Resolución de escenarios en control de acceso a grupo en entornos distribuidos*

Joan Arnedo-Moreno
Estudis d'Informàtica, Multimèdia i Telecomunicació
Universitat Oberta de Catalunya
jarnedo@uoc.edu

Jordi Herrera-Joancomartí
Estudis d'Informàtica, Multimèdia i Telecomunicació
Universitat Oberta de Catalunya
jherreraj@uoc.edu

Resumen

La aparición de entornos totalmente distribuidos, tales como las redes peer-to-peer, ha permitido la creación de infraestructuras de servicios sin la necesidad de un proveedor centralizado. Si bien en su inicio estos entornos se concibieron como totalmente abiertos, existen motivos (seguridad, control de ámbito, etc.) por los cuales puede ser deseable crear grupos diferenciados. Para lograrlo, es necesario aplicar controles de acceso, existiendo diferentes escenarios diferenciados según el grado de implicación de los distintos componentes involucrados. En este artículo se presenta como adaptar distintos mecanismos de control de acceso a grupos de manera que puedan amoldarse al máximo de dichos escenarios.

1. Introducción

Las aplicaciones peer-to-peer se conceptualitzaron inicialmente como un entorno totalmente abierto sobre una red superpuesta, con el objetivo de englobar el máximo número de pares posible. Esto se debe al hecho de que las aplicaciones más populares han sido básicamente, y aún siguen siendo, las de intercambio de ficheros, tales como en su momento Napster o actualmente BitTorrent [1, 8]. En ellas, el par es capaz de acceder a cualquier recurso por el mero hecho de formar parte de la propia red.

Sin embargo, existen entornos en los que puede ser deseable segregar la red en distintas comunidades o grupos diferenciados, si bien no necesariamente disjuntos, de manera que el acceso a los recursos disponibles quede restringido a los componentes del grupo. Un ejemplo de este tipo de entornos es una organización con distintos departamentos o grupos operativos: cualquier segmentación dada por interses diferenciados. Este concepto fue introducido en JXTA [15] como *grupo de pares*, o *peer-group*, siendo, de hecho, uno de los pilares fundamentales de esta arquitectura.

Para lograrlo, es necesario implantar mecanismos de control de acceso que permitan dicha segregación. De este modo, se pasa de un entorno llano, donde cualquier componente de la red puede acceder a todos los recursos, a otro segmentado en grupos donde el acceso a los servicios o recursos está supeditado a la pertenencia a cada grupo. Sin embargo, es importante que los mecanismos que lo permitan sigan la misma filosofía original del entorno *peer-to-peer*: basarse en un sistema no centralizado, sin ningún proveedor externo. El propio grupo debería ser capaz de auto-gestionarse a través de los recursos agregados por sus componentes. En caso de no aplicar este principio, se pierde la esencia de un entorno totalmente distribuido.

Bajo esta premisa, es posible clasificar el acceso al grupo en diferentes escenarios generales. En [3] se propone una clasificación según

*Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia y Tecnología con el proyecto SEG2004-04352-C04-04 PROPRIETAS-WIRELESS.

el grado de implicación de los componentes del grupo en el proceso de ingreso de un nuevo miembro y los pasos necesarios para identificar a un par como miembro del grupo. A partir del estudio de dicha clasificación, es posible analizar cada escenario según el grado de relevancia de los pares dentro del grupo.

De cara a implantar mecanismos de seguridad en este tipo de entornos, en [17] se puede hallar la lista de requisitos mínimos exigibles en una red *peer-to-peer*. Para el control de acceso en este tipo de entornos existen diferentes aproximaciones, resumidas en [11] y [5]. Si bien dichos artículos se centran en redes *adhoc* en general, el paralelismo entre el acceso a grupos y a una red *adhoc* es directo.

Sin embargo, ninguno de los mecanismos existentes es capaz de resolver directamente todos los escenarios definidos en [3], a menos que se apliquen políticas arbitrarias sobre los componentes del grupo. La mayoría de mecanismos están muy restringidos a escenarios específicos. Un reto interesante es ver qué modificaciones es posible aplicar a los mecanismos existentes de cara a que estos puedan solventar el máximo de escenarios.

