supone que existe una relación de confianza entre el arranque y los dispositivos que intentan conectarse. Específicamente, el arranque tiene un conjunto de claves secretas precompartidas con todos los dispositivos no asociados. Estas claves se utilizan para asegurar la comunicación entre el arranque y los dispositivos no asociados. La clave precompartida tiene una función similar al nombre y la contraseña de la red doméstica, pero el beneficio de usar una clave precompartida es que el instalador tiene control total sobre la clave. Esto permite al instalador preconfigurar los dispositivos con la clave antes de configurarlos en un hogar. En esencia, estamos utilizando una segunda asociación de seguridad (las claves precompartidas) para iniciar la asociación de seguridad WiFi. Se describen los beneficios de este diseño con respecto a otros métodos en la Sección V .

Visualizamos los siguientes dos casos de uso para nuestro trabajo (aunque no se limita a estos casos de uso):

1. Un instalador llega a la casa de alguien para instalar múltiples dispositivos WiFi. Esto podría ser parte de un sistema de seguridad o un estudio epidemiológico que implica el despliegue de múltiples sensores ambientales en el hogar. Todos los dispositivos que forman parte de la instalación se han configurado con una clave precompartida cuando se actualizan con el software y se preparan para la implementación. El instalador instala los dispositivos donde necesitan ir y los enciende. Luego, el instalador conecta el dispositivo de arranque al enrutador inalámbrico de la casa a través de Ethernet. El instalador ingresa la información del cliente, como una identificación del cliente, en el dispositivo de arranque que permite que el dispositivo de descarga descargue de forma segura la clave secreta de los servidores de la compañía que está conectada con los dispositivos recién instalados. El instalador luego le pide al cliente que ingrese el nombre y la contraseña de su red WiFi.
2. Similar al caso de uso número uno, pero en lugar de que un instalador venga a la casa, se envía una caja de dispositivos WiFi al cliente para que el cliente se autoinstale. El cliente coloca los dispositivos y descarga una aplicación en su teléfono inteligente o computadora portátil. Este dispositivo actúa como un dispositivo de arranque temporal. El dispositivo del cliente recibe la clave compartida escaneando un código QR que vino con los dispositivos o usando credenciales de inicio de sesión y descargando la clave de forma segura desde los servidores de la compañía. Luego, el cliente ingresa el nombre y la contraseña de la red WiFi en el dispositivo de arranque temporal, que transmite esta información de manera segura a todos los dispositivos no asociados.

En este documento, identificamos posibles vectores de ataque a nuestro protocolo y mostramos que es resistente. En particular, protegemos contra un adversario que intenta engañar a los dispositivos para que se conecten a un punto de acceso de rouge, así como a otros vectores de amenazas como espionaje, manipulación de paquetes y ataques de repetición. Nuestro protocolo, basado en la transmisión unidireccional desde el arranque a los dispositivos no asociados sin ningún comentario, utiliza la codificación de borrado para minimizar los efectos de la pérdida de paquetes inalámbricos.

Evaluamos nuestro protocolo en muchas configuraciones y configuraciones diferentes. Demostramos que nuestro protocolo funciona en una variedad de enrutadores inalámbricos y no tiene ningún efecto en la red cuando se ejecuta, y es mucho más rápido para configurar múltiples dispositivos en comparación con los enfoques convencionales.

**SECCION II.**

## **Protocolo seguro de transferencia de asociación**

Para que un dispositivo WiFi se conecte a la red de un hogar, debe tener el nombre y la contraseña de la red. Llevar esta información a dispositivos sin teclados y pantallas lleva mucho tiempo, especialmente cuando hay muchos dispositivos para conectar. Este problema continuará empeorando a medida que se implementen más dispositivos IoT en los hogares como parte de sistemas comerciales y estudios de investigación. Especialmente encontramos que esto era un problema cuando desplegamos sensores de calidad del aire en los hogares de los participantes como parte de un estudio de investigación de asma pediátrica. Como parte de este estudio, implementamos diez sensores de calidad del aire en el hogar de cada familia participante. Descubrimos que llevó mucho tiempo implementar estos sensores porque una gran parte del tiempo implicaba conectar cada sensor a la red inalámbrica del hogar.

Un enfoque común para resolver este problema para dispositivos IoT comerciales es que un dispositivo cree su propia red inalámbrica temporal. Esto permite que la persona que configura el dispositivo IoT se conecte a la red inalámbrica temporal a través de un teléfono inteligente. Seleccionan el nombre de red al que desean que se conecte el dispositivo e ingresan la contraseña, que luego proporciona al dispositivo IoT la información que necesita para conectarse a la red WiFi. Una vez que el teléfono inteligente se desconecta, el nuevo dispositivo desactiva la red inalámbrica temporal y se conecta al enrutador inalámbrico doméstico. Este proceso funciona bien con un nuevo dispositivo, pero se convierte en una molestia al instalar varios dispositivos y cada vez más insostenible a medida que aumenta el número de dispositivos. Configurar cada dispositivo de uno en uno requiere un proceso largo para el instalador y aumenta la posibilidad de que un dispositivo esté configurado incorrectamente. Una instalación larga no es deseable debido a los altos costos de mano de obra, así como a los inconvenientes para el residente. Si un cliente está autoinstalando dispositivos, un proceso de configuración largo y complicado puede ser desalentador o confuso. Para abordar este problema, creamos un enfoque novedoso para enviar de forma segura el nombre y la contraseña de la red a los dispositivos inalámbricos no asociados, que llamamos*Protocolo de transferencia segura de asociación* (STRAP). CORREA permite que un dispositivo inicie su conexión a la red inalámbrica doméstica con la ayuda de un dispositivo ya conectado a la red (ya sea a través de Ethernet o WiFi).

