Protocolo de acotamiento de distancias basado en canales con ruido

Valeri Korjik
Sección de Comunicaciones
CINVESTAV-IPN
Av. I. P. N. 2508
07000 México, D.F., MEXICO
Fax: (52)-5747-7088,
Tel: (52)-5747-7000 × 3450 vkorjik@mail.cinvestav.mx

Guillermo Morales-Luna
Sección de Computación
CINVESTAV-IPN
Av. I. P. N. 2508
07000 México, D.F., MEXICO
Fax: (52)-5747-7002,
Tel: (52)-5747-7000 × 3355 gmorales@cs.cinvestav.mx

Kirill Morozov
Departamento de Seguridad de Telecomunicaciones
Universidad Estatal de Telecomunicaciones
Moika 65, San Petersburgo, 191186, RUSIA
Fax: (812)-312-1078, Tel: (812)-315-8374
kirill@fem.sut.ru

Resumen

Consideramos un protocolo de acotamiento de distancias que le permite a una parte verificadora estimar una cota superior práctica para la distancia física a una parte corresponsal. El protocolo puede proteger contra llamados "fraudes mafiosos" en los que una parte se identifica ante una parte verificadora utilizando terceras partes. Otro ataque a un protocolo de acotamiento de distancias está dado por la falsificación de la distancia real entre dos partes por medio de un corresponsal deshonesto. Para prevenir ambos tipos de fraudes, el protocolo de acotamiento de distancias ha de poseer una primitiva de compromiso por bits (*Bit Commitment*). En este artículo desarrollamos una idea tendiente a lograr tal primitiva y consecuentemente un protocolo de acotamiento de distancias basado en la realización de canales con ruido conectando varias partes. Para esto, derivaremos fórmulas para estimar la seguridad y la confiabilidad del protocolo de compromiso por bits y presentaremos un algoritmo que optimiza a sus parámetros principales habiendo logrado una complejidad mínima. Mostraremos un ejemplo para ilustrar que nuestro protocolo es, en efecto, confiable y seguro desde el punto de vista de la teoría de la información. Finalmente discutiremos el problema relativo al establecimiento de canales con ruido conectando varias partes.

Abstract

We consider a distance bounding protocol that enables the verifying party to determine a practical upper-bound on the physical distance to a proving party. This protocol can protect against so called "mafia frauds" in which a party identifies himself to a verifying party using the third party being aware of it. Another attack on distance bounding protocol is a falsification of real distance between parties by dishonest prover. To prevent both types of frauds the distance bounding protocol should contain Bit Commitment primitive. In this paper we develop the idea to achieve this primitive and hence a distance bounding protocol based on making noisy channels connecting parties. To solve this problem we derive the formulas to estimate security and reliability of bit commitment protocol and present an algorithm that optimizes the main parameters provided minimal complexity. An example is given to show that this protocol is indeed reliable and information-theoretically secure. We also discuss the problem on how to establish a noisy channel connecting parties.

Palabras claves: Fraudes mafiosos, protocolo de acotamiento de distancias, primitiva de compromiso por bits, canales con ruido, ampliación de privacidad, códigos de corrección de errores.

Introducción

Un *fraude mafioso* es un fraude en tiempo real que puede ser aplicado en cualquier esquema de identificación por un corresponsal frauduento $\overline{P}$ y un verificador $\overline{V}$, cooperantes uno con el otro. Le permite a $\overline{P}$ convencer a un verificador honesto V de una proposición relativa a la información secreta de un corresponsal honesto *P*, sin necesidad de conocer porción alguna de la información secreta de este último. Con tal propósito, cuando P está a punto de iniciar el cumplimiento del protocolo con $\overline{V}$, $\overline{V}$ establece, digamos, un enlace por radio con $\overline{P}$ para enviarle toda información que le transmita *P*, y $\overline{P}$ a su vez ha de enviársela a *V*. La misma estrategia es aplicada por $\overline{P}$, para enviar a $\overline{V}$ toda información que le haya enviado V, para que $\overline{V}$ se la haga llegar a P. En esencia, $\overline{V}$ y $\overline{P}$ actúan como un único ente transparente, asentado en medio de P y V. Todo esto le permite a $\overline{P}$ suplantar ante V la identidad de P, sin que P o V noten el fraude. En la figura 1 mostramos esto esquemáticamente.

