Improvement of a fully distributed decision making protocol for CRN

Adrián Fernández
Ms.C Free Software's student
Universitat Oberta de Catalunya
Gijón, Spain
adrianfernandez85[at]uoc.edu

Carles Garrigues Olivella
Ms.C Free Software's director
Universitat Oberta de Catalunya
Barcelona, Spain
cgarrigues[at]uoc.edu

***Abstract*—La deteción del espectro libre para las comunicaciones inalámbricas en un momento puntual es una tarea compleja cuyo desarrollo se simplica al realizarse de forma distribuida por una red de radio cognitiva. Sin embargo existes dificultades y vulnerabilidades de seguridad que han de ser tenidas en cuenta y solventadas a la hora de autenticar y validar los nodos de la red. Este artículo presenta una propuesta de mejora del protocolo fully distributed decision making protocol for CRN con el fin de llevar a cabo esta tarea de detección del espectro de una manera eficiente y segura.**

Keywords—redes de radio cognitiva, medicion del espectro, protocolo seguro, fully distributed decision making, protocolo distribuido.

I. INTRODUCTION

Conocer y aprovechar las bandas libres en un espectro es una tarea fundamental para las comunicaciones móviles. Sin embargo la tarea de monitorizar este espectro supone un reto importante a superar.

Una Solución para realizar dicha tarea se basa en la utilización de redes de radio cognitiva [1], en las cuales un conjunto de nodos, cuya cantidad puede variar, monitorizan el espectro electromagnético a su alrededor y son capaces de obtener conclusiones, tomar decisiones y adaptarse de una manera autónoma e independiente; en el momento que un nodo detecta un espectro libre puede comunicarlo al resto de nodos de la red para que estos conozcan la información y decidan si utilizarlo. A este tipo de redes, al igual que a todas las redes inalámbricas les afecta el problema del nodo oculto, ya que debido a la degradación en la calidad, la intensidad o posibles interferencias del entorno no todos los nodos están visibles y accesibles entre si.

Para solucionar este problema hay estudios que proponen utilizar Detección del Espectro Distribuido (Distributed Spectrum Sensing, DSS[2]), esta propuesta, pese a solucionar los problemas en la detección del espectro introducen nuevas restricciones de seguridad como la de tener un nodo principal estático que se encargue de validar al resto de nodos de la red mediante una infraestructura de clave pública.

El protocolo estudiado Fully Distributed Decision Maken Protocol for CRN[3] elimina esta restricción adaptando la solución a un escenario real en el cual tanto la tipología de la red como los propios nodos que la componen puede cambiar constantemente sin que esto suponga un problema. Este protocolo se basa en un sistema de reputación en el que a cada nodo se le asigna una puntuación en base a los resultados proporcionados previamente, esa reputación es usada para tener en cuenta los datos que proporcione de una manera ponderada para que los posibles errores que provengan de un nodo malicioso o en mal estado no repercutan negativamente en la decisión global tomada por la red de sensores.

En este artículo se propone una mejora de dicho algoritmo eliminando la dependencia de una infraestructura de clave pública, reduciendo así la complejidad de cálculo y el tráfico de red necesario para su implantación en un entorno real.

Antes de definir el nuevo protocolo en profundidad en los capítulos III, IV y V, se mostrarán las diferencias más significativas con su predecesor, además de establecer los requisitos y consideraciones oportunas de seguridad que se implantarán.

II. SEGURIDAD

Los riesgos de seguridad a los que se enfrenta una red de sensores son variados, desde fallos y errores en las lecturas o transmisiones debidos a la propia red hasta ataques malintencionados y premeditados con la intención de provocar una degradación en la calidad o el nivel del servicio.

Al igual que en el protocolo original se requiere del uso de cifrado para garantizar tanto la autenticidad de los nodos como la privacidad e integridad en las comunicaciones entre los mismos. Dado que estos nodos pueden ser pequeños equipo sin mucha capacidad computacional se utilizarán funciones hash y criptografía simétrica que no requiere gran potencia de cómputo pero sirven para gantizar los aspectos mencionados.

En este protocolo se elimina la necesidad, y por lo tanto el problema, de la autenticación de los nodos cuando pretenden unirse a la red. En su lugar se permite la libre adhesión de todo aquel que lo desee, dejándole un periodo de tiempo aislado en cuarentena, siendo escuchado y analizado por el resto de nodos hasta verificar si la información proporcionada es válida, momento en el cual pasaría a formar parte de pleno derecho de la red, o si no lo es, momento en el cual sería expulsado e ignorado.