CORREA consta de tres componentes, como se muestra en la Figura 1: dispositivos no asociados que intentan conectarse, el enrutador inalámbrico doméstico y un dispositivo que ayuda a los dispositivos no asociados a conectarse, lo que llamamos el "arranque". CORREA no requiere modificaciones en el enrutador inalámbrico doméstico. El arranque ejecuta una aplicación que transmite de manera segura el nombre y la contraseña de la red, y los dispositivos WiFi no asociados ejecutan una aplicación para recibir esta información. El arranque puede ser un dispositivo que el instalador trae al hogar (como una computadora portátil, teléfono inteligente o un dispositivo conectado a Ethernet) o una aplicación que el consumidor instala en uno de sus dispositivos. El dispositivo de arranque debe poder inyectar tramas Ethernet o WiFi en la red. Suponemos que existe una relación de confianza entre el dispositivo de arranque y los dispositivos que intentan conectarse, y que ambos tipos de dispositivos se han programado con una ID de instalación y claves compartidas utilizadas para el cifrado y la protección de integridad. Esperamos que esta información se cargue en los dispositivos cuando se actualiza con firmware y se prepara para una instalación.

El principal desafío que abordamos en este documento es que no hay una forma directa de enviar información segura a los dispositivos no asociados utilizando solo WiFi. Suponemos que todos los hogares están utilizando encriptación WiFi (WPA, WPA2) y, como resultado, los dispositivos no asociados no pueden descifrar los datos sin conocer primero el nombre y la contraseña de la red. Para dificultar esta tarea, dado que el dispositivo de arranque tiene una aplicación que se ejecuta en el espacio de usuario, no tiene el concepto de tramas 802.11 y en el nivel más bajo solo puede enviar tramas Ethernet. Todos los datos enviados por esta aplicación serán encapsulados en un marco 802.11 y encriptados por el adaptador inalámbrico (si el dispositivo de arranque es inalámbrico) o el enrutador inalámbrico (si el dispositivo de arranque está conectado). Para sortear estos obstáculos,

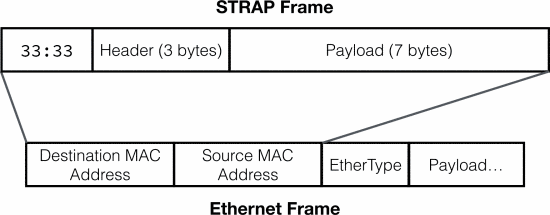
El primer problema que debemos superar es cómo un dispositivo WiFi no asociado puede recibir tramas de una red con la que no está asociado. Para resolver este problema, utilizamos el modo monitor. El modo monitor es el modo de un adaptador inalámbrico que pasa todas las tramas 802.11 recibidas para un canal específico, independientemente del destino previsto y de qué red es parte la trama. Esto permite que un dispositivo WiFi reciba tramas, pero si la red está encriptada, entonces la carga útil de la trama no se puede leer.

Esto lleva a nuestro segundo problema, ¿cómo puede un dispositivo en modo monitor recibir datos sin cifrar? La idea clave para este problema es que un enrutador inalámbrico no cifra el encabezado 802.11, que incluye las direcciones de destino y de origen. Esto significa que un dispositivo no asociado en modo monitor puede leer las direcciones de origen y destino de las tramas cifradas 802.11. Usando este hecho, podemos enviar datos codificados en las direcciones de origen y destino. Una cosa a tener en cuenta es que nuestro código de nivel de aplicación trata con tramas Ethernet y los enrutadores inalámbricos encapsulan las tramas Ethernet en tramas 802.11. Afortunadamente, los enrutadores inalámbricos copian directamente las direcciones de origen y destino de Ethernet y las insertan en las direcciones de origen y destino del marco 802.11 [2]. Esto permite que los datos sean enviados por un dispositivo ya conectado (ya sea a través de Ethernet o WiFi), a través del enrutador inalámbrico de la casa, a un dispositivo no asociado en modo monitor.

Las direcciones de origen y destino constituyen 12 bytes en una trama Ethernet y 802.11. Esto significa que, como máximo, se pueden codificar 12 bytes de datos en estos dos campos. Dado que un dispositivo no asociado no puede transmitir en una red, la comunicación solo puede ser en una dirección, por lo que la dirección MAC de origen no necesita ser enrutable de regreso al dispositivo de arranque. Sin embargo, se debe tener cuidado en cuanto a cómo se codifica la información en las direcciones. Los bytes en la dirección MAC tienen un significado específico que debe seguirse o un marco corre el riesgo de ser rechazado o colisionar con otras direcciones MAC. El bit menos significativo del primer byte de una dirección MAC especifica si la dirección es multidifusión (1) o unidifusión (0). El segundo bit menos significativo del primer byte especifica si la dirección MAC es globalmente única (0) o administrada localmente (1) [3]. Para seguir esta convención, establecemos estos bits en 10 (administrado localmente y unidifusión). Al hacerlo, nos aseguramos de que, independientemente de los datos que se envíen, las direcciones de origen y destino no colisionen con las direcciones MAC comerciales.

Incluso con seguir estas reglas de dirección MAC, los datos arbitrarios no se pueden codificar directamente en la dirección de destino. Un marco que se envía con una dirección MAC de destino aleatorio no será enrutable y el enrutador inalámbrico lo descartará. La dirección de destino debe tener los siguientes dos requisitos. Primero, debe ser siempre enrutable, independientemente de qué datos se codifiquen. En segundo lugar, la trama debe transmitirse en la interfaz inalámbrica del enrutador inalámbrico para que los dispositivos no asociados puedan recibir la trama. Para abordar estos requisitos, utilizamos una información clave sobre las direcciones MAC de destino especiales que tienen estas propiedades: difusión (FF: FF: FF: FF: FF: FF), multidifusión IPv4 (01: 00: 5E: xx: xx: xx) [4] y multidifusión IPv6 (33: 33: xx: xx: xx: xx) [5], donde las x de las direcciones se pueden reemplazar con un identificador único para ese grupo de multidifusión. Estas tres direcciones siempre son enrutables por el enrutador inalámbrico y siempre hacen que el enrutador inalámbrico envíe la trama en todas sus interfaces, incluida la interfaz inalámbrica. Para nuestros propósitos, las tres direcciones cumplirían el mismo objetivo de que el enrutador inalámbrico envíe el marco en su interfaz inalámbrica. Sin embargo, la dirección de multidifusión IPv6 proporciona los bytes más no utilizados, lo que nos permite codificar más información en la dirección. Por esta razón, seleccionamos la dirección de multidifusión IPv6 como la dirección de destino, lo que nos deja con 10 bytes de datos utilizables.