En el presente artículo se propone qué elementos deben incorporar algunos los de mecanismos actuales de control de acceso a grupo en entornos *peeer-to-peer* o *adhoc* de modo que sean capaces de resolver el máximo de los escenarios definidos en [3]. Se hace especial énfasis en aquellos escenarios que actualmente no se encuentran directamente resueltos.

Por una parte, se presentan los mecanismos de acceso a grupos basados en Autoridad de Certificación (AC). Dichos sistemas disponen de amplia popularidad, existiendo diversas propuestas [18, 16]. Por otra parte, se propone una resolución para un sistema autoorganizado. En concreto, el basado en red de confianza expuesto en [4].

En las propuestas se tiene especialmente en cuenta el hecho que no es posible limitar la capacidad de un componente del grupo únicamente mediante políticas. Para que un componente no pueda realizar una acción no deberá tener acceso a la información o a los mecanismos necesarios para realizarla.

El artículo se divide de la siguiente manera. En la sección 2 se hace un breve resumen de los escenarios a resolver. A continuación, se exponen la propuestas para resolver dichos escenarios. Concretamente, en la sección 3 se describe la solución mediante AC distribuida, y en la sección 4 mediante el sistema basado en red de confianza. En ambos casos, previamente se da una pequeña explicación de en qué consiste cada mecanismo. Finalmente, la sección 5 expone las conclusiones.

2. Escenarios de control de acceso

En [3], el proceso de control de acceso se subdivide en dos pasos claramente diferenciados:

Registro: Proceso mediante el cual un nuevo miembro pide ser aceptado en el grupo. En este paso, se generan las credenciales necesarias para que el miembro potencial pueda demostrar posteriormente su pertenencia al grupo. Se asume que el registro tan solo se realiza una única vez. El proceso de registro puede requerir una invitación previa por parte de alguno de los miembros actuales, o, como mínimo, conocimiento de la existencia del grupo.

Autenticación: Proceso mediante el cual un miembro se conecta al grupo, probando que forma parte de éste mediante las credenciales generadas en el registro. Identificamos como conexión al grupo la posibilidad de acceso a sus servicios o recursos.

Teniendo en cuenta estos dos procesos, se pueden definir distintos escenarios de control de acceso basados en el nivel de implicación de los miembros del grupo. La definición de dichos escenarios se realiza sobre dos ejes primordiales: el número de miembros que debe colaborar para llevar a cabo cada paso y la existencia de restricciones respecto a qué miembros pueden llevarlo a cabo.

En el primer eje se concretan dos casos: los de *par único* y los *colaborativos*. Mientras que en el primer caso se asume que un único miembro es suficiente de cara a completar el proceso, en el otro, se requiere la colaboración de

distintos miembros para poder llevar a cabo satisfactoriamente el proceso.

Para el segundo eje, se tiene en cuenta la existencia, así como el tamaño, de dos subconjuntos dentro del grupo G, los cuales son los únicos capacitados para llevar a cabo los procesos de registro y autenticación, denominados Γ^R y Γ^A, respectivamente.

Ambos ejes de la clasificación tienen fuertes implicaciones al analizar aspectos clave tales como la disponibilidad, el grado de igualdad entre pares o la resistencia a confabulaciones.

2.1. Escenarios de registro

Escenario 1R: Al resultar que $\Gamma^R = \emptyset$, este escenario contempla dos interpretaciones: o bien no se requiere registro y cualquier par se considera automáticamente miembro del grupo, o bien se está considerando un grupo cerrado donde no se aceptan nuevo integrantes.

Bajo la primera interpretación, el concepto de grupo como conjunto de pares segregados dentro de la red deja de tener sentido. Sin embargo, la opción de un grupo por defecto es útil en algunos entornos, como es el caso del NetPeerGroup en JXTA [15].

Escenario 2Rs: En este escenario, solo un subconjunto de miembros del grupo (Γ^R) puede registrar nuevos integrantes, pero individualmente.

Escenario 3Rs: Este escenario mantiene la igualdad entre pares permitiendo a cada integrante de G la opción de registrar nuevos integrantes sin restricción alguna.