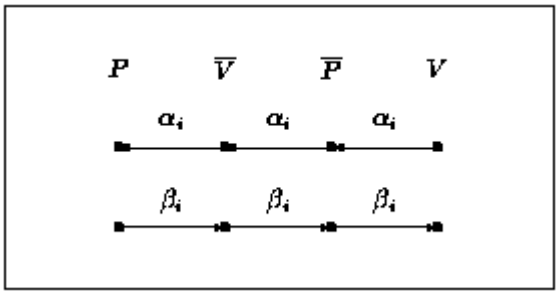


Figura 1: Un fraude mafioso en un esquema de identidad.

No hay métodos prácticos para prevenir fraudes mafiosos salvo por la *técnica de acotamiento de distancias*. La característica principal de este protocolo es la medición de la distancia entre V y su corresponsal P mediante un rápido intercambio de bits a través de un canal que los conecte. Mas, para evitar falsificaciones de la distancia, P ha de enviar cada bit β_i inmediatamente después de recibir un correspondiente bit α_i. Las secuencias de bits $(\alpha_i)_{i\leq l}$ y $(\beta_i)_{i\leq l}$ deben concatenarse, alternando un bit de una con el correspondiente de la otra, y la palabra resultante debe ser firmada por P utilizando una llave secreta propia. Presentamos este protocolo, propuesto en [1], en la figura 2.

A partir de aquí, V puede determinar una cota superior a la distancia a P usando el mayor de los tiempos de retardo entre el envío de cada bit α_i y la recepción del correspondiente bit β_i de vuelta, $i \leq l$. V aceptará este protocolo si y sólo si P está cerca de V y la firma recibida es la correcta de P para el mensaje $m = \alpha_1\beta_1\alpha_2\beta_2\cdots\alpha_l\beta_l$. Es claro que si el esquema de firmado es seguro y P no está cerca de V, entonces un fraude mafioso tiene una probabilidad de éxito de a lo sumo 2^{-l}.

Desafortunadamente existe otro ataque que puede romper este protocolo de acotamiento de distancias y se da en una situación en la que P , quien posee su llave secreta, es deshonesto y procura falsificar su distancia al verificador (véase la figura 3).

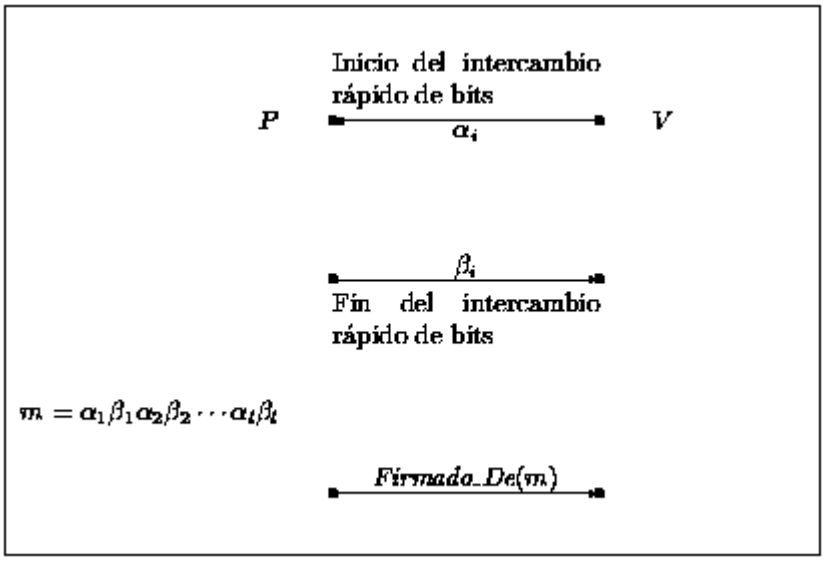
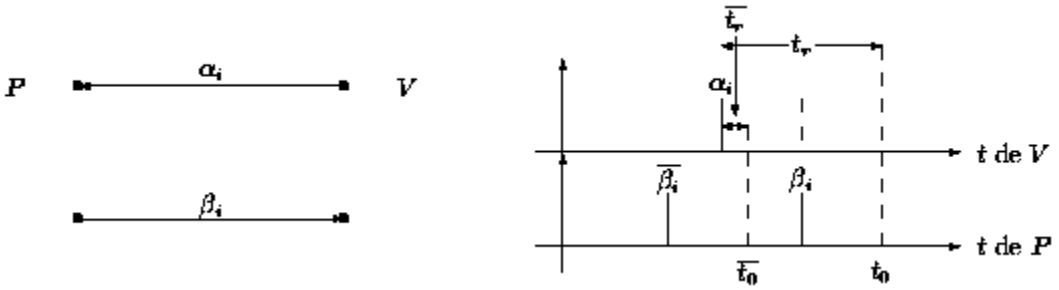