Dado que estamos usando la dirección MAC de multidifusión IPv6 como la dirección de destino, es importante comprender cómo otras aplicaciones que usan esta dirección MAC y STRAP se afectarán entre sí. Para tratar el tráfico de multidifusión IPv6 de otras aplicaciones, STRAP utiliza un campo de ID de 6 bits en su encabezado (consulte la siguiente sección para obtener más detalles). Esto permite que un dispositivo identifique de forma exclusiva el tráfico de multidifusión IPv6 e ignore el tráfico que no está destinado a él. STRAP solo afectaría a otra aplicación que use la dirección de multidifusión IPv6 si el ID del grupo de multidifusión coincide exactamente con los datos que STRAP está enviando. Este efecto se minimizaría ya que la dirección de destino de las tramas STRAP cambia entre cada trama debido a la paquetización y el cifrado.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-2-source-large.gif)

**Figura 2:**

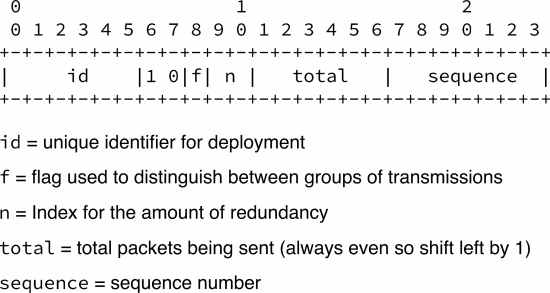
La composición de un marco STRAP y cómo encaja en un marco ethernet.

[Ver todo](https://ieeexplore.ieee.org/document/8487333/all-figures)

Usando la dirección de origen completa y parte de la dirección de multidifusión IPv6 como la dirección de destino, podemos codificar 10 bytes de datos dentro de cada trama de Ethernet. La Figura 2 muestra cómo se ajusta un marco STRAP dentro de un marco Ethernet. Reconocemos que la capacidad de un dispositivo ya conectado de enviar datos arbitrarios a dispositivos inalámbricos no asociados podría tener muchas aplicaciones diferentes, como notificaciones de emergencia, pero para este documento limitamos el uso para enviar el nombre y la contraseña de la red. En las siguientes secciones, describimos el diseño de STRAP.

### A. Encabezado

Usando la dirección de origen y la dirección de destino IPv6 como se describe anteriormente, hay 10 bytes disponibles para codificar datos. No esperamos que el nombre y la contraseña de la red se ajusten a 10 bytes, por lo que diseñamos STRAP para admitir datos fragmentados. Creamos un formato de encabezado como se muestra en la Figura 3. Usamos los primeros 3 bytes de la dirección de origen como encabezado para nuestro protocolo y el resto de los bytes como carga útil. Los primeros 6 bits se utilizan como un ID único para identificar la instalación. Dado que cada dispositivo no asociado estará en modo de monitor, escuchando toda la comunicación inalámbrica en un determinado canal, es importante que el dispositivo pueda filtrar los datos que no son intencionales para él. Los bits 6 y 7 configuran la dirección MAC para ser administrada localmente y unidifusión, como se mencionó anteriormente. El bit 8 es una bandera utilizada para distinguir entre diferentes grupos de transmisiones. La bandera se alterna entre uno y cero, lo que permite que un dispositivo sepa cuándo un grupo de transmisiones ha finalizado y otro ha comenzado. Los bits 9 y 10 se usan como un índice en una matriz predeterminada para la cantidad de codificación de borrado que se ha agregado. Esto se explica más enSección II-C . Los bits 11 a 16 dan el número total de paquetes que se envían. Con STRAP, nos aseguramos de que siempre se envíe un número par de paquetes, por lo que el número total de paquetes debe desplazarse a la izquierda por uno. Los últimos 7 bits (bits 17 a 23) representan el número de secuencia de ese paquete. El resto de los 7 bytes se utilizan como carga útil para enviar el nombre y la contraseña de la red cifrada. Una cosa a tener en cuenta es que solo se pueden enviar 126 paquetes en una ronda de transmisiones, debido al tamaño del campo total en el encabezado. Esto permite transferir 882 bytes de datos. Esto no es un problema para transmitir el nombre y la contraseña de la red, ya que el tamaño máximo de un nombre de red es de 32 bytes y el tamaño máximo de una contraseña es de 64 bytes [6]. Si se convirtiera en un problema, la información puede dividirse en múltiples intercambios y los datos aún pueden transmitirse.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-3-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-3-source-large.gif)

**Fig. 3:**

Formato de encabezado STRAP

[Ver todo](https://ieeexplore.ieee.org/document/8487333/all-figures)

### B. Cifrado y protección de integridad

Para garantizar que el nombre y la contraseña de la red estén protegidos, utilizamos AES-128 con CBC [7] para cifrar los datos. Se genera un vector de inicialización (IV) y se utiliza para cifrar los datos y se envía junto con la carga útil cifrada. También se agrega un número de secuencia "global" a la carga útil. Usamos el término "global" para distinguir entre el número de secuencia que forma parte del encabezado descrito en la Figura 3 . Utilizamos el tiempo actual en forma de una marca de tiempo de época como nuestro número de secuencia global, ya que es monótono. Como el número de secuencia global es monótono, protege contra ataques de repetición. Se crea un código de autenticación de mensaje basado en los datos cifrados y el número de secuencia global. Usamos SHA256 como nuestro hash para crear el código de autenticación del mensaje. Esto se agrega a la carga útil.

