XVII Jornadas de Ingeniería Telemática
JITEL 2025
Universidad de Extremadura

Actas de las XVII Jornadas de Ingeniería Telemática (JITEL 2025), Cáceres (España), 12-14 de noviembre de 2025.

ISBN

DE-RCM: Desanonimización Explicable de MACs Aleatorias en 802.11 WLANs

Juan Manuel Montes-Lopez, Pablo Serrano, Marco Gramaglia, Aruna Prem Bianzino
Departamento de Ingeniería Telemática
Universidad Carlos III de Madrid
Avda. Universidad, 30. 28911 Leganés.
{jumontes, pablo, mgramagl, abianzin}@it.uc3m.es

El uso de WiFi puede revelar patrones de comportamiento que comprometen la privacidad. Para abordar este problema se han propuesto esquemas de Direcciones MAC Aleatorias y Cambiantes (RCM, por sus siglas en inglés) para modificar periódicamente las direcciones MAC, con el objetivo de desacoplar la identidad del dispositivo de sus patrones de uso. En este artículo diseñamos DE-RCM, un esquema que desanonimiza de forma explicable MACs aleatorias a partir datos históricos del comportamiento de los dispositivos WiFi. DE-RCM se basa en *random forests* y ofrece una precisión del 82% con tan sólo dos semanas de datos para el conjunto de 100 dispositivos considerado.

***Palabras Clave*—WiFi, RCM, desanonimización**

I. INTRODUCCIÓN

La actividad inalámbrica de los dispositivos móviles deja un rastro de información que puede utilizarse para identificar inequívocamente a los usuarios. Por ejemplo, para el caso de redes móviles, el trabajo [1] muestra que cuatro puntos espacio-temporales son suficientes para identificar al 95% de los individuos, mientras que para el caso de WiFi, en [2] se analiza cómo la superposición de redes preferidas revela vínculos sociales entre individuos.

Para evitar la relación tan estrecha entre comportamiento espacio-temporal e identidad, recientemente se ha propuesto el uso de Direcciones MAC Aleatorias y Cambiantes (RCM, por sus siglas en inglés), cuya idea clave es modificar la dirección MAC empleada en WiFi para reducir la cantidad de información asociable a un dispositivo. Existe una amplia variedad de esquemas RCM [3]; a modo de ejemplo, los dispositivos Android permiten tanto un esquema *persistente*, donde el dispositivo genera una dirección aleatoria por cada red (evitando unir información de diferentes redes), como un esquema *no persistente*, donde la dirección se cambia cada vez que se asocia a una red o pasadas 24 horas (con el objetivo de anonimizar dentro de la propia WiFi).

En este artículo, analizamos si, incluso bajo esquemas no persistente, existen patrones de uso que puedan servir para identificar inequívocamente a un usuario dentro de la misma red WiFi (nótese que tanto [1], [2] analizaron escenarios mucho más amplios). Para ello, analizamos las trazas de uso real de un conjunto de 28 voluntarios en un edificio universitario. Analizamos diferentes características diarias de sus dispositivos e identificamos ciertas características que pueden servir para identificar parcialmente un subconjunto de dispositivos. Aprovechando estas observaciones, diseñamos DE-RCM: Desanonimización Explicable de Direcciones MAC Aleatorias, basado en *random forests*. Evaluamos su rendimiento emulando un esquema RCM no persistente con un período diario, alcanzando una precisión en la desanonimización de hasta el 80%, en función de la cantidad de información previa disponible sobre la actividad del dispositivo. Gracias al uso de *random forests* y su correspondiente explicabilidad, nuestros resultados pueden ayudar a diseñar mejores algoritmos RCM.

