Refinamiento Probabilístico del Ataque de Revelación de Identidades

Alejandra Guadalupe Silva Trujillo, Javier Portela García-Miguel, Luis Javier García Villalba
Grupo de Análisis, Seguridad y Sistemas (GASS), Departamento de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid, España
Email: {asilva, javiergv}@fdi.ucm.es, jportela@estad.ucm.es

***Resumen*—En la actualidad muy pocas empresas reconocen que se encuentran continuamente en riesgo al estar expuestos a ataques informáticos tanto internos como externos. Más allá de simplemente instalar herramientas de protección contra hackers y células del crimen organizado tales como antivirus y firewalls, deben incluir mecanismos adecuados de seguridad en TI que brinden protección a los ataques que son cada vez más complejos. Existen diversos estudios que muestran que aún cuando se aplique el cifrado de datos en un sistema de comunicación, es posible deducir el comportamiento de los participantes a través de técnicas de análisis de tráfico. En este artículo presentamos un ataque a un sistema de comunicación anónimo basado en el ataque de revelación de identidades. El refinamiento probabilístico presenta una mejora sustancial respecto al ataque previo.**

***Palabras clave*—Análisis de tráfico, ataques estadísticos de revelación, comunicaciones anónimas, privacidad.** ***(Traffic analysis, statistical disclosure attacks, anonymous communications, privacy)*.**

I. Introducción

Empresas, organizaciones y sociedad generan millones de datos diariamente desde diferentes fuentes tales como: operaciones comerciales y mercantiles, redes sociales, dispositivos móviles, documentos, entre otros. La mayor parte de esta información se almacena en bases de datos altamente sensibles. Se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual y cualquier otro que pueda utilizarse para generar un daño, llámese robo de identidad, extorsión ó fraude por mencionar algunos.

La seguridad en los *data centers* se ha vuelto una de las grandes prioridades ya que tanto los ladrones de datos y células del crimen organizado buscan insistentemente infiltrarse en el perímetro de defensas a través de complejos ataques con un éxito alarmante, derivando en efectos devastadores. Hoy en día estamos inmersos en una sociedad digital donde podemos organizar un evento y enviar una invitación por Facebook; compartir fotos con amigos por medio de Instagram; escuchar música a través de Spotify; preguntar la ubicación de una calle utilizando Google Maps. La información personal es protegida por medio de la legislación y aunque no en todos los países se aplique efectivamente, en el ámbito de la sociedad digital funciona de manera diferente [1]. Toda la información disponible acerca de una persona puede ser referenciada con otra y dar lugar a prácticas de violación de la intimidad.

Cada persona tiene el derecho de controlar su información personal y proporcionarla a ciertas terceras partes. Desde la década pasada se observa una mayor preocupación por cómo se maneja la información privada de los usuarios en el ámbito gubernamental y de las empresas. Y recientemente, después de la filtración de información de un técnico estadunidense de la CIA al mundo, aumentaron las mesas de diálogo, investigaciones y fundamentalmente se creó toda una polémica en torno a la privacidad de los datos y lo expuesto que estamos a ser objetos de monitorización.

Las organizaciones privadas y públicas, así como las personas deben incluir la protección de la privacidad más allá de los típicos aspectos de integridad confidencialidad y disponibilidad de los datos. Aplicaciones utilizadas para garantizar la protección de la privacidad son por ejemplo los sistemas de resistencia a la censura, espionaje, entre otros; algunos de ellos utilzados para ofrecer seguridad a disidentes o periodistas viviendo en países con regímenes represores. Dentro de la misma rama de tecnologías, también existen mecanismos utilizados para acelerar la transición de cifrado como un servicio, que incluye cifrado basado en hardware con almacenamiento de llaves, esquemas de protección centralizada de datos para aplicaciones, bases de datos, ambientes virtuales de almacenamiento, y controles de acceso basados en roles.

Los ataques en las redes de comunicación son un serio problema en cualquier organización. Las nuevas tecnologías tienen un gran reto al buscar mejorar soluciones de seguridad para centros de datos. Se ha probado que el análisis de tráfico y la topología de una red, no proporcionan suficiente protección en la privacidad de los usuarios aún cuando se apliquen mecanismos de anonimato, ya que a través de información auxiliar, un atacante puede ser capaz de menguar sus propiedades. En el contexto de las redes de comunicación, con el análisis del tráfico se puede deducir información a partir las características observables de los datos que circulan por la red tales como: el tamaño de los paquetes, su origen y destino, tamaño, frecuencia, temporizacion, entre otros.