### C. Codificación de borrado

La codificación de borrado es el proceso de agregar datos redundantes a los datos originales de modo que si hay pérdida de datos, el mensaje aún se puede recuperar. La pérdida de datos es una consideración importante para STRAP. Como estamos utilizando la dirección de destino de multidifusión IPv6, no hay acuses de recibo de la capa de enlace, por lo que nuestras tramas no se benefician de los reintentos de la capa de enlace. Utilizamos Zfec [8] como nuestro algoritmo de codificación de borrado. Zfec tiene dos parámetros,k y metro. metro es la cantidad total de bloques que se producirán y kes el número de bloques necesarios para construir el mensaje original. Ajustemetro y kproduce bloques de datos de diferentes tamaños. Seleccionamosmetrotal que el tamaño del bloque es igual a nuestro tamaño de carga útil, 7 bytes. Para decodificar los datos de Zfec, el receptor debe saberk y metro. metrose incluye en el encabezado del paquete como el número total de paquetes. Para guardar bits, no queremos enviarkdirectamente. En cambio, usamos una matriz de valores predeterminados y enviamos un índice a esa matriz. Los valores en esta matriz representan la pérdida máxima tolerada mientras se puede decodificar el mensaje. Por ejemplo, la matriz [.2 ,. 4 ,. 6 ,. 8] representaría una pérdida del 20%, una pérdida del 40%, una pérdida del 60% y una pérdida del 80%. Si el dispositivo de arranque quiere soportar una pérdida del 40%, codifica los datos usando Zfec de modo quek = .4 m y establece los bits 9 y 10 de cada encabezado en 01. Cuando un receptor recibe un paquete, lo indexa en la matriz utilizando los bits 9 y 10, usa este valor para calcular k Residencia en metroy decodifica el mensaje. Diseñamos STRAP para admitir velocidades de codificación de borrado múltiples para que pueda adaptarse al entorno en el que se está ejecutando. Permite que STRAP comience con una codificación de borrado mínima y aumente si es necesario.

### D. Correr CORREA

Figura 4muestra el flujo general de datos a través de STRAP. Para comenzar el proceso de transferencia de la información de asociación, el instalador ingresa su nombre y contraseña de red WiFi en una interfaz en el dispositivo de arranque. El nombre y la contraseña de la red que se ingresan primero se cifran utilizando la clave de cifrado precompartida y el IV generado aleatoriamente. Se crea un código de autenticación de mensaje utilizando una clave de integridad precompartida, datos cifrados y un número de secuencia global. El IV, el número de secuencia global, los datos cifrados y el código de autenticación del mensaje se concatenan juntos y se ejecutan a través del algoritmo de codificación de borrado. Finalmente, los datos se dividen en paquetes, se agregan bytes de encabezado y se envían como tramas Ethernet vacías con solo las direcciones de origen y destino establecidas. Para garantizar que todos los dispositivos reciban los datos,

Cada uno de los dispositivos inalámbricos no asociados que ejecutan STRAP ingresa al modo monitor y escanea a través de todos los canales, escuchando cuadros del dispositivo de arranque (usando el segmento de ID del encabezado para filtrar los paquetes no deseados). Si un dispositivo recibe tramas con diferentes valores de marca, sabe que se ha iniciado una nueva transmisión y descarta las tramas con la antigua bandera. Una vez que un dispositivo ha recibido suficientes tramas para completar el mensaje, autentica el mensaje (usando el MAC y el número de secuencia global), descifra el mensaje y se conecta al enrutador inalámbrico doméstico. Después de que un dispositivo se conecta a la red, realiza las tareas necesarias para notificar al dispositivo de inicio que se ha conectado, como notificar a un servidor que el dispositivo de inicio está conectado. A medida que pasa el tiempo, el arranque aumenta la cantidad de codificación de borrado que agrega a los datos. Esto ayuda a atrapar cualquier dispositivo que tenga una alta pérdida y no pueda decodificar los datos. Una vez que todos los dispositivos esperados se han conectado, la persona que los instala puede evitar que el arranque envíe los datos. Si cambia el nombre de la red inalámbrica, se puede volver a ejecutar STRAP con el nuevo nombre y contraseña de la red. Si un dispositivo STRAP no puede conectarse a la red programada, automáticamente comienza a escuchar tramas STRAP.

### E. Modelo de amenaza y análisis de seguridad

Con STRAP, suponemos que existe una relación de confianza entre el arranque y los dispositivos que intentan conectarse, y que se han cargado dos claves criptográficas en los dispositivos no asociados que se están instalando, antes de colocar los dispositivos en el hogar de una persona. Una de las claves se usa para el cifrado y la otra para la protección de la integridad. Estas claves tienen una función similar al nombre de red y contraseña de la red inalámbrica del hogar (para asegurar la comunicación), pero con la importante diferencia de que no tiene que ser ingresada manualmente por un usuario o instalador. La clave está controlada por la empresa que fabrica los dispositivos. La clave podría cargarse en los dispositivos cuando los dispositivos se actualizan con firmware. El dispositivo de arranque también se puede preconfigurar con las claves compartidas, o un instalador puede cargar las claves compartidas en el dispositivo de arranque, por ejemplo,

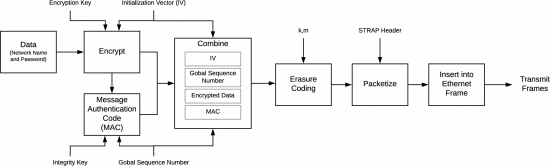
Nuestro modelo adversario incluye atacantes activos y pasivos. Un adversario puede espiar la conversación y reproducir cuadros capturados previamente o inyectar nuevos cuadros, pero no tiene acceso físico a los dispositivos. Los ataques de denegación de servicio, como la interferencia, están más allá del alcance de este documento. El objetivo de un adversario es obtener acceso a la red inalámbrica del hogar o engañar a los dispositivos de conexión para que se conecten a un punto de acceso de rouge. Potencialmente, esto podría dar al adversario acceso a los datos que produce el dispositivo.