Figura 2: Acotamiento de distancias para prevenir fraudes mafiosos.



Las líneas gruesas marcan envíos de bits. Las punteadas marcan recibimientos de bits. Las variables con sobrelíneas corresponden a valores falsificados. t_r es pues el verdadero retraso en tiempo, en tanto que $\overline{t_r}$ es un falso retraso en tiempo

Figura 3: Un fraude de un corresponsal deshonesto que envía bits demasiado rápido.

Si P conociese los tiempos en los que V le enviará sus bits α_i, entonces puede proceder a enviarle a V sus propios bits $\overline{\beta_i}$ en tiempos "correctos" antes de que arribe α_i, independientemente de su distancia a V. En consecuencia, el protocolo mostrado en la figura 2 está imposibilitado de prevenir este fraude. Para resolver el problema es necesario escoger los bits β_i de manera que dependan de los bits α_i. La manera más sencilla es imponer la condición $\beta_i = \alpha_i$, mas con esta estrategia subsiste la vulnerabilidad al ataque de fraudes mafiosos. Para evitar ambos

tipos de fraudes imponemos la condición $\beta_i = \alpha_i \oplus m_i$, donde la secuencia de bits $m_1, m_2, \ldots, m_l$ es generada por P y V queda comprometido por ella, utilizando un *esquema de compromiso* (*commitment scheme*}) seguro. Tal protocolo, propuesto en [1], queda esquematizado en la figura 4.

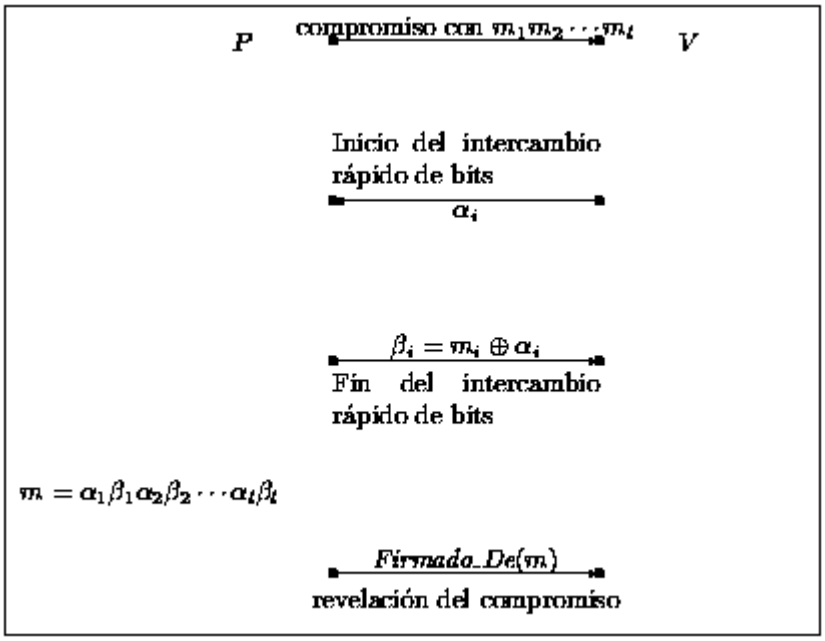


Figura 4: Protocolo para prevenir ambos tipos de fraudes.