En este artículo nos enfocamos en mostrar cómo el análisis de tráfico de datos puede comprometer el anonimato de un sistema de comunicación anónima a través de técnicas y métodos que arrojen como resultado los patrones de comunicación de

ISBN: 978-84-9717-323-0

los elementos que la componen.

La composición del presente artículo es de la siguiente manera, en primer lugar la introducción. En la sección II abordamos el estado del arte. La siguiente sección describe el algoritmo utilizado, haciendo énfasis en el refinamiento probabilístico. En la sección IV presentamos la aplicación del algoritmo. Y finalmente en la sección V mostramos las conclusiones sobre los resultados y trabajos futuros

II. Estado del arte

II-A. Privacidad

La definición de privacidad de acuerdo a [2] es el derecho de un individuo a decidir qué información acerca de él mismo puede ser comunicada a otro y bajo qué circunstancias.

Economistas, sociólogos, historiadores, abogados, ingenieros en sistemas informáticos, por mencionar algunos, han adoptado su propia definición de privacidad, tal como su valor, alcance, prioridad y curso de estudio. Detalles relacionados a los antecedentes, legislación e historia de la privacidad se muestran en [3]. De acuerdo a los expertos, privacidad e intimidad son conceptos difíciles de definir; consideramos parte de ello: las condiciones de salud, identidad, orientación sexual, comunicaciones personales, preferencias religiosas, estados financieros, además de muchas otras características. Trabajos relacionados en cómo las PETs se han aplicado desde áreas del entorno económico, social y técnico [4].

Las bases de la legislación respecto a la privacidad datan del año 1948, en la Declaración Universal de Derechos Humanos donde se estableció que ninguna persona debía ser sujeta a interferencias arbitrarias en su privacidad, familia, hogar o correspondencia, así como a su honor y reputación. Pero, a pesar de los avances políticos y legales que se han dado, no ha sido posible resolver algunos de los problemas fundamentales para evitar los abusos que se dan todos los días. La falta de claridad y precisión en los derechos a la libertad de expresión y los límites de información son un problema latente.

El desarrollo e los medios de comunicación digital, el auge de las redes sociales, la facilidad de acceso a dispositivos tecnológicos, está permeando la tranquilidad de miles de personas en su vida pública y privada. Ejemplos abundan, como el caso de una funcionaria de una localidad belga, quien fue sorprendida y videograbada mientras mantenía relaciones sexuales en las oficinas del Ayuntamiento. La grabación fue realizada y subida a Internet por un grupo de jóvenes. Otro escándalo se dio cuando el presidente del Instituto de Seguridad Social de Guatemala quién fue filmado en su oficina cuando realizaba actos poco legales. A diferencia del primer caso, en éste último sí existía un crimen que perseguir y la acción se justificaba para dar a conocer los hechos públicamente.

Como éstos, muchos más casos son parte del material disponible en internet y en los medios convencionales, como los videos que se filtraron de la Viceministra de Cultura y Juventud de Costa Rica, y del concejal del PSOE en Yébenes, España. A nadie parece importar los efectos que continúan afectando vidas, donde la indiferencia parece ser la constante. La participación de los derechos humanos nacionales e internacionales, el gobierno, los medios de comunicación así como la sociedad parecen estar lejanos de este problema. El escándalo a expensas de la intrusión y diseminación de la vida privada e íntima de las personas es inaceptable. Es un círculo vicioso que tiene su origen en la violación de un derecho, pero más cuando se lleva a las redes sociales y de ahí a la mayoría de los medios de comunicación con el pretexto de ser noticia.

II-B. Privacy Enhancing Technologies

La Comisión Europea define las Tecnologías que mejoran la privacidad [5] como “El uso de los PETs puede ayudar a diseñar sistemas de comunicación y servicios de forma que minimiza la recolección y uso de datos personales y facilita el cumplimiento con la regulación de protección de datos”. No hay una definición aceptada por completo de las PETs, así como tampoco existe una clasificación. La literatura relacionada a las categorías de los PETs de acuerdo a sus principales funciones, administración de privacidad y herramientas de protección de privacidad [6] [7] [8]. En general las PETs son observadas como tecnologías que se enfocan en:

a. Reducir el riesgo de romper principios de privacidad y cumplimiento legal.
b. Reducir al mínimo la cantidad de datos que se tienen sobre los individuos.
c. Permitir a los individuos a mantener siempre el control de su información.