Escenarios colaborativos. 2Rc y 3Rc: En ambos casos, existe un número mínimo de miembros que debe colaborar antes de poder registrar un nuevo integrante. La diferencia primordial entre 2Rc y 3Rc se encuentra en la existencia del subconjunto Γ^R.

2.2. Escenarios de autenticación

Escenario 1A: En este escenario no existe ningún proceso de autenticación. Nuevamente, esto implica dos posibles interpretaciones: se asume que cualquier par es aceptado por defecto como parte del grupo, situación que vuelve a eliminar el concepto propio de grupo segregado, o bien estamos en una situación el la cual no se aceptan más conexiones al grupo.

Escenario 2As: Cualquier integrante puede autenticar por si mismo al miembro que accede, proporcionando la mayor flexibilidad y disponibilidad.

Escenario 3As: Solo aquellos integrantes con la capacidad de registrar, los pertenecientes a Γ^R, pueden autenticar. Normalmente, este escenario se apoyará en un escenario de registro 2Rs o 2Rc.

Escenario 4As: Este escenario contempla que solo los integrantes que formaron parte del proceso de registro tienen la capacidad de autenticar miembros. Esta opción tiene sentido, ya que es lógico pensar que aquellos integrantes que generaron la credencial del nuevo miembro dispondrán de un mayor grado de información fiable de cara a autenticarlo.

Escenarios colaborativos. 2Ac, 3Ac, 4Ac: Son escenarios equivalentes a los 2As, 3Ac y 4Ac, pero cierto número de integrantes deben colaborar de cara a autenticar al miembro que se quiere autenticar.

También se contempla la posibilidad de combinar los distintos escenarios de modo que miembros a distintos niveles de la jerarquía de subconjuntos deban colaborar para autenticar a B. Dichos escenarios son denominados *escenarios combinados* (*mixed scenarios*). Sin embargo, no se analizarán en este artículo.

Finalmente, vale la pena remarcar que no todos los escenarios de autenticación se pueden combinar con los de registro, puesto que no siempre tiene sentido. Siempre existe una dependencia. Por ejemplo, no tiene sentido tener un escenario de autenticación 4Ac cuando se está usando un escenario de registro basado en un único par (2Rs, 3Rs).

3. Sistemas basados en AC

Un sistema ampliamente aceptado para el control de acceso a grupo es el uso de una AC. Ésta se encarga de generar certificados digitales para los miembros del grupo, de modo que posteriormente sean usados como credenciales en el proceso de autenticación [7].

Inicialmente, una AC se considera una entidad totalmente centralizada con una ubicación específica. Sin embargo, dicha aproximación no se ajusta a un entorno como *peer-to-peer*, al no poder darse la garantía que un par específico siempre estará conectado.

Una solución a este problema pasa por el uso de una AC distribuida mediante un criptografía umbral [19, 14]. Un subconjunto de pares dentro del grupo cooperan para proporcionar las funcionalidades de una AC completa. La clave privada de la AC es fragmentada y repartida entre n de estos pares, de modo que es necesaria al colaboración de t de ellos para firmar el certificado del nuevo miembro.

3.1. Escenarios de registro

Tanto la aproximación de AC centralizada como su extensión al sistema umbral permiten la resolución de los distintos escenarios de registro descritos en la Sección 2.

Si bien los sistemas umbral son especialmente indicados para resolver los escenarios colaborativos (como veremos más adelante), estrictamente también pueden resolver los escenarios individuales (2Rs, 3Rs), aplicando $t = 1$. En términos generales, para estos escenarios el sistema es equivalente a una AC replicada, ya sea entre un número limitado de integrantes del grupo (escenario 2Rs) o entre todos ellos (escenario 3Rs).

Sin embargo, es importante destacar que el comportamiento de un sistema de AC umbral para la resolución de los escenarios individuales, tal y como lo acabamos de describir, es básicamente el mismo que un sistema mediante clave simétrica compartida. Esto tiene distintas implicaciones, la mayor de las cuales se produce cuando uno de los miembros capaces de registrar abandona Γ^R. En este caso, será necesario cambiar la clave privada de la AC, lo cual técnicamente es equivalente a rehacer el grupo, puesto que todos los certificados emitidos hasta el momento dejarán de tener validez. En el caso 3Rs las implicaciones son todavía peores, dado que $\Gamma^R = G$ y por tanto esta situación sucede con cualquier baja del grupo.