Con la información recibida en el cuarto paso de esa figura, V verifica si acaso los bits $\tilde{m}_i = \alpha_i \oplus \beta_i$ coinciden con los bits m_i comprometidos por P. Si así fuera, entonces V calcula m de igual forma a como lo hace P y verifica si la firma recibida corresponde, en efecto, a la de P para el mensaje m. En caso afirmativo, V calcula una cota superior de su distancia a P mediante el máximo de los tiempos de retraso y, finalmente, V habrá de aceptar si y sólo si P está cerca de V.

Así pues, un protocolo de compromiso por bits es una componente sumamente importante del protocolo de acotamiento de distancias que previene ambos fraudes, el de tipo "mafioso" y el de un corresponsal deshonesto. En la sección siguiente consideraremos el caso especial de este protocolo basado en canales con ruido.

Protocolo de compromiso por bits basado en canales con ruido

En el caso del protocolo de compromiso por bits, un corresponsal (Alberto) desea comprometerse con una predicción $m = m_1 m_2 \cdots m_l$ pero no quiere revelar esa predicción a un miembro de la mafia (Marco) sino hasta algún momento posterior. El verificador (Benito), por su lado, desea asegurar que Alberto no cambie de parecer después de que él se haya comprometido con su predicción (pues si se le permitiera hacerlo, en el caso de que Alberto fuese deshonesto, él podría romper el protocolo de acotamiento de distancias).

El protocolo puede instrumentarse mediante el sencillo algoritmo siguiente:

1. Benito genera una cadena aleatoria de bits R y se la envía a Alberto.
2. Alberto calcula el texto cifrado $c = E_L(R,m)$ y se lo envía a Benito. Aquí L es una llave aleatoria y la pareja (R,m) denota a la concatenación de R con m.

Ni Benito ni Marco pueden desencriptar el mensaje (R,m), así que ambos ignoran cuál es la cadena m.

Ahora bien, si Alberto decide revelar su compromiso, puede realizar el protocolo siguiente:

1. Alberto envía la llave L a Benito.
2. Benito desencripta el mensaje y recupera (R,m). Habiendo recuperado m, al comprobar que aparezca su cadena aleatoria R está verificando también la validez de la cadena m.

Es obvio que para mantener la seguridad de este protocolo es necesario imponer condiciones de cómputo limitado a Marco y a Alberto. De hecho es imposible presuponer lo contrario. Supongamos pues que Alberto y Benito se conectan mediante un *canal simétrico binario*, BSC_p, (por sus siglas en inglés, *Binary Symmetric Channel*). Es decir, por un canal que cambia el valor de cada bit con una probabilidad P durante su transmisión de una parte a la otra. Seguiremos el protocolo propuesto en [2].

Alberto y Benito convienen en utilizar un código binario lineal (n,k), C, con distancia minimal de código, d. Supondremos que existe un BSC_p, mediante el cual Alberto envía mensajes a Benito, y además que existen canales sin ruido con los que ellos intercambian mensajes. En consecuencia, hemos de suponer que existe un $BSC_{p'}$ entre Alberto y Marco, también.

Tras de una fase de inicialización, Alberto y Benito realizan el siguiente *protocolo 1*:

1. Alberto elige una palabra aleatoria $c \in C$, en el código C, y una cadena aleatoria de n bits, b. Con ello, Alberto calcula una cadena x de l bits tal que
$$m = x \oplus h_b(c) \tag{1}$$
donde $h_b : C \to \{0,1\}$ es una función de dispersión (*hash*) elegida en la clase $Universal_2$ de [3] y determinada por la cadena b. A cada palabra de código c la transforma en una cadena de l bits, donde l es la longitud de la cadena m con la que se ha de establecer el compromiso.
2. Alberto envía c a través del BSC_p y le transmite a Benito, por medio de los canales sin ruido, las palabras b y x.
3. Benito conserva c', b y x, donde c' es la versión recibida de c, acaso corrupta por el canal ruidoso.