Varios investigadores se han centrado en proteger la privacidad y los datos personales por medio de técnicas criptográficas. Las aplicaciones PETs tales como seguros digitales individuales o administradores virtuales de identidad se han desarrollado para plataformas confiables de cómputo. Tradicionalmente las PETs han estado limitadas para proporcionar pseudononimato [9]. En contraste a los datos totalmente anónimos, el pseudononimato permite que datos futuros o adicionales sean relacionados a datos actuales. Este tipo de herramientas son programas que permiten a individuos negar su verdadera identidad desde sistemas electrónicos que operan dicha información y sólo la revelan cuando sea absolutamente necesario. Ejemplos incluyen: navegadores web anónimos, servicios email y dinero electrónico. Para dar un mejor enfoque acerca de las PETs, consideremos la taxonomía de Solove [10] utilizada para categorizar la variedad de actividades que afectan la privacidad. Para mayor información respecto a las propiedades de privacidad en escenarios de comunicación anónimos vea [9].

- Recolección de información: Vigilancia, Interrogatorio.
- Procesamiento de la Información: Agregación, Identificación, Inseguridad, Uso secundario, Exclusión.
- Difusión de la Información: Violación de la confidencialidad, Divulgación, Exposición, Aumento de la accesibilidad, Chantaje, Apropiación, Distorsión.
- Invasión: Intrusiones, Interferencia en la toma de decisiones.

La recolección de la información puede ser una actividad dañina, aunque no toda la información es sensible, ciertos

datos definitivamente lo son. Cuando la información es manipulada, utilizada, combinada y almacenada. se etiqueta a dichas actividades como Procesamiento de la información; cuando la información es liberada, encaja en las actividades conocidas como Difusión de la información. Finalmente, el último grupo de las actividades es la Invasión que incluye violaciones directamente a individuos. Todas estas actividades son parte de las prácticas comunes de las compañías que se dedican a recolectar información, como la preferencia de compras, hábitos, nivel educativo, entre otros. Todo ello por medio de múltiples fuentes para propósitos de venta.

En otras sub-disciplinas de las ciencias computacionales, la privacidad también ha sido motivo de investigación principalmente en como las soluciones de privacidad se pueden aplicar en contextos específicos. En otras palabras, definir el proceso de cuándo y cómo deben aplicarse las soluciones de privacidad. Antes de elegir una tecnología de la protección de privacidad surgen varias preguntas que deben responderse dado que no existe la certeza de que una tecnología soluciona un problema en específico. Una de las preguntas a considerar es quién define qué es la privacidad, el diseñador de tecnologías, los lineamientos de la organización, o los usuarios [11].

II-C. Comunicaciones anónimas

Las comunicaciones anónimas tienen como objetivo ocultar las relaciones en la comunicación. Dado que el anonimato es el estado de ausencia de identidad, las comunicaciones anónimas se pueden lograr removiendo todas las características identificables de una red anónima. Consideremos a un sistema donde se concentra un conjunto de actores en una red de comunicación, tales como clientes, servidor y nodos. Estos actores intercambian mensajes por medio de canales públicos de comunicación. Pitfzmann y Hansen [9] definieron el anonimato como el estado de ser no identificable dentro de un conjunto de sujetos, conocido como el conjunto anónimo. Una de las principales características del conjunto anónimo es su variación en el tiempo. La probabilidad que un atacante puede efectivamente revelar quién es el receptor de un mensaje es exactamente de $1/n$, siendo n el número de miembros en el conjunto anónimo. La investigación en esta área se enfoca en desarrollar, analizar y llevar a cabo ataques de redes de comunicación anónimas. La infraestructura del Internet fue inicialmente planteado para ser un canal anónimo, pero ahora sabemos que cualquiera puede espiar la red. Los atacantes tienen diferentes perfiles tales como su área de acción, rango de usuarios, heterogeneidad, distribución y localización. Un atacante externo puede identificar patrones de tráfico para deducir quiénes se comunican, cuándo y con qué frecuencia.