Ahora describimos algunos de los posibles vectores de ataque. Los datos transmitidos se cifran utilizando un secreto compartido, que solo el arranque y los dispositivos que intentan conectarse saben, por lo que el adversario no podrá descifrar los datos. Dado que la misma información se transmitirá varias veces, actualizamos el IV entre cada ronda de transmisiones para lograr la seguridad semántica. Esto asegura que un adversario que escucha múltiples rondas de transmisiones no podrá aprender nada sobre el nombre y la contraseña de la red. El adversario no puede imitar el dispositivo de arranque, engañando a los dispositivos para que se conecten a un punto de acceso de rouge, ya que no conoce las claves secretas, por lo que los datos que crea y envía no pasarán la verificación de integridad en los dispositivos que intentan conectarse. Suponiendo que un participante haya cambiado el nombre de su red y que un adversario haya capturado las tramas de este protocolo cuando el participante estaba usando el nombre de la red anterior, el adversario podría establecer un punto de acceso con el nombre de la red anterior y reproducir las tramas que había capturado. Sin embargo, los dispositivos de conexión detectarán este ataque debido al número de secuencia global. El adversario no puede cambiar el número de secuencia global (o ninguno de los datos cifrados) sin que los dispositivos lo detecten, debido al código de autenticación del mensaje.

**SECCION III.**

## **Implementación**

Implementamos el transmisor y receptor STRAP en Raspberry Pi 3s usando Python. Hemos puesto a disposición del público el código fuente de STRAP [9]. Para el receptor STRAP, utilizamos el adaptador inalámbrico MediaTek MT7601 (Ralink 7601) que admite el modo de monitor. Conectamos el transmisor STRAP (el dispositivo de "arranque") a través de Ethernet al punto de acceso doméstico. Cuando el dispositivo que ejecuta el receptor STRAP se inicia, busca cualquier red inalámbrica previamente conocida para conectarse. Si no puede encontrar una red, inicia el receptor STRAP. El receptor escanea aleatoriamente a través de los canales WiFi escuchando mensajes STRAP, esperando un segundo en cada canal. Si el receptor detecta un mensaje STRAP, se detiene en ese canal hasta que recibe todos los cuadros necesarios para decodificar el mensaje. Si el receptor STRAP no puede recibir ningún mensaje STRAP, intenta nuevamente conectarse a cualquier red previamente conocida. Este proceso continúa hasta que el dispositivo pueda conectarse a una red.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-4-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-4-source-large.gif)

**Fig. 4:**

Flujo de datos a través de la correa.

[Ver todo](https://ieeexplore.ieee.org/document/8487333/all-figures)

El transmisor STRAP lo inicia un instalador que ingresa el nombre y la contraseña de la red en una página web que se ejecuta localmente en el dispositivo de arranque. El script Python usa la biblioteca Scapy Python [10] para inyectar tramas Ethernet en la red. El transmisor STRAP envía continuamente tramas cada 50 ms hasta que todos los dispositivos esperados se hayan conectado y el instalador detenga el dispositivo de arranque.

**SECCION IV.**

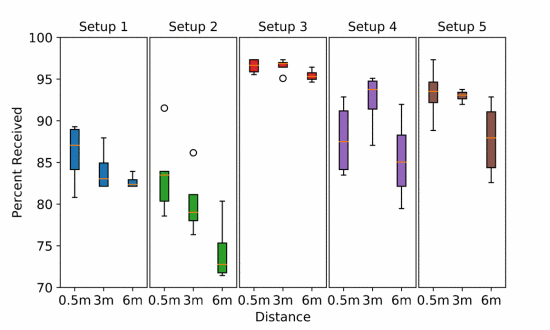
## **Evaluación**

Integramos STRAP con dos sensores de calidad del aire, el Dylos DC1100 [11] y el Plantower PMS3003 [12] . Ambos sensores están disponibles comercialmente y miden la concentración de partículas en el aire. CORREA se ha utilizado en hogares para implementar estos sensores de calidad del aire, con múltiples sensores por hogar.

Evaluamos cuatro aspectos de STRAP: soporte de hardware, características de pérdida observadas durante el uso de STRAP, efecto de STRAP en el funcionamiento normal de la red y facilidad de uso de STRAP en comparación con la solución de red temporal comúnmente utilizada.

### A. Soporte de enrutador inalámbrico

Probamos STRAP utilizando cinco enrutadores inalámbricos en cuatro ubicaciones para garantizar que nuestro protocolo sea compatible con una amplia gama de marcas. Probamos STRAP en un Apple Airport Extreme (cuarta generación), Google Fiber Network Box GFRG200, Net-gear Nighthawk R7000, Linksys WRT3200ACM y TP-Link WR940N. De los cinco enrutadores inalámbricos que probamos, todos admitían nuestro protocolo. Aunque estamos sobrecargando el propósito de las direcciones de origen y destino del

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-5-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-fig-5-source-large.gif)

**Fig. 5:**

Porcentaje de tramas recibidas en diferentes configuraciones experimentales (diferentes enrutadores inalámbricos, diferentes ubicaciones) frente a la longitud de la ruta.