Si Alberto quisiese revelar su compromiso m, inicia entonces el siguiente *protocolo 2*:

1. Alberto envía c a Benito, por medio de un canal sin ruido.
2. Benito revela la palabra comprometida m, calculada mediante la expresión (1), pues él conoce x, b y c. Calcula la distancia de Hamming $d_H(c,c')$ entre c y c', y si acaso $d_H(c,c') \le l_0$, donde l_0 es un cierto umbral, entonces Benito acepta m. En otro caso la rechaza.

La evaluación del desempeño de este protocolo puede realizarse calculando los valores siguientes:

i. La probabilidad P_c de una *decodificación óptima correcta* de *m* por Marco, basada en su conocimiento de *C*, *c*'', *b*, *x* y la función de dispersión h_b, donde *c*'' es la versión que él recibió de *c*, corrupta por el canal $BSC_{p'}$ entre Alberto y Marco. La probabilidad P_c puede ser acotada superiormente mediante la desigualdad de Fano

$$l + (1 - P_c)\log_2 \frac{1 - P_c}{2^l - 1} + P_c \log_2 P_c \le I_0 \tag{2}$$

donde I_0 es la cantidad de información de Shannon que la falta a Benito (y a Marco) sobre *m* dados *c*'', *b*, *x* y la función de dispersión h_b. El valor I_0 puede a su vez ser acotado mediante el Teorema de Ampliación de la Privacidad [4]:

$$I_0 \le 2^{-(n-r-t-l)} \tag{3}$$

y aquí

- $r = n - k$ es el número de símbolos a revisar en el código *C*, y
- $t = n\left(1 + \log_2\left(p'^2 + (1-p')^2\right)\right)$ es la información de Renyi [4] que Marco gana con *c*'', recibido a través del $BSC_{p'}$.

ii. La probabilidad P_{FR} de que ocurra $d_H(c, c') > l_0$. En esta situación, la palabra comprometida *m* es *falsamente rechazada* por Benito, a pesar de que Alberto ha sido honesto en su ejecución del protocolo. Se puede ver fácilmente que P_{FR} puede acotarse como sigue:

$$P_{FR} \le \sum_{i=l_0+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{4}$$

iii. La probabilidad P_{FD} de que se elija $\tilde{c} \in C$, $\tilde{c} \ne c$ tal que $d_H(\tilde{c}, c') \le l_0$. Eligiendo una tal $\tilde{c}$, Alberto puede tener éxito en un intento por cambiar su compromiso y consecuentemente en *falsificar su distancia* a Benito. Suponiendo que un Alberto deshonesto envía una cadena *w* tal que la palabra más cercana $c \in C$ en el código *C* ocurre a una distancia de Hamming *s* a *w*, y tomando en cuenta que para cualquier otra palabra en el código $\tilde{c} \ne c$ se debe cumplir $d_H(w, \tilde{c}) \ge d - s$, como una consecuencia de la propiedad de la distancia de Hamming podemos estimar la probabilidad de que anuncios de cualquier otra palabra $\tilde{c}$ en el código que haya sido enviada por Alberto sea también aceptada por Benito:

$$P_s(\tilde{c}) \le \sum_{i=0}^{d-s} \binom{d-s}{i} (1-p)^i p^{d-s-i} \sum_{j=0}^{l_0-i} \binom{n-d+s}{j} p^j (1-p)^{n-d+s-j} \tag{5}$$

Por tanto, la probabilidad P_{FD} de que se cambie el compromiso de Alberto, y en consecuencia se falsifique su distancia a Benito, queda acotada superiormente como sigue

$$P_{FD} \le \max\left\{\frac{1}{2^l}, \max_{1 \le s \le d/2} P_s(\tilde{c})\right\} \tag{6}$$