En cuanto a la privacidad y la integridad de los mensajes, se toma como solución el cifrado mediante una clave simétrica

que forma parte de una cadena de claves generadas por cada nodo, las cuales son fácilmente verificables pero prácticamente imposibles de predecir. De esta forma los nodos pueden enviar su información firmada mediante su clave, posteriormente envían la clave que se utilizó, de esta forma el resto de la red puede verificar que la clave efectivamente era la siguiente de la cadena del nodo en cuestión, comprobando por lo tanto que el mensaje firmado fue enviado, y no alterado, por el nodo emisor.

Otro aspecto que se tiene en cuenta es el cálculo cuantitativo de las señales electromagnéticas del entorno de cada nodo, de esta forma un nodo no tiene la necesidad de tomar la decisión de si un espectro está libre o está siendo usado, únicamente ha de captar estas señales y enviar la medición a la red, liberándole de esta forma de tareas de cálculo. Gracias a esta característica también se añade una mayor tolerancia al ruido, ya que se trabaja con valores relativos sin poner límites absolutos a las mediciones.

Debido a que el funcionamiento de la red se basa en la confianza en los nodos a través de su reputación, es necesario que la infraestructura inicial en el momento de la puesta en funcionamiento sea correcta y legítima, de tal forma que sus decisiones sean fiables. Una vez que la red esté en funcionamiento se podrán añadir nuevos nodos desconocidos, ya que estos serán evaluados y tratados por el resto de una forma autónoma.

III. DIFERENCIAS CON SU PREDECESOR

Este protocolo pretende ser una evolución del Fully distributed decision making protocol for crn, por lo tanto está basado en él realizando ciertas modificaciones.

- Se elimina la infraestructura de clave pública, prescindiendo del requisito de que el nodo coordinador tenga acceso a internet para validar los certificados, por lo cual tampoco es necesario que ningún nodo disponga de certificado digital ni tenga que enviarlo para unirse a la red.
- Cualquier nodo puede ejercer el rol de coordinador, por lo tanto no es necesario que aquellos que dispongan de conexión a internet se anuncien como candidatos antes de la votación. También se elimina el problema de que en un momento dado sea necesario realizar un cambio de coordinador y no haya ningún candidato disponible. Ahora aunque haya un único nodo en la red, sea cual sea, podría ejercer el rol de coordinador de la red.
- Cuando la reputación de un nodo cae por debajo de cero no es expulsado de la red, en lugar de ello pasa a estar en modo invitado, esto quiere decir que sus datos serán escuchados por el resto, pudiendo con ello volver a recuperar su reputación si son correctos, pero no serán tenidos en cuenta a la hora de realizar el cálculo final.
- Se mantiene la tabla de reputación de cada nodo, sin embargo cuando un nuevo miembro ingresa en la red se le asigna por defecto un valor de *-2* por el resto. También se añade un contador que se inicializará en *5*. Esto implica que de sus cinco primeros envíos de datos han de ser correctos al menos tres para no ser expulsados de la red y pasar a estar admitidos.

IV. ELECCIÓN DEL NODO COORDINADOR

El rol del nodo coordinador se mantiene intacto del protocolo original, siendo este el encargado de verificar la validez de los mensajes de los nodos, además de calcular los resultados. La elección de este nodo está basada en su reputación, además esta reputación es conocida por todos ya que forma parte del contenido de los mensajes enviados, por lo tanto, en cualquier momento si un nodo detecta que existe otro con mayor reputación que el coordinador puede proponer su reemplazo.

El proceso de elección del nodo coordinador es el siguiente:

1. Un nodo con reputación suficiente, por lo tanto de confianza para el resto, propone la elección de un coordinador.
2. Cada nodo selecciona al que más reputación y envía su voto en texto claro y firmado mediante su clave.
3. Una vez terminada la votación cada nodo envía la clave para que se pueda verificar que tanto la firma como el voto eran correctos.
4. El ganador se escoge por mayoría simple, entonces el nodo coordinador actual envía un mensaje a todos anunciando el resultado mediante un mensaje firmado.
5. Después de haber enviado el resultado, el coordinador envía la clave utilizada para que nuevamente pueda ser verificada su firma.
6. Como las votaciones fueron públicas, se incrementa la reputación de aquellos nodos que votaron al ganador y se decrementa la de aquellos cuyos votos fueron para otro candidato, ya que sus datos no eran correctos.
    a. Si el 50% o más de los nodos no están de acuerdo con la elección del ganador se penaliza la reputación del coordinador por haber enviado un resultado que no es conforme a la mayoría y se realiza una nueva votación.