II. DATOS EMPLEADOS

Los datos se obtienen de la red `eduroam` del Campus de Leganés de la Universidad Carlos III de Madrid (UC3M), que consta de 278 puntos de acceso (APs) desplegados en siete edificios,[1] la mayoría de los cuales tienen al menos tres plantas, y cada AP proporciona cobertura para aproximadamente 100 m^2. Cada vez que un dispositivo se asocia o reasocia con un AP diferente, el AP notifica a un servidor RADIUS; además, este servidor actualiza el estado de cada dispositivo con una periodicidad de al menos 15 minutos. Además de la información espacio-temporal, a saber, marca de tiempo, identificador de usuario, direcciones MAC del dispositivo y del AP al que está conectado, el servidor RADIUS también recopila el número total de bytes transmitidos y recibidos.

[1] https://www.uc3m.es/life-on-campus/campuses-plans/leganes

En este trabajo nos centramos en 28 voluntarios que aceptaron esta recopilación de datos, en su mayoría personal de investigación, lo que resultó en un total de 98 dispositivos diferentes durante un período de 15 meses. Obtenemos la información del servidor RADIUS a través de una API que protege las identidades de los usuarios y los dispositivos realizando un hash MD5 de los identificadores y las direcciones. Para simplificar, decidimos restringir nuestro análisis a un único edificio con 47 APs, ya que el 95% de los voluntarios pasaron la mayor parte de su tiempo asociados a alguno de estos APs.

III. ATRIBUTOS PARA LA DESANONIMIZACIÓN

En esta sección, analizamos diversos atributos de las trazas de los dispositivos que podrían servir para caracterizarlos inequívocamente.

A. Horas de llegada y salida

Primero analizamos tres características temporales: la hora de la primera y última conexión y el tiempo total de conexión. Estos aspectos son relevantes en nuestro entorno académico, donde los horarios y hábitos deberían reflejarse en las trazas obtenidas.

Nuestros resultados muestran que la mayoría de los dispositivos se conectan por primera vez alrededor de las 8 AM, explicable dado que la mayoría de los usuarios son investigadores. Se observa cierta variabilidad en las horas de conexión y desconexión entre las 6 AM y las 6 PM, lo que podría corresponder a los horarios menos regulares de algunos estudiantes. Por su parte, las horas de desconexión tienden a concentrarse alrededor de las 6 PM. Por último, en cuanto al tiempo total de conexión, lo más reseñable es que hay dispositivos que permanecen conectados durante la 24 horas, lo que sugiere que son equipos de escritorio o portátiles que permanecen en la red de forma continua.

En resumen, se confirma que la información temporal permite identificar parcialmente ciertos tipos de dispositivos, pero para una identificación más precisa se requiere información adicional.

B. Número de APs diferentes visitados

A continuación, analizamos el comportamiento de los dispositivos mientras están conectados a la red. En primer lugar, nos centramos en el grupo de dispositivos que permanecen siempre conectados, los cuales representan el 16% del total. Observamos que estos dispositivos se conectan constantemente a un único punto de acceso (AP), lo que sugiere que se trata de ordenadores portátiles o de escritorio sin conexión cableada.

Para el resto de dispositivos, calculamos el número de APs diferentes a los que se asocia (denotado como #APs) durante un período de tiempo de longitud T, que varía entre 1 día, 1 semana, 2 semanas y 1 mes. Más específicamente, calculamos para cada dispositivo el número medio de #APs para 250 períodos diferentes de longitud T[2]. Según los resultados: a) al considerar $T = 1$ día, #APs varía entre 1 y 10.3, con una media de 3.3 APs (nótese que nuestro análisis se limita a un solo edificio); b) al extender a $T = 1$ semana, los valores de #APs prácticamente se duplican, lo que indica una variación significativa al pasar de un patrón diario a uno semanal; c) para $T = 2$ dos semanas, el incremento de #APs de del 50%, mientras que d) para $T = 1$ mes, los resultados son prácticamente idénticos a los del caso anterior.

De acuerdo con estos resultados, se confirma que tanto un día o una semana pueden ser insuficientes para capturar la movilidad de un dispositivo, mientras que más de un mes puede resultar redundante.