En la literatura se ha clasificado a los sistemas de comunicación anónima en dos categorías: sistemas de alta latencia y baja latencia. Las primeras tienen como objetivo proporcionar un fuerte nivel de anonimato pero son aplicables a sistemas con actividad limitada que no demandan atención rápida tal como el correo electrónico. Por otro lado, los sistemas de baja latencia ofrecen mejor ejecución y son utilizados en sistemas de tiempo real, como por ejemplo aplicaciones web, mensajería instantánea entre otros. Ambos tipos de sistemas se basan en la propuesta de Chaum [12], quién introdujo el concepto de *mix*. El objetivo de una red de *mixes* es ocultar la correspondencia entre elementos de entrada con los de salida, es decir encubrir quien se comunica con quien. Una red de *mixes* reúne un cierto número de paquetes de usuarios diferentes llamado el conjunto anónimo, y entonces a través de operaciones criptográficas cambia la apariencia de los paquetes de entrada, por lo que resulta complicado para el atacante conocer quiénes se comunican. Los *mixes* son el bloque base para construir todos los sistemas de comunicación de alta latencia [12]. Por otro lado en los últimos años, se han desarrollado también sistemas de baja latencia, como por ejemplo: Crowds [13], Hordes [14], Babel [15], AN.ON [16], Onion routing [17], Freedom [18] and Tor [19]. Actualmente, la red de comunicación anónima más utilizado es Tor, que permite navegar de manera anónima en la web. En [20] se muestra un comparativo de la ejecución de sistemas de comunicación de alta y baja latencia.

II-D. Redes mixes

En 1981, Chaum introduce el concepto de las redes *mixes* cuyo propósito es ocultar la correspondencia entre elementos de entrada con los de salida. Una red de mixes recolecta un número de paquetes desde diferentes usuarios llamado el conjunto anónimo, y entonces cambia la apariencia de los paquetes de entrada a través de operaciones criptrográficas. Lo anterior hace imposible relacionar entradas y salidas. Las propiedades de anonimato serán más fuertes en tanto el conjunto anónimo sea mayor. Un *mix* es un agente intermediario que oculta la apariencia de un mensaje, incluyendo su longitud. Por ejemplo, supongamos que Alice genera un mensaje para Bob con una longitud constante. Un protocolo emisor ejecuta varias operaciones criptográficas a través de las llaves públicas de Bob. Después, la red *mix* oculta la apariencia del mensaje al decodificarlo con la llave privada del *mix*.

El proceso inicial para que Alice envíe un mensaje a Bob utilizando un sistema de *mixes* es preparar el mensaje. La primera fase es elegir la ruta de transmisión del mensaje; dicha ruta debe tener un orden específico para enviar iterativamente antes de que el mensaje llegue a su destino final. La siguiente fase es utilizar las llaves públicas de los *mixes* elegidos para cifrar el mensaje, en el orden inverso en que fueron elegidos. En otras palabras la llave pública del último *mix* cifra inicialmente el mensaje, después el penúltimo y finalmente la llave pública del primer *mix* es usada. Cada vez que se cifra el mensaje una capa se construye y la dirección del siguiente nodo es incluida. De esta manera cuando el primer *mix* obtiene un mensaje preparado, dicho mensaje será descifrado a través de la llave privada correspondiente y será direccionado al siguiente nodo.

Los ataques externos se ejecutan desde fuera de la red, mientras que los internos son desde nodos comprometidos los cuales son de hecho parte de la misma red. Las redes de *mixes* son una herramienta poderosa para mitigar los ataques externos al cifrar la ruta emisor- receptor. Los nodos

participantes de una red *mix* transmiten y retardan los mensajes con el fin de ocultar su ruta. Pero es posible que puedan estar comprometidos y llevar a cabo ataques internos. Este tipo de problema se trata en [13] al ocultar el emisor o receptor de los nodos de transmisión.

II-E. Análisis de tráfico

El análisis de tráfico pertenece a la familia de técnicas utilizada para deducir información de los patrones de un sistema de comunicación. Se ha demostrado que el cifrado por sí mismo no garantiza el anonimato. Aún cuando el contenido de las comunicaciones sean cifradas, la información de enrutamiento debe enviarse claramente ya que los ruteadores deben determinar el siguiente punto de la red a dónde se direccionará el paquete. En [21] se muestran algunos de las técnicas de análisis de tráfico utilizadas para revelar las identidades en una red de comunicación anónima.

II-F. Ataques estadísticos

La familia de ataques estadísticos fue iniciada por Danezis en [22] donde introdujo el ataque estadístico de revelación (*Statistical Disclosure Attack, SDA*). En dicho trabajo se nota que llevando a cabo un amplio número de observaciones por cierto período de tiempo en una red de *mixes*, se puede calcular la probabilidad de distribuciones de envío/recepción de mensajes y con ello menguar la identidad de los participantes en un sistema de comunicación anónimo. A partir de éste ataque se desarrollaron muchos más tomando como base el análisis de tráfico para deducir cierta información a partir de los patrones de comportamiento en un sistema de comunicación.