El problema sobre cómo seleccionar los parámetros principales del protocolo de compromiso por bits utilizado como parte del protocolo de acotamiento de distancias puede ser resuelto por el algoritmo siguiente:

1. Fíjese los valores de P_{FR}, P_c, P_{FD}, n, p y p'.

2. Tómese $l = -\log_2 P_c + 1$.
3. Encuéntrese un umbral l_0 de la ecuación (4), dados P_{FR}, p y n.
4. Fíjese I_0 que cumpla con la relación (2), dados l y P_c.
5. Calcúlese el mínimo valor posible $k = n - r$, donde r ha de cumplir con la condición (3).
6. Encuéntrese la mínima distancia de Hamming d del código (n,k)-lineal utilizando la cota para códigos BCH, [5].
7. Calcúlese P_{FD}' utilizando (6) y revísese si acaso $P_{FD}' \leq P_{FD}$. Si **sí** actualícese $P_{FD} := P_{FD}'$, decreméntese n y repítase el algoritmo con el fin de obtener un protocolo de compromiso por bits más eficiente. En otro caso, encuéntrese $l > -\log_2 P_c + 1$ que minimice P_{FD}' mediante una repetición de este algoritmo del paso 3. al 7. Si el mínimo P_{FD}' calculado así excediese a P_{FD}, entonces increméntese n y repítase el algoritmo.

Ejemplo: Consideremos $P_c = 10^{-6}$, $P_{FR} = 10^{-4}$, $P_{FD} = 4.5 \times 10^{-5}$, n = 16383 y p = 0.18. Entonces al hacer las evaluaciones de acuerdo con el algoritmo descrito obtendremos l = 20, $l_0 = 3133$, $I_0 = 1.6 \times 10^{-9}$, t = 8114, k = 8164 y d = 1175. Esto significa que ambos Marco y Alberto, en un papel deshonesto, prácticamente no tienen posibilidad alguna de falsificar su distancia a Benito. ∝

Discusión de los resultados principales y de un problema abierto

La aplicación del protocolo de compromiso por bits al problema de acotamiento de distancias proporciona un ejemplo un tanto extraño en el que una predicción m ha de ser protegida para no ser revelada ante un agente mafioso (no un verificador) y para que no sea cambiada por un corresponsal deshonesto (Alberto).

Aquí, un problema muy importante es el arreglo de un canal ruidoso. Este puede ser avalado como seguro por una tercera parte confiable, que garantice sus propiedades. En tal caso, sin embargo, sería inútil considerar el protocolo descrito porque el problema de compromiso por bits podría ser resuelto por esa misma parte confiable.

Afortunadamente, en nuestro escenario el verificador (Benito) es completamente honesto y no habría él de atacar este protocolo de manera alguna. Así pues, él puede montar un canal ruidoso basado, por ejemplo, en un generador de ruido espacial y seleccionar su parámetro P de manera que se obtenga el protocolo más eficiente.

Un problema abierto queda planteado por la manera en la que se ha de usar un canal cuántico para que sea equivalente a un BSC_p, entre Alberto y Benito, y un $BSC_{p'}$ entre Alberto y Marco, con valores garantizados para p y p'.

Referencias

1. S. Brands, D. Chaum, Distance-bounding protocols, *Proc. Eurocrypt '93*, Lecture Notes in Computer Science, nr. 765, 1993, pp. 344-359.

2. C. Crepeau, Efficient cryptographic protocols based on noisy channels*, Proc. Eurocrypt '97*, Lecture Notes in Computer Science, nr. 1233, 1997, pp. 306-317.
3. D. R. Stinson, Universal hashing and authentication codes, Advances in Cryptology, *Proc. Crypto '91*, Lecture Notes in Computer Science, nr. 576, 1992, pp. 74-85.
4. C. Bennet, G. Brassard, C. Crepeau, U. Maurer, Generalized privacy amplificaction, *IEEE Trans. on IT*, vol. 41, nr. 6, 1995, pp. 1915-1923.
5. F. G. Mac Williams and N: J. A: Sloan, *The theory of error-correcting codes*, New York, North-Holland,1976.