Los nodos conocen la reputación del resto de nodos de la red, por lo tanto solo se admitirán a trámite aquellas elecciones propuestas por un nodo cuya reputación haya sido verificada por lo demás que es positiva, en ningún caso por un nodo invitado o uno que no disponga de la suficiente fiabilidad. La reputación mínima para proponer una elección de coordinador es un parámetro que habrá que ajustar dependiendo de las condiciones particulares de cada red y cada situación concreta.

V. REGISTRO DE NUEVOS NODOS

Cuando un nodo pretende unirse a la red se siguen los siguientes pasos:

1. El nodo *Q* que se desea unir escoge un número aletaorio R_Q y prepara una cadena de hashes de longitud *N*, donde *N* es escogido de acuerdo a la disponibilidad de memoria de *Q*. Los valores de esta cadena de hashes serán utilizados como claves para el firmado de mensajes.

   $V_Q[N-1] = R_Q$

   $V_Q[N-2] = hash(R_Q)$

   $V_Q[N-3] = hash(hash(R_Q))$

   …

   $V_Q[0] = hash(V_Q[1])$

   El valor $V_Q[0]$ es la primera clave de firmado utilizada por el nodo *Q*. Esto implica que en el siguiente paso el resto de nodos conocerán este valor VQ[0], y una vez que *Q* transmita un mensaje firmado y posteriormente su clave $V_Q[1]$ los demás nodos podrán verificar que $V_Q[0]=hash(V_Q[1])$, sin embargo no les será posible predecir el valor de $V_Q[1]$ a partir de $V_Q[0]$.

2. El nuevo nodo anuncia su llegada y su deseo de incorporarse a la red.

3. Los nodos aceptan al nuevo incorporado en estado *invitado*. A este nodo se le asigna una reputación inicial de -2. Asímismo los nodos de la red crean un contador inicializado en 5, dicho contador se irá decrementando cada vez que el nodo invitado realice un envío de datos a la red.

4. Una vez que el contador llegue a 0 se expulsará al nodo de la red si su reputación es negativa, sin embargo se le permitirá unirse, ya sin el estatus de invitado, si llegado este momento dispone de una reputación positiva.

Los datos proporcionados por estos nodos invitados serán tenidos en cuenta únicamente para actualizar su reputación, pero en ningún caso para como parte del cálculo del resultado final.

VI. DETECCIÓN DEL ESPECTRO COOPERATIVA

Esta es la parte del proceso más crítica, ya que aquí es donde los nodos realizan la detección del espectro de una manera cooperativa para, entre todos, obtener un resultado final determinando si está libre o no. Por lo tanto en este proceso es donde los procesos de validación de datos y nodos adquiere una mayor importancia, ya que un nodo malicioso o con deficiencias en su funcionamiento podría enviar datos erroneos a la red y provocar que se obtenga el resultado incorrecto.

Para evitar estos posibles problemas es aquí donde se tiene en cuenta y se utiliza el mencionado sistema de reputación de los nodos, impidiendo que un nodo no fiable o malicioso pueda interferir en el buen funcionamiento de la red.

Cada nodo utilizará una tabla de reputación construida de la siguiente forma:

$ReputationTable = [[Id_1, Reputation_S[1], V_1[i]],…[Id_s, Reputation_S[S], V_S[j]]$

Donde *S* es el número total de nodos en la red en el momento actual, *Id* es el identificador del nodo, *Reputation* es la reputación almacenada para el nodo y *V* son las claves privadas que ha utilizado.

Para llevar a cabo la detección cooperativa del espectro se siguen los siguiente pasos:

1. El nodo coordinador anuncia el inicio de una ronda de detección, indicando el canal que será escaneado.

2. Cada nodo realiza la detección de manera independiente y genera un resultado propio, reportando la siguiente información:

   $Results = [Id_S, SensingResult_S, Sign_S]$

Siendo Id_S el identificador del propio nodo, $SensingResult_S$ el resultado obtenido durante la detección del espectro y $Sign_S$ la firma del mensaje.

3. El nodo coordinador espera a que se reciba la información de todos los nodos o a que se agote un tiempo de espera preestablecido. Una vez que ocurra uno de estos dos eventos envía un nuevo mensaje solicitando a los nodos que publiquen la clave que utilizaron para firmar su mensaje previo.