Los ataques contra redes de *mixes* son conocidos también como ataques de intersección [23]. Se toma en cuenta la secuencia de un mensaje a través de una misma ruta en la red, esto quiere decir que se analiza el tráfico. El conjunto de los receptores más probables se calcula para cada mensaje en la secuencia e intersección de los conjuntos lo que permite conocer quién es el receptor de un determinado mensaje. Los ataques de intersección se diseñan basándose en la correlación de los tiempos donde emisores y receptores se encuentran activos. Al observar los elementos que reciben paquetes durante las rondas en las que Alice está enviando un mensaje, el atacante puede crear un conjunto de receptores más frecuentes de Alice. La información proporcionada a los atacantes es una serie de vectores representando los conjuntos de anonimato observados de acuerdo a los t mensajes enviados por Alice. Dentro de la familia de ataques estadísticos, cada uno de ellos se modela con un escenario muy específico; y en algunos casos poco semejantes al comportamiento de un sistema de comunicación real. Algunos asumen que Alice tiene exactamente m receptores y que envía mensajes a cada uno de ellos con la misma probabilidad, o bien son ataques que se enfocan en un solo usuario como soluciones individuales que son interdependientes, cuando la realidad indica cuestiones diferentes.

III. ALGORITMO

El objetivo de nuestro algoritmo es extraer información relevante sobre las relaciones entre cada par de usuarios. En [24] se describe el problema, así como el marco base y supuestos. Las tablas de las rondas donde se muestran los patrones de comunicación entre usuarios se representan con valores de 1 si existe relación y 0 en caso contrario. El atacante es capaz de observar cuántos mensajes son enviados y recibidos, es decir las sumas marginales por fila y columna de cada ronda 1, ...,T donde T es el número total de rondas. En cada ronda sólo consideramos usuarios que reciben y envían mensajes. Por lo tanto, decimos que un elemento (i, j) está presente en una ronda si las marginales correspondientes son diferentes a 0.

Hemos adoptado el término "cero trivial", que son los elementos que representan pares de usuarios que nunca han coincidido en ninguna ronda, Denotando n_{ij} el contenido del elemento (i, j), n_{i+} el valor marginal de la fila i, n_{+j} el valor marginal de la columna j, n la suma de los elementos y r el número de filas.

Algoritmo 1: Descripción del algoritmo

1. Generar n_{11} de una distribución uniforme entera donde $i = 1, j = 1$;
2. Iniciar un recorrido por columnas, para cada elemento n_{k1} en esta columna hasta $k-1$, se calculan nuevas cotas para n_{k1} a partir de la siguiente ecuación:

$$\text{máx}\big((0, (n_{+1} - \sum_{i=1}^{k-1} n_{i1}) - \sum_{i=k+1}^{r} n_{i+}\big) \leq$$

$$n_{ij} \leq \text{mín}(n_{k+}, n_{+j} - \sum_{i=1}^{k-1} n_{i1})$$

   n_{k1} se genera según un entero uniforme;
3. El último elemento de la fila se rellena automáticamente al coincidir las cotas superior e inferior coinciden, haciendo $n_{(k+1)+} = 0$ por conveniencia;
4. Cuando se completa la columna ésta se elimina de la tabla y se recalculan las marginales por fila n_{i+} y el valor n;
5. La tabla tiene ahora una columna menos y se repite el proceso hasta llenar todos los elementos;

Al final lo que obtenemos son una serie de tablas factibles generadas para cada ronda. Por lo que la media de cada elemento sobre todas las tablas para todas las rondas es una estimación de su valor real. La media obtenida por elemento y ronda se agrega sobre todas las rondas la cual representa un estimado de la tabla agregada $\widehat{A}$. Para cada elemento, se estima la probabilidad de cero, calculando el porcentaje de tablas con elemento cero para cada ronda en que el elemento está presente y multiplicando las probabilidades obtenidas para todas esas rondas. En la tabla resultante los elementos se ordenan por

su probabilidad de cero a excepción de los elementos que son cero triviales. De esta manera, los elementos con menor probabilidad de ser cero son los que se consideran candidatos a tener una relación. Para llevar a cabo la clasificación seleccionamos un punto de corte p y consideramos "celdas cero" si probabilidad de cero $> p$, en tanto las "celdas positivas" son aquellas donde la probabilidad de cero$< 1 - p$. Aquellas celdas que no entran en estas dos categorías se les llama "no clasificadas".