C. Entropía

En la sección anterior se analizó el número de APs diferentes a los que se conectan los dispositivos, sin tener en cuenta el tiempo que pasa en cada AP. En esta sección se considera tanto el número de APs como el tiempo que pasa en cada uno mediante el cálculo de la *entropía H* de la traza, definida como [4] $H = \sum_{i=1}^{\#AP} p_i \log_2(p_i)$, donde p_i representa la cantidad relativa de tiempo que el dispositivo pasa en el AP i.[3]

Se representa la Función de Distribución Acumulada (CDF) de la entropía para cada dispositivo utilizando las mismas ventanas de tiempo consideradas anteriormente en la Fig. 1. Los principales resultados son: (1) independientemente T, casi el 20% de los dispositivos tienen una entropía cercana a cero, es decir, prácticamente no se mueven[4]; (2) la entropía crece con T, es decir, los dispositivos visitan más lugares diferentes a medida que se considera más tiempo; (3) hay poca diferencia en términos de entropía entre dos semanas y un mes, lo que sugiere que un valor umbral $T = 2$ semanas para capturar el patrón de movilidad de un dispositivo[5]; (4) además de los dispositivos con entropía cercana a cero, existe una notable variedad en términos de entropía entre los dispositivos, lo que confirma que esta métrica también podría servir para re-identificar dispositivos.

D. APs más frecuentes

Aquí analizamos los k APs a los que un dispositivo pasa más tiempo conectado, motivado por el trabajo previo de [2] que identificó que la lista de SSIDs preferidos de un dispositivo puede servir para revelar relaciones entre dispositivos. El primer desafío es el cálculo de k, ya que un valor muy pequeño no distinguirá entre dispositivos (p.ej.,

[2]Para minimizar posibles sesgos en nuestros resultados, seleccionamos aleatoriamente 250 períodos de T días de duración para cada dispositivo.

[3]Una entropía baja indica que se pasa la mayor parte del tiempo conectado a pocos APs, mientras que un valor alto indica que el tiempo de conexión está distribuido de manera más uniforme entre múltiples APs. Dado un valor de H, se puede estimar un *número efectivo* de ubicaciones distintas $L = 2^H$, que representa el número de $\#APs$ que, si se visitaran por igual, darían el mismo valor de H.

[4]Nótese que en la Sección A identificamos que el 16% de los dispositivos siempre están conectados a la red. Aquí hemos identificado que algunos dispositivos, *cuando están conectados*, prácticamente siempre están conectados al mismo AP.

[5]Por ejemplo, la entropía al considerar un día es $H = 0.40$, es decir, una movilidad efectiva a lo largo de $L = 2^{0.40} = 1.32$ APs, mientras que para los casos de una semana, dos semanas y un mes, la movilidad efectiva sería de 1.74, 1.96 y 1.99, respectivamente.

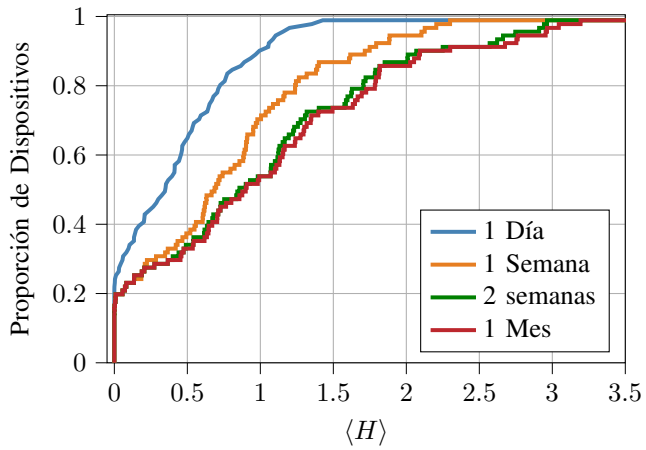

Fig. 1. ECDF de la Entropía H.

usuarios que comparten despacho), mientras que un valor excesivamente grande podría clasificar como diferentes dos días distintos del mismo usuario. Para determinar el valor adecuado de k, consideramos los seis APs más utilizados y calculamos el porcentaje promedio de tiempo que pasan conectados a ellos, lo que revela que la mayoría de los dispositivos pasan alrededor del 70% en el AP más frecuente y un 20% adicional en el segundo AP más común. En consecuencia, un dispositivo dedica el 90% de su tiempo de conexión en $k = 2$ APs, valor que usaremos para nuestro análisis posterior.