Por estos motivos, el uso de una AC para resolver estos dos escenarios no es muy recomendable salvo en casos muy específicos (principalmente, grupos donde nunca hay bajas en Γ^R o G).

Por lo que respecta a los escenarios de registro colaborativos, los sistemas basados en AC umbral se presentan como una buena solución. El escenario 2Rc (donde el registro se lleva a cabo de forma conjunta por más de un par que pueda registrar) se resuelve directamente, ya que se reconoce la existencia del subconjunto Γ^R, que corresponde a los pares que disponen de una parte de la clave privada de la AC.

Por otro lado, el escenario 3Rc (donde todos los pares del grupo pueden registrar y se precisa más de uno de ellos para el registro) también es de resoluble si se generaliza el esquema umbral de modo que que $|\Gamma^R| = n = |G|$. Es decir, todos los integrantes del grupo forman parte del esquema umbral.

Por último, es importante destacar que, aunque el hecho de que todos los integrantes del grupo puedan registrar nuevos pares es técnicamente posible, se debe tener presente que en grupos grandes este sistema tiene problemas de escalabilidad [10]. Uno de los mayores problemas de los sistemas basados en AC umbral es que las claves de la AC deben ser renovadas y redistribuidas cada vez que cambia el parámetro n. Esto sucede cada vez que hay un cambio en Γ^R (o para el caso 3Rc, cada vez que cambian los miembros de G). Por ello, los entornos donde dicho subconjunto es relativamente dinámico esta renovación de las claves de la AC genera una gran sobrecarga.

3.2. Escenarios de autenticación

La resolución de los escenarios de autenticación descritos en la Sección 2 mediante esquemas de AC (centralizada o umbral) no es tan directa como en los escenarios de registro. Aplicando dichos sistemas de forma directa,

tan solo resuelven el escenario 2As, puesto que el certificado de la AC del grupo se distribuye entre todos sus miembros de G y por tanto el certificado generado puede ser validado por cualquiera de ellos de forma individual.

Las posibilidades de resolución del resto de escenarios de autenticación se discuten a continuación.

Para la resolución del escenario 3As, se puede limitar el acceso al certificado de la AC únicamente a los miembros de Γ^R. De este modo, solo ellos dispondrán de toda la información necesaria para autenticar a otros pares. En esta solución, el subconjunto Γ^R no permite bajas arbitrarias, puesto que una vez un miembro dispone del certificado de la AC, la única manera de anular su uso de cara a la autenticación sería cambiar la clave privada de la AC.

El uso de una AC tampoco permite resolver directamente los distintos casos colaborativos. Para permitir su resolución es necesario añadir funcionalidades al esquema base. Una primera posibilidad es usar un esquema de autenticación basado en sistemas bizantinos [13], de manera que varios pares deban llegar a un acuerdo sobre la pertenencia de un miembro o no al grupo. Una propuesta en este sentido la podemos encontrar en COCA [18]. Sin embargo, el uso de sistemas bizantinos solo contribuye al aspecto colaborativo del escenario desde una perspectiva de tolerancia a fallos. La colaboración entre miembros no está realmente forzada para restringir que un único miembro no pueda resolver el proceso.

Para resolver los escenarios colaborativos desde una perspectiva mecánica, y no de tolerancia a fallos, es necesario obligar a los miembros a colaborar, del mismo modo que sucede en el registro para los escenarios 2Rc o 3Rc. Para ello, es necesario extender el esquema umbral a la clave pública de la AC, y con ello al proceso de autenticación.

Los escenarios más problemáticos en un mecanismo basado en AC son aquellos donde únicamente los participantes en el proceso de registro (Γ_B^R) están autorizados a autenticar un integrante del grupo (escenarios 4As y 4Ac). Dado que la información guardada por el subconjunto Γ^R es común a todos sus componentes y no existe ningún elemento único para cada uno (salvo la parte de la clave privada), no es posible conseguir esta limitación. En consecuencia, este escenario no es resoluble mediante una AC umbral.