El algoritmo utilizado en [24] presupone inicialmente equiprobabilidad de las tablas extraídas. Al desarrollarlo se obtienen, al margen de una primera clasificación de las celdas (*i*, *j*) en 1 ó 0 según exista comunicación o no entre ese par de usuarios, estimaciones para la tasa de mensajes enviados por ronda para cada celda. A partir de estas estimaciones iniciales, puede volver a desarrollarse el algoritmo en un segundo ciclo, en el cual las tablas no se generan con equiprobabilidad. En el primer ciclo del algoritmo el valor de cada celda en cada tabla-ronda era generado según una distribución uniforme manteniendo las restricciones dadas por la información marginal conocida. En este segundo ciclo existen varias posibilidades teniendo en cuenta las primeras estimaciones:

a. Generar el valor de cada celda en cada tabla-ronda según una distribución de Poisson cuyo parámetro lambda es la tasa estimada de mensajes por ronda para esa celda.
b. Generar el valor de cada celda en cada tabla-ronda según la distribución de probabilidad discreta del número de mensajes por ronda en esa celda. Esta distribución es construida a partir de los resultados del primer ciclo del algoritmo, estimando probabilidades de 0, 1, 2, ... mensajes según su porcentaje relativo de ocurrencias.

Este segundo ciclo puede volver a servir de base para ciclos sucesivos en un proceso iterativo. En los resultados siguientes se ha utilizado la opción b). Para llevar a cabo nuestro ataque, primero por cuestiones pedagógicas, simulamos los datos de un sistema de correo electrónico. Para la generación de rondas definimos el número de usuarios participantes *N*, lambda que es el promedio de mensajes enviados por ronda en la celda (*i*, *j*) y el número de rondas *NR* que se desea generar.

1. Con las rondas simuladas se ejecuta el Algoritmo 1 y se obtienen las tablas factibles de cada ronda. Posteriormente se lleva a cabo un test de clasificación binaria para los elementos calculados, donde 0 en la celda (*i*, *j*) significa que no existe relación entre el emisor *i* y el receptor *j*, en tanto 1 significa que sí hay comunicación entre ellos.
2. Generar métricas características para los tests de clasificación binaria (sensibilidad, especificidad, valor predictivo negativo, valor predictivo positivo).
3. Con la información de las tablas factibles para cada ronda se calculan las frecuencias relativas de 0, 1, 2, ... mensajes para cada celda y se obtiene una aproximación a la distribución de probabilidad del número de mensajes por ronda, a partir de la normalización de esas frecuencias relativas.
4. Se vuelve a ejecutar el algoritmo utilizando las probabilidades estimadas para cada celda, normalizadas en cada caso a sus restricciones, en lugar de la distribución uniforme.
5. Se generan métricas de clasificación binaria y se vuelven a estimar las probabilidades.
6. Se itera el proceso a partir del punto 4.

IV. Aplicación del Algoritmo

Llevamos a cabo un gran número de simulaciones luego de generar rondas. El algoritmo no proporciona soluciones uniformes, dado que algunas tablas son más probables que otras debido al orden utilizado al ir llenando filas y columnas. No nos enfocamos en encontrar soluciones para un solo usuario, por lo que: i) Reordenamos aleatoriamente filas y columnas antes de calcular tablas factibles; ii) Conservamos solo las tablas factibles diferentes.

La Tabla I presenta los resultados obtenidos aplicando los algoritmos anteriormente descritos. Los resultados de la iteración 1 corresponden a la aplicación de lo que llamamos primer ciclo [24]; a partir de la iteración 2 se ejecuta el segundo ciclo y de acuerdo a los resultados que obtuvimos pudimos observar que tres iteraciones nos proporcionaban mejores resultados en la mayoría de los casos. Se puede observar también que la complejidad de las rondas crece cuando el número de usuarios y el número de rondas es mayor.