A continuación, analizamos para este valor de k cuántos dispositivos son *únicos*, es decir, ningún otro dispositivo tiene los mismos dos APs más frecuentes en el mismo día. Según nuestros resultados, el 88% de los dispositivos tienen una pareja de APs que los hacen únicos cada día. También medimos cuántas veces a lo largo de los días un dispositivo tiene el mismo par de APs más frecuentes: sólo el 33% de los dispositivos. De esta manera, aunque la tupla de $k = 2$ de los APs más comunes puede servir para caracterizar un dispositivo en un día determinado, esta característica es insuficiente para identificar unívocamente a un dispositivo a lo largo de varios días.

E. Tráfico descargado

Como última característica que pueda servir para identificar a los dispositivos analizamos el tráfico descargado por día (previa confirmación que el tráfico de subida es directamente proporcional al tráfico descargado). Según nuestros resultados preliminares, la distribución sigue una *ley de potencias*, que revela una cola pesada sugiriendo tanto la presencia de tráfico de *streaming* o actualizaciones importantes de software, como transferencias de datos de mucha menor envergadura (como navegación o actividades en segundo plano). De esta manera, el tráfico descargado también podría servir para identificar a ciertos usuarios. Además, observamos que, en promedio, los dispositivos consumen aproximadamente 350 MB de datos mientras están conectados a la red (ligeramente por debajo del consumo diario promedio en España de 400 MB[6]).

IV. DISEÑO DE DE-RCM

En esta sección se presenta DE-RCM, el algoritmo de desanonimización para reidentificar un dispositivo comparando sus características diarias actuales con las calculadas a partir de la actividad de los últimos T días. DE-RCM se basa en *Random Forests*, método basado a su vez en Árboles de Decisión que mejora el rendimiento y la robustez al promediar las predicciones de múltiples árboles entrenados en diferentes subconjuntos de datos. Para interpretar los resultados, utilizamos LIME [5], que aproxima las predicciones del modelo con un modelo interpretable alrededor de instancias específicas. En este trabajo, decidimos utilizar *random forests* con árboles poco profundos para la clasificación, debido a su mayor precisión y eficacia con datos limitados [6].

A. Generación de instancias

Calculamos el *perfil* diario de dispositivo basándonos en los atributos presentados. El perfil del dispositivo i en un día se define como $\mathbf{x}_i = (T_s,\ t_a,\ \#APs,\ H, [APs], D)$, donde T_s representa el tiempo total en la red, t_a la hora de llegada, $\#APs$ el número de puntos de acceso diferentes visitados, H la entropía, $[APs]$ los dos puntos de acceso más comunes, y D el tráfico total descargado. La desanonimización requiere determinar si dos perfiles pertenecen al mismo dispositivo o no, comparando sus características mediante un clasificador. Para generar instancias para el clasificador, dados dos perfiles $\mathbf{x}_i$ y $\mathbf{x}_j$ se calcula la tupla $(\mathbf{\Delta x}_{i,j}, \delta_{i,j})$, donde $\Delta \mathbf{x}_{i,j}$ representa la diferencia numérica entre los perfiles[7] comparados, mientras que $(\delta_{i,j})$ es una etiqueta binaria, con un valor de 1 si los perfiles corresponden al mismo dispositivo y 0 en caso contrario.