Como se ha podido observar, los esquemas basados en AC están muy focalizados a los escenarios colaborativos, en el caso del registro, y los de par único en el caso de la autenticación. A pesar de ello, es posible modificar algunos aspectos de su comportamiento para poder resolver de manera satisfactoria el resto de escenarios. Sin embargo, es importante tener presente que al hacerlo aparecen fuertes restricciones en el proceso de baja de un miembro de Γ^R, por lo que la utilización de este tipo de soluciones no siempre puede ser factible.

4. Sistemas basados en red de confianza

En los mecanismos basados en red de confianza, cada miembro del grupo dispone de su propia clave privada, diferente de la del resto de miembros, y posee la capacidad de generar relaciones de confianza hacia otros integrantes. Para crear una nueva relación de confianza, un par firma con su clave privada la clave pública del par en el cual confía (en cierto modo, cada par actúa como una AC autónoma). Un nuevo miembro es aceptado en el grupo a partir de la generación de dichas relaciones. Esta aproximación es la que define el modelo PGP [9].

Los mecanismos basados en red de confianza representan una aproximación interesante al permitir una mayor autonomía de cada par. Este hecho encaja perfectamente con la naturaleza de *peer-to-peer*.

Una propuesta inicial basada en este modelo y aplicada sobre redes *adhoc* se puede hallar en [6, 12]. En ella se expone un mecanismo para autenticar pares sobre una red de confianza pre-existente. Sin embargo, si bien sienta las bases para una alternativa al uso de una AC distribuida, dicha propuesta está más ligada a la autenticación de la identidad del par que al control de pertenencia a grupo.

Un mecanismo mucho más específico a este

entorno se expone en [4], donde se traducen la propias relaciones de confianza a la prueba de pertenencia al grupo. En ella se explicita el subconjunto Γ^R de miembros que pueden crear relaciones de confianza, pero no existen restricciones específicas sobre qué pares pueden formar parte de él, siendo muy dinámico.

Existen dos tipos distintos de relaciones de confianza, según entre qué pares se crea. La relaciones de *patrón* son unidireccionales y se establecen entre los miembros de Γ^R y el resto de miembros. Las relaciones de *backbone*, en cambio, son bidireccionales y se establecen únicamente entre miembros de Γ^R. Mediante la combinación de ambos tipos es posible garantizar que existen caminos de confianza entre todos los miembros del grupo.

4.1. Escenarios de registro

Los mecanismos de red de confianza están enfocados a maximizar la autonomía de los pares. Es por este motivo que su aplicabilidad es más directa en los escenarios de registro de par único (2Rs y 3Rs).

Así pues, en [4] se resuelve directamente el escenario 2Rs, puesto que en dicha propuesta ya se contempla un subconjunto Γ^R de forma explícita. Adicionalmente, la resolución del escenario 3Rs también es posible con esta misma aproximación se vuelve a ampliar al caso general $\Gamma^R = G$ (en este caso, solo existirían relaciones de *backbone*). En este sentido, conceptualmente se trata del mismo caso que en el escenario colaborativo mediante una AC umbral. Partiendo del caso específico, se amplia a todo el grupo.

En lo que respecta a los escenarios colaborativos, la propuesta ya contempla la resolución de dichos escenarios. Para ello, se considera necesario que t miembros confíen en el nuevo par que ha de formar parte del grupo (generando las correspondientes relaciones de confianza) para completar con éxito el proceso de registro. La resolución de ambos escenarios mediante este sistema añade, a su vez, la posibilidad de resolver el proceso de manera totalmente asíncrona, un aspecto muy necesario en un sistema *peer-to-peer*. La diferencia a entre la resolución de los casos 2Rc y 3Rc, nuevamente, recae únicamente en el ámbito de Γ^R ($\Gamma^R \subset G$ o $\Gamma^R = G$), al igual que en los casos de par único.

4.2. Escenarios de autenticación

En los escenarios de autenticación se puede ver claramente la fuerte contraposición entre los mecanismos basados en AC y los basados en red de confianza. En estos últimos, al ser cada par totalmente autónomo y no guardar información alguna respecto al resto