Tabla I
Resultados de la Simulación

No. de usuarios	Iteración	Sensibilidad	Especificidad	VPP	VPN	% de clasificación
10	1	0.9876	0.5789	0.9166	0.9090	0.91
	2	0.9876	0.9473	0.9473	0.9876	0.98
	3	0.9876	0.9473	0.9473	0.9876	0.98
	4	0.9473	0.9876	0.9473	0.9876	0.98
15	1	0.3225	0.9948	0.9090	0.9018	0.90
	2	0.6774	0.9948	0.9545	0.9507	0.95
	3	0.8387	0.9948	0.9629	0.9747	0.97
	4	0.8064	0.9948	0.9615	0.9698	0.96
20	1	0.1818	0.9857	0.6666	0.8846	0.87
	2	0.7272	0.9857	0.8888	0.9583	0.95
	3	0.8181	0.9857	0.9	0.9718	0.96
	4	0.7272	0.9857	0.8888	0.9583	0.95
25	1	0.2297	0.9969	90.9444	0.8507	0.85
	2	0.4324	1	1	0.8858	0.89
	3	0.5540	1	1	0.9080	0.91
	4	0.6486	1	1	0.9261	0.93
30	1	0.1058	0.9981	0.90	0.8764	0.8768
	2	0.2235	0.9981	0.95	0.8909	0.8928
	3	0.3764	0.9981	0.96	0.9104	0.9136
	4	0.3058	0.9981	0.96	0.9013	0.904
35	1	0.0441	0.9986	0.8571	0.8544	0.85
	2	0.2205	0.9986	0.9677	0.8780	0.88
	3	0.2720	0.9986	0.9736	0.8851	0.89
	4	0.2941	0.9986	0.9756	0.8882	0.89

En la Figura 1 se modela la tasa de clasificación respecto a las veces que se ha iterado el algoritmo. Se puede observar una mejora en el porcentaje de clasificación en todos los casos, en relación a la iteración 1.

V. Conclusiones

En las redes de comunicación, los *mixes* ofrecen protección contra observadores al ocultar la apariencia de los mensajes,

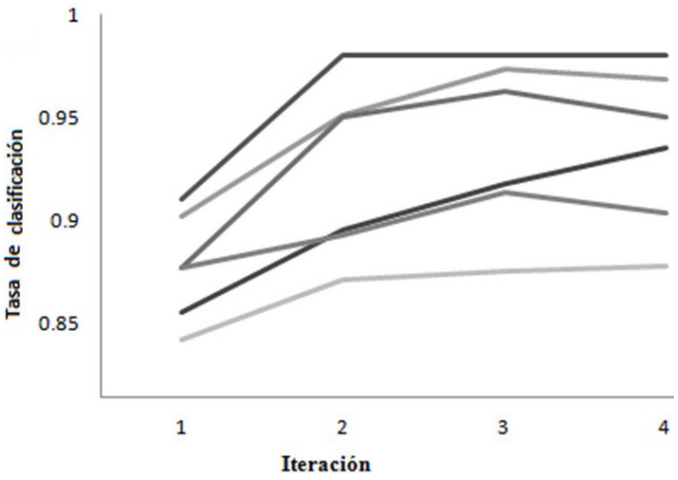

Figura 1. Tasa de clasificación vs. Número de iteración

sus patrones, longitud y enlaces entre emisores y receptores. El objetivo de este trabajo es desarrollar un ataque estadístico global para revelar la identidad de emisores y receptores en una red de comunicaciones que está protegida por técnicas estándar basadas en *mixes*. Para efecto de refinar nuestro ataque tomamos en cuenta las tablas factibles no repetidas, calculamos las frecuencias relativas para cada celda y obtuvimos una aproximación a la distribución de probabilidad del número de mensajes. El método puede ser aplicado en otro tipo de sistemas de comunicación como por ejemplo en redes sociales y protocolos punto a punto; asimismo puede ser implementado fuera del dominio de las comunicaciones como la revelación estadística de tablas públicas y la investigación forense. Nuestro método es afectado por muchos factores como el número de usuarios y el número promedio de mensajes por ronda lo que deriva a una alta complejidad de las tablas que influye de manera negativa en el ataque. El alcance en la tasa de clasificación muestra que entre mayor es el número de rondas se obtienen mejores resultados. Finalmente iteramos el algoritmo. Es necesaria mayor investigación para definir con cuántas iteraciones se pueden ver mejores resultados. De acuerdo a la literatura revisada, podemos concluir que los protocolos de anonimización propuestos hasta ahora consideran escenarios muy específicos. Los ataques estadísticos de intersección se centran en un usuario solamente, sin considerar las relaciones entre todos los usuarios.

Agradecimientos

El Grupo de Investigación GASS agradece la infraestructura proporcionada por el Campus de Excelencia Internacional (CEI) Campus Moncloa Clúster de Cambio Global y Nuevas Energías (y, más concretamente, el sistema EOLO como recurso de computación de alto rendimiento HPC - High Performance Computing), infraestructura financiada por el Ministerio de Educación, Cultura y Deporte (MECD) y por el Ministerio de Economía y Competitividad (MINECO).