B. Proceso de inferencia

Una vez entrenado el modelo con información de días previos, comparamos el perfil de un dispositivo desconocido con los perfiles del conjunto de entrenamiento, calculando las diferencias correspondientes y asignando al dispositivo desconocido la identidad del dispositivo con menor diferencia. Matemáticamente, sea $\{d\}$ el conjunto de dispositivos conocidos y $\{\mathbf{x_t}\}_d$ como el conjunto de perfiles para un dispositivo específico d del conjunto de entrenamiento. Sea d_n el dispositivo desconocido y su vector de características $\mathbf{x_n}$. La desanonimización consiste en encontrar el dispositivo con la mayor probabilidad promedio de coincidir, esto es:

$$d_n = \arg\max_d \left(\frac{1}{T_d} \sum_{t=0}^{t=T_d} P(y = 1 | \Delta \mathbf{x_{t,n}}) \right) \qquad (1)$$

donde $\Delta \mathbf{x_{t,n}}$ es la diferencia entre el perfil del dispositivo d en el día t y el perfil del nuevo dispositivo d_n y $P\left(y = 1 | \Delta \mathbf{x_{t,n}}\right)$ es la probabilidad de que los perfiles correspondan al mismo dispositivo.

[6]https://bandaancha.eu/articulos/consumo-datos-moviles-linea-alcanza-12-11043

[7]Para $[APs]$, calculamos la superposición de la lista de APs, que varía de 0 (sin superposición) a 2 (misma lista)

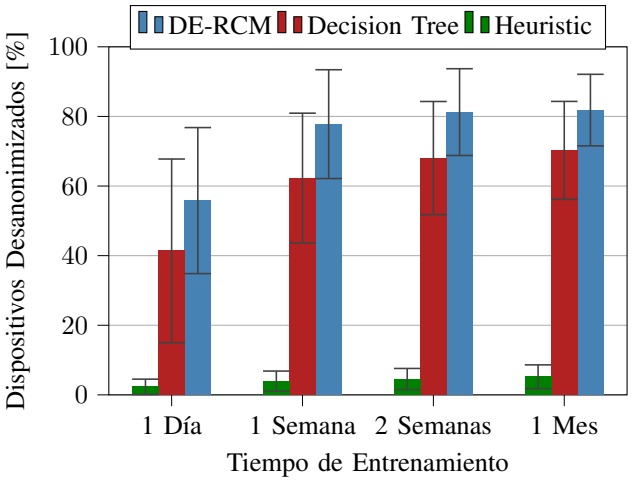

Fig. 2. Precisión para diferentes periodos de entrenamiento T.

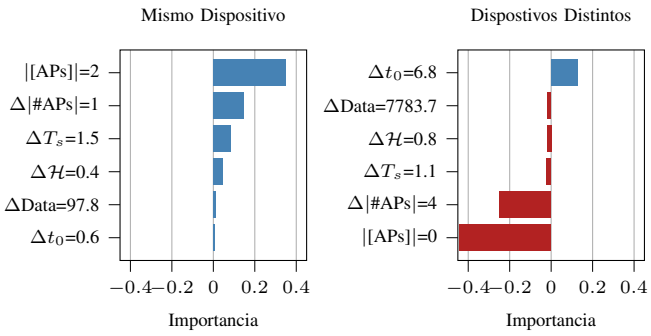

Fig. 3. Explicabilidad de las decisiones de DE-RCM.

V. ANÁLISIS DE PRESTACIONES

A continuacion evaluamos el rendimiento de DE-RCM, comparándolo con: *Decision Tree*, un modelo que clasifica dividiendo recursivamente en subconjuntos basados en los atributos, y *Heurístico*, un clasificador basado exclusivamente en los $k = 2$ APs más visitados.