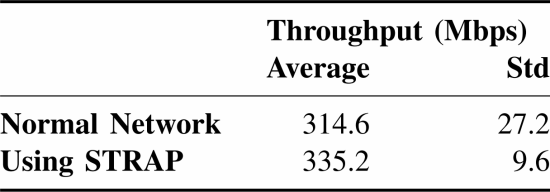
[Ver todo](https://ieeexplore.ieee.org/document/8487333/all-figures)

Marco de Ethernet, codificamos los datos para que la dirección de origen no choque con ninguna otra dirección MAC configurando el bit administrado localmente y la dirección de destino se utiliza con la dirección MAC estándar para IPv6. Como resultado, STRAP funciona en todos los enrutadores inalámbricos que hemos probado.

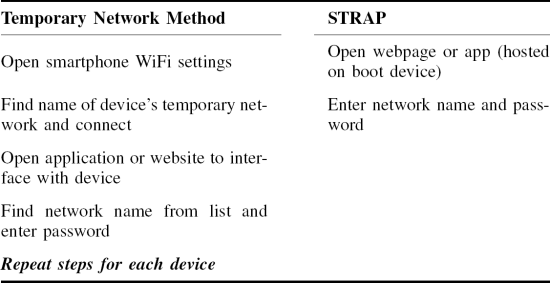
### B. Características de pérdida

Probamos STRAP a tres distancias diferentes de un enrutador inalámbrico (menos de. 5 m, 3 my 6 m) para comprender los patrones de pérdida y ayudarnos a informarnos cuánta codificación de borrado necesitamos. Es importante comprender la pérdida, ya que las tramas 802.11 que se envían son de multidifusión y no se benefician de las retransmisiones de la capa de enlace. Utilizamos los mismos cinco enrutadores inalámbricos en las mismas cuatro ubicaciones del experimento anterior. Ejecutamos STRAP, que mide la cantidad de paquetes que recibió un dispositivo que intentaba conectarse a la red. Figura 5muestra los resultados de estos experimentos. Cada gráfico muestra los resultados de una de las cinco configuraciones de puntos de acceso mencionadas en la sección anterior. Se muestra un diagrama de caja para cada una de las tres distancias de transmisión. Es probable que las variaciones entre las cinco configuraciones se deban a las condiciones ambientales variables para la misma longitud de ruta. Los resultados muestran que la CORREA funciona bien incluso desde 6 m, con el porcentaje más bajo recibido superior al 70%. Esta cantidad de pérdida se puede superar mediante el uso de la codificación de borrado.

**Tabla I:** Velocidad de red durante el tráfico de red normal y mientras se ejecuta la correa.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-table-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-table-1-source-large.gif)

**Tabla II:** Número de pasos para configurar dispositivos utilizando el método de red temporal en comparación con la correa.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-table-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/8486798/8487301/8487333/8487333-table-2-source-large.gif)

### C. Gastos generales de red

Medimos el efecto de STRAP en la otra actividad de la red. Hacemos esto ejecutando iperf bajo operación normal de la red y mientras ejecutamos STRAP. Ejecutamos iperf en dos computadoras portátiles, una conectada de forma inalámbrica y la otra conectada a través de Ethernet. Los datos se envían desde la computadora portátil conectada a Ethernet a la computadora portátil conectada de forma inalámbrica. La tabla I muestra los resultados de estos experimentos. Aunque el rendimiento promedio durante el uso de STRAP fue ligeramente mayor, una prueba t de dos muestras no muestra diferencias estadísticamente significativas (enα = 0.05) entre el rendimiento de iperf usando STRAP versus no usarlo. En otras palabras, el uso de STRAP no afecta el rendimiento de la velocidad de datos de la red.

### D. velocidad

Evaluamos cuánto tiempo tarda un receptor STRAP en conectarse a un enrutador inalámbrico. El tiempo que le toma a un receptor STRAP recibir el nombre y la contraseña de la red depende de qué tan rápido el receptor pueda encontrar el canal del enrutador inalámbrico al que está conectado el dispositivo de arranque y capturar suficientes marcos STRAP para decodificar el nombre y la contraseña de la red. Suponiendo que el receptor STRAP tenga once canales WiFi para escanear, el dispositivo de arranque ya está transmitiendo y el receptor STRAP hace una pausa en cada canal durante un segundo (consulte la Sección III ), tomará al menos 1 segundo y como máximo 11 segundos .

El tiempo que lleva transmitir todas las tramas STRAP depende de qué tan grandes sean el nombre y la contraseña combinados de la red y la cantidad de codificación de borrado utilizada. Analizamos el mejor y el peor de los casos para STRAP. En el mejor de los casos, suponiendo un nombre y contraseña de red pequeños y sin pérdida en la red, se necesitarían solo 11 de los 14 cuadros para que el receptor obtenga el nombre y la contraseña de la red. Con STRAP, se transmite una trama cada 50 ms, por lo que se necesitarían 550 ms para recibir las primeras 11 tramas.

En el peor de los casos, se necesitarían 120 cuadros para ser enviados, el número máximo de cuadros que admite STRAP y solo 24 cuadros recibidos (pérdida del 80%). Tenga en cuenta que para enviar el número máximo de tramas, la codificación de borrado debería establecerse en una pérdida del 80% y la combinación de nombre de red y contraseña debería tener 111 caracteres de longitud. Como se indicó anteriormente, STRAP transmite tramas cada 50 ms, por lo que tomaría 6 segundos recibir todas las tramas necesarias. Sin embargo, para que un receptor STRAP capture al menos una transferencia completa de esas tramas, el receptor debe estar en ese canal el doble de ese tiempo, 12 segundos. Combinando los mejores y peores casos con el tiempo que lleva escanear los canales WiFi, STRAP puede variar de 1.55 segundos a 23 segundos. Este tiempo permanece constante independientemente de cuántos dispositivos se estén conectando. El tiempo necesario para otros enfoques,

A continuación, comparamos el número de pasos necesarios para configurar un dispositivo utilizando el método estándar de convertir el dispositivo en una red temporal en comparación con el uso de STRAP. Los pasos se muestran en la Tabla II . Usando el método de red temporal, se necesitan cuatro pasos para *cada dispositivo* que está configurado. CORREA solo requiere dos pasos en total, independientemente de la cantidad de dispositivos que se estén configurando.