4. Cada nodo envía la clave utilizada en el paso 2.

5. Cada nodo construye un resultado final a partir de los datos recibidos, teniendo en cuenta la reputación de cada nodo mediante la función ponderada presentada por Chen en [4].

6. Los nodos calcula la varianza estadística entre los valores correspondientes a los nodos cuya decisión coincide con la decisión final.

7. Aquellos nodos cuyo resultado de la detección se encuentre dentro del rango Media±Varianza reciben un incremento de su reputación. Aquellos que proporcionasen un resultado fuera de ese rango serán penalizados.

8. El coordinador, envía sus resultados informando del resultado final, los cambios de reputación y las posibles expulsiones de nodos que hayan perdido toda su reputación, invitados que hayan sido aceptados y/o expulsados.

Si al menos el 50% de los nodos no están de acuerdo con los resultados publicados por el coordinador se anulará el proceso de detección, se penalizará la reputación del propio coordinador y se realizará una nueva elección de nodo coordinador.

VII. DISCUSIÓN

Una de las ventajas presentadas por el protocolo original es que permite introducir nuevos nodos en la red sin necesidad de tener que enviarles la reputación del resto de nodos y sus claves, en esta nueva versión, también se elimina la necesidad de que el nuevo nodo envíe su certificado y tenga que ser validado por el nodo coordinador frente a una autoridad de validación externa, sin que esto implique una pérdida en la seguridad de la red gracias al cambio del paradigma en la autenticación y en el sistema de reputación.

Se mantiene el bajo consumo de ancho de banda gracias a la poca necesidad de transmisiones de datos y a las funciones HMAC que pueden ser generadas y verificadas utilizando pocos recursos mediante los métodos propuestos por [5] y [6].

Se añade tolerancia a ruido y posibles deficiencias puntuales mediante el uso de la varianza se puede deliminar un rango de valores aceptables, de esta forma aunque el valor proporcionado por un nodo difiera ligeramente del valor correcto no será penalizado.

En cuanto a la seguridad el protocolo es invulnerable a ataques del tipo Man in the Middle debido a que todos los mensajes enviados por los nodos van firmados mediante una clave que únicamente estos pueden conocer, por lo tanto un atacante que intercepte estos mensajes podría leerlos, lo cual no tiene ninguna implicación ya que todos los mensajes que circulan por la red son públicos y no hay necesidad de ocultarlos, sin embargo no podrían ser alterados y enviados de nuevo ya que la firma delataría esta modificación.

En la defensa contra ataques de tipo Sybil se presentan cambios, aunque el protocolo sigue siendo resistente. Al prescindir de certificados, un nodo malicioso podría introducirse en la red y ser aceptado, sin embargo formaría parte con el rol de *invitado*, por lo tanto sus mediciones fraudulentas no te tendrán en cuenta y al no enviar datos correctos terminará siendo expulsado, por lo cual no podría conseguir inyectar datos corruptos.

No existe ningún nodo estático o con privilegios especiales que al ser vulnerado pueda comprometer toda la red, cualquier nodo puede ser ignorado o expulsado si su comportamiento no es el correcto, por lo tanto no existe un punto débil en la red por el que un atacante pudiera atacar.

REFERENCIAS

[1] J. Mitola III and G.Q. Maguire Jr. Cognitive radio: making software radios more personal. IEEE personal communications, 6(4):13–18, 1999.

[2] S.M. Mishra, A. Sahai, and R.W. Brodersen. Cooperative sensing among cognitive radios. In IEEE International Conference on Communications, pages 1658–1663. IEEE Computer Society, 2006.

[3] C. Garrigues, H. Rifà-Pous, G.Navarro-Arias, Fully Distributed Cooperative Spectrum Sensing for CRN, UOC.

[4] R. Chen, J.-M. Park, and K. Bian. Robust distributed spectrum sensing in cognitive radio networks. In INFOCOM. The 27th Conference on Computer Communications, pages 1876–1884. IEEE Computer Society, 2008.

[5] Y. Sella. On the computation-storage trade-offs of hash chain traversal. In Financial Cryptography, volume 2742 of LNCS, pages 270–285, 2003

[6] M. Fischlin. Fast verification of hash chains. In The Cryptographers' Track at the RSA Conference (CT-RSA), volume 2964 of LNCS, pages 339–352, 2004.