A. Precisión

Primero, analizamos la precisión de DE-RCM para diferentes valores del período de entrenamiento T. Al igual que en los casos anteriores, para minimizar los sesgos, seleccionamos aleatoriamente 250 períodos de T días consecutivos, entrenamos el modelo en cada período y probamos su capacidad para identificar los perfiles de los dispositivos al día siguiente. La precisión se define como la proporción de dispositivos identificados correctamente sobre el número total de dispositivos en ese día.

En la Fig. 2 se presenta la precisión para DE-RCM y los otros métodos. Según los resultados, incluso con $T = 1$ día, DE-RCM alcanza un 55%, mucho más que una elección al azar (aprox. el 3%). La precisión mejora cuanto mayor es T, con más del 80% con 2 semanas. Como referencia, el rendimiento del heurístico es muy bajo, alcanzando como máximo una tasa de éxito del 5% (ligeramente superior al azar), mientras que el árbol de decisión alcanzar una precisión del 70%, es decir, un 10% peor que DE-RCM (y sin explicabilidad).

B. Explicabilidad

Aquí ilustramos la capacidad de DE-RCM para producir desanonimización explicable, aprovechando el peso relativo de los atributos LIME. Por simplicidad, nos centramos en $T = 2$ semanas. En la Fig. 3 representamos la explicación proporcionada por LIME para una identificación correcta del mismo dispositivo en diferentes días (figura de la izquierda), y una identificación correcta de diferentes dispositivos (figura de la derecha). Según estos resultados, la característica más influyente en el proceso de clasificación es la lista de los APs más comunes, $[APs]$. Más específicamente, la decisión de *mismo dispositivo* está motivada por tener una lista idéntica de los APs más comunes (fila superior) y valores similares para el resto de los parámetros (tiempo total, entropía, etc.), mientras que la decisión de *dispositivo diferente* está motivada por diferentes listas de los APs más comunes (fila inferior) y número de diferentes APs visitados, con valores similares para el resto de los parámetros.

VI. RESUMEN Y TRABAJO FUTURO

Hemos presentado un prometedor método para desanonimizar trazas que empleen RCM, validado con un conjunto reducido de usuarios. Para un trabajo futuro estamos ampliando el número de dispositivos estudiados, y empleando los resultados de explicabilidad para mejorar el diseño de los métodos RCM.

AGRADECIMIENTOS

Agradecemos a Rafael Calzada por su apoyo en el proceso de recolección y a Jose Furones por su guía en protección de datos. También agradecemos a Emmanuel Mera por los análisis iniciales. Este trabajo ha sido financiado por el Programa de Investigación e Innovación Horizon-JU-SNS-2022 de la Unión Europea (No. 101139198, iTrust6G), por el Ministerio de Asuntos Económicos y Transformación Digital de España y la Unión Europea-NextGenerationEU a través de los proyectos UNICO 5G I+D 6G-RIEMANN y 6G-SORUS, y por la Comunidad de Madrid (ORDEN 5696/2024) a través del proyecto TUCAN6-CM (TEC-2024/COM-460).

REFERENCIAS

[1] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the Crowd: The privacy bounds of human mobility," *Scientific Reports*, vol. 3, p. 1376, 2013.

[2] M. Cunche, M. A. Kaafar, and R. Boreli, "I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests," in *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2012, pp. 1–9.

[3] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of mac address randomization in mobile devices and when it fails," 2017.

[4] X. Lu, E. Wetter, N. Bharti, A. J. Tatem, and L. Bengtsson, "Approaching the Limit of Predictability in Human Mobility," *Scientific Reports*, vol. 3, no. 1, p. 2923, Oct. 2013.

[5] M. T. Ribeiro, S. Singh, and C. Guestrin, ""Why Should I Trust You?": Explaining the Predictions of Any Classifier," Aug. 2016. [Online]. Available: http://arxiv.org/abs/1602.04938

[6] T. C. Au, "Random Forests, Decision Trees, and Categorical Predictors: The "Absent Levels" Problem," Oct. 2018, arXiv:1706.03492 [cs, stat]. [Online]. Available: http://arxiv.org/abs/1706.03492