Con base en estas evaluaciones, concluimos que STRAP funcionará con el enrutador inalámbrico de un hogar, trabajará desde una variedad de distancias, no tendrá ningún efecto en la red de un hogar mientras se ejecuta, y facilitará la instalación de dispositivos que los métodos tradicionales.

**SECCION V.**

## **Enfoques alternativos y trabajos relacionados**

El escenario de implementación que exploramos es que un instalador de una compañía que proporciona un sistema IoT llegará a un hogar con muchos dispositivos necesarios para ser instalados. Alternativamente, la compañía puede simplemente enviar por correo un conjunto de dispositivos con instrucciones, y el usuario sirve como instalador.

Dado que suponemos que existe una relación de confianza entre la persona que instala los dispositivos y los dispositivos en sí mismos, y que cada dispositivo tiene que ser programado con una clave compartida, tendría sentido programar los dispositivos con el nombre y la contraseña de la red WiFi del hogar. en lugar de la clave compartida antes de instalar los dispositivos en el hogar. Sin embargo, este enfoque tiene inconvenientes. Primero, un residente puede sentirse incómodo al dar su contraseña de WiFi, y un instalador puede no querer ser responsable de almacenarla. En segundo lugar, puede haber una alta tasa de errores al comunicar el nombre y la contraseña de la red, en parte debido a las contraseñas largas y difíciles predeterminadas en los enrutadores inalámbricos domésticos. Estas contraseñas pueden ser difíciles de transmitir con precisión (por ejemplo, confundir una letra mayúscula "o"). Un nombre de red o contraseña incorrectos solo se detectan después de instalar los dispositivos. En este caso, el instalador necesitaría reprogramar los dispositivos con la información correcta. Dependiendo del dispositivo, esto podría no ser posible en un hogar o podría llevar mucho tiempo.

Otra solución sería utilizar el dispositivo de arranque como un punto de acceso en sí. Los dispositivos que intentan conectarse podrían configurarse para conectarse automáticamente a la red del dispositivo de inicio y luego el dispositivo de inicio podría compartir el nombre y la contraseña de la red con los dispositivos. Sin embargo, este enfoque requiere que el dispositivo de arranque pueda convertirse en un punto de acceso que limite los tipos de hardware admitidos. En una configuración de autoinstalación en la que un cliente usa su propio dispositivo como dispositivo de arranque, esto podría no ser posible.

Una posible solución al problema de arranque WiFi es usar un modelo de seguridad WiFi alternativo. WPA Enterprise es una alternativa al método tradicional de seguridad residencial, WPA2. En lugar de proporcionar un nombre de red y contraseña, un dispositivo se conecta al punto de acceso y proporciona un nombre de usuario y contraseña. Un servidor de autenticación RADIUS autentica al usuario permitiendo que el dispositivo se conecte a la red o rechaza el dispositivo, desconectándolo de la red. Esto requiere que el dispositivo que intenta conectarse tenga tres datos: nombre de red, nombre de usuario y contraseña. Un hogar podría crear un nombre de usuario y una contraseña para los dispositivos que se instalarán, aliviando el problema de tener que programar los dispositivos con esta información. Sin embargo, aún sería necesario programar el nombre de la red y si el nombre de la red cambia, los dispositivos tendrían que reprogramarse nuevamente. Otra alternativa sería configurar una red inalámbrica sin seguridad (abierta) y utilizar un portal cautivo para autenticar a los usuarios. Esto resuelve el problema de tener que programar un dispositivo con una contraseña, aunque crea nuevos problemas al no tener los datos transmitidos encriptados. Ambos enfoques no son características compatibles con los enrutadores inalámbricos de consumo estándar y requerirían una configuración avanzada para la configuración. No es aceptable esperar que un hogar los soporte para instalar dispositivos en el hogar. CORREA funciona sin modificaciones en el enrutador inalámbrico doméstico. Otra alternativa sería configurar una red inalámbrica sin seguridad (abierta) y utilizar un portal cautivo para autenticar a los usuarios. Esto resuelve el problema de tener que programar un dispositivo con una contraseña, aunque crea nuevos problemas al no tener los datos transmitidos encriptados. Ambos enfoques no son características compatibles con los enrutadores inalámbricos de consumo estándar y requerirían una configuración avanzada para la configuración. No es aceptable esperar que un hogar los soporte para instalar dispositivos en el hogar. CORREA funciona sin modificaciones en el enrutador inalámbrico doméstico. Otra alternativa sería configurar una red inalámbrica sin seguridad (abierta) y utilizar un portal cautivo para autenticar a los usuarios. Esto resuelve el problema de tener que programar un dispositivo con una contraseña, aunque crea nuevos problemas al no tener los datos transmitidos encriptados. Ambos enfoques no son características compatibles con los enrutadores inalámbricos de consumo estándar y requerirían una configuración avanzada para la configuración. No es aceptable esperar que un hogar los soporte para instalar dispositivos en el hogar. CORREA funciona sin modificaciones en el enrutador inalámbrico doméstico. Ambos enfoques no son características compatibles con los enrutadores inalámbricos de consumo estándar y requerirían una configuración avanzada para la configuración. No es aceptable esperar que un hogar los soporte para instalar dispositivos en el hogar. CORREA funciona sin modificaciones en el enrutador inalámbrico doméstico. Ambos enfoques no son características compatibles con los enrutadores inalámbricos de consumo estándar y requerirían una configuración avanzada para la configuración. No es aceptable esperar que un hogar los soporte para instalar dispositivos en el hogar. CORREA funciona sin modificaciones en el enrutador inalámbrico doméstico.