Referencias

[1] B. Krishnamurthy. “Privacy and Online Social Networks: can color less green ideas sleep furiosly?” IEEE Security and Privacy, Vol. 11, No. 3, pp. 14–20, May 2013.
[2] A. Westin. “Privacy and Freedom”, Vol. 25, New York: Atheneum: Washington and Lee Law Review, 1968.
[3] R. Gellman y P. Dixon. “Online Privacy: A Reference Handbook”, Santa Barbara, CA.: ABC - CLIO, September, 2011.
[4] R. Gross and A. Acquisti. “Information revelation and privacy in online social networks”, Proceedings of the 2005 ACM workshop on Privacy in the electronic society, Alexandria, VA, USA, pp. 71–80, November 2005.
[5] European Commission. “Press release: Privacy Enhancing Technologies (PETs)”, May 2, 2007.
[6] L. Fritsch. “State or the art of privacy-enhancing technology (PET)”, Norwegian Computing Center Report, Oslo, Norway, 2007.
[7] The META Group, “State of the art of privacy-enhancing technology (PET)”, Danish Ministry of Science, Technology and Innovation, Denmark, March, 2005.
[8] C. Adams. “A Classification for Privacy Techniques”, University of Ottawa Law and Technology Journal, Vol. 3, No. 1, pp. 35–52, 2006.
[9] A. Pfitzmann y M. Hansen. “Anonymity, unlinkability, unobservability, pseudonymity, and identity management: a consolidated proposal for terminology”, TU Dresden, February 2008.
[10] D. Solove. “A Taxonomy of Privacy”, University of Pennsylvania Law Review, Vol. 154, No. 3, January, 2006.
[11] C. Diaz y S. Gurses. “Understanding the landscape of privacy technologies”, Proc. of the Information Security Summit, pp. 58–63, Prague, Czech Republic, May, 2012.
[12] D. Chaum. “Untraceable electronic mail, return addresses, and digital pseudonyms”, Communications ACM, Vol. 24, No. 2, pp. 84–90, February 1981.
[13] M. K. Reiter y A. D. Rubin. “Crowds: anonymity for Web transactions”, ACM Transactions on Information Security and System Security (TISSEC), Vol. 1, No. 1, pp. 66-92, November 1998.
[14] B. Levine y C. Shields. “Hordes: a multicast based protocol for anonymity”, Journal of Computer Security, Vol. 10, No. 3, pp. 213-240, September 2002.
[15] C. Gulcu y G. Tsudik. “Mixing Email BABEL”, in Proceedings of the 1996 Symposium on Network and Distributed System Security, pp. 2-16, San Diego, CA, USA., February 1996.
[16] O. Berthold, H. Federrath y S. Kospel. “Web MIXes: A system for anonymous and unobservable Internet access”, in Proceedings of the International workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, pp. 115-129, Berkeley, CA, USA., July 2000.
[17] D. Goldschlag, M. Reed y P. Syverson. “Hiding Routing Infomation”, in Proceedings of the the First Workshop on Information Hiding, pp. 137-150, London, UK, 1996.
[18] A. Back, I. Goldberg y A. Shostack. “Freedom systems 2.1. security issues and analysis”, Zero Knowledge Systems, May 2001.
[19] R. Dingledine, N. Mathewson y P. Syverson. “Tor: The second-generation onion router”, in Proceedings of the the 13th USENIX Security Syposium, pp. 303-320, San Diego, CA, USA, August 2004.
[20] K. Loesing. “Privacy-enhancing Technologies for Private Services”, University of Bamberg, 2009.
[21] M. Edman y B. Yener. “On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems”, ACM Computing Surveys, Vol. 42, No. 1, pp. 1–35, December 2009.
[22] G. Danezis. “Statistical disclosure attacks: Traffic confirmation in open environments”, in Proceedings of the Security and Privacy in the Age of Uncertainty Conference, (SEC2003), Kluwer, pp. 421–426, May 2003.
[23] J. F. Raymond. “Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems”, in Proceedings of the International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability”, New York, NY, USA, 2001.
[24] J. Portela García-Miguel, D. Rupérez Cañas, A. L. Sandoval Orozco, A. G. Silva Trujillo y L. J. García Villalba. “Ataque de Revelación de Identidades en un Sistema de Correo Electrónico”, Actas de la XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012), Donostia-San Sebastián, España, Septiembre 2012.