Otra forma de sortear este problema es no depender en absoluto del WiFi de un hogar y, en su lugar, utilizar la conectividad celular. Sin embargo, el uso de celulares puede tener un costo prohibitivo y podría no ser una opción para algunos tipos de dispositivos o implementaciones. Por esta razón, nos enfocamos en mejorar el arranque de WiFi.

Existen muchos enfoques para iniciar la conectividad inalámbrica de un dispositivo pequeño (uno sin pantalla o teclado) a un enrutador inalámbrico. Esbozamos algunos de los enfoques utilizados por los dispositivos IoT actuales. Un enfoque común es que el dispositivo IoT cree un punto de acceso temporal, lo que permite al usuario conectarse y programar el nombre y la contraseña de la red en el dispositivo. Muchas empresas, como Amazon, adoptan este enfoque para sus dispositivos Echo [13] , y es una característica estándar para muchos SoC WiFi, como Espressif ESP8266 [14] y TI CC3200 [15]. Por lo general, cuando un dispositivo se inicia por primera vez y no puede conectarse a una red, ingresa al modo de punto de acceso. Luego se le solicita al usuario que se conecte a la red temporal, generalmente a través de una aplicación de teléfono inteligente. Una vez conectado, el usuario ingresa el nombre y la contraseña de la red, generalmente a través de una aplicación, que programa el dispositivo. El dispositivo cambia del modo de punto de acceso al modo cliente y se conecta a la red. Si bien este enfoque funciona bien para algunos dispositivos, no se escala cuando se trata con muchos dispositivos. Tener que ingresar un nombre de red y contraseña rápidamente se vuelve engorroso y propenso a errores, especialmente cuando se implementan múltiples dispositivos en una sola instalación. Este enfoque también requiere algún tipo de aplicación de teléfono inteligente para guiar a un usuario a través de la configuración e ingresar las credenciales de WiFi.

Otro enfoque sería utilizar WiFi Protected Setup (WPS) [16]. La promesa de WPS es simplificar la conexión de un nuevo dispositivo a una red WiFi. Esto permite que un usuario tenga una red segura pero no tenga que ingresar una contraseña en el dispositivo. WPS tiene dos modos: PIN y botón pulsador. Con el modo PIN, una persona ingresa un PIN en el dispositivo que desea conectarse. El PIN proviene del enrutador inalámbrico, generalmente en la etiqueta en la parte inferior del enrutador inalámbrico. Con el segundo modo, presione el botón, se presiona un botón en el enrutador inalámbrico y en el dispositivo que desea conectarse. La información se intercambia entre las dos entidades, lo que permite que el dispositivo se conecte a la red. Si bien WPS parece abordar este problema de arranque, existen inconvenientes con la implementación. Primero, el modo PIN de WPS sufre ataques de fuerza bruta en línea y fuera de línea [17]. Como resultado, los expertos en seguridad recomiendan desactivar WPS [18] . En segundo lugar, WPS *no forma* parte de la especificación WiFi y, como resultado, no todos los enrutadores inalámbricos lo admiten. Dado que tanto el enrutador inalámbrico de la casa como los dispositivos que intentan conectarse deben ser compatibles con WPS para funcionar, no tener soporte completo hace que este enfoque sea inviable. CORREA no depende de una función del enrutador inalámbrico para funcionar y en su lugar utiliza tramas básicas de Ethernet.

Otra opción es utilizar un canal fuera de banda para comunicar el nombre y la contraseña de la red. Algunos dispositivos comerciales, como Google Home, utilizan Bluetooth con el fin de recibir información de asociación WiFi [19] . Otros dispositivos comerciales, como el Amazon Dash Button, utilizan "ultrasonido" para transmitir datos entre un teléfono inteligente y un dispositivo [20] . Con Bluetooth, una persona solo puede programar un dispositivo a la vez. Con ambos métodos, estos enfoques requieren hardware adicional y están estrechamente relacionados con una aplicación de teléfono inteligente. Nuestro enfoque no requiere ningún hardware adicional en el dispositivo o una aplicación de teléfono inteligente.

STRAP sobrecarga el propósito de las direcciones de origen y destino de las tramas Ethernet y 802.11 para codificar datos. Se utilizan enfoques similares para canales encubiertos. Los canales encubiertos WiFi se centran principalmente en dos métodos principales para transmitir información, el tiempo y el encabezado 802.11. Los canales encubiertos de sincronización WiFi codifican información en la sincronización entre cuadros [21] [22] . Los canales encubiertos que usan el encabezado 802.11 sobrecargan el propósito de un campo para transmitir datos, como lo hace STRAP con las direcciones de origen y destino. Dicho trabajo incluye la modificación del control de secuencia y los campos de control de fragmentos del encabezado MAC 802.11 [23] o el cambio de velocidad [24]. Otros canales encubiertos se centran en modificar los campos de IP y TCP que los dispositivos no usan o no suelen comprobar [25] .

**SECCION VI.**

## **Conclusión**

En este documento, hemos discutido la motivación, el diseño, la implementación y la evaluación de STRAP. STRAP permite la conectividad de arranque de múltiples dispositivos a la red inalámbrica de un hogar al mismo tiempo. Es un diseño novedoso que codifica datos en las direcciones de origen y destino de las tramas Ethernet. Nuestra evaluación muestra que STRAP funciona con una variedad de enrutadores y no tiene ningún efecto en la red cuando se ejecuta. También mostramos que STRAP es mucho más rápido en comparación con los enfoques convencionales para conectar dispositivos a la red inalámbrica de un hogar.

### EXPRESIONES DE GRATITUD

La investigación reportada en esta publicación fue apoyada por NIBIB del US NIH bajo el número de premio 1U54EB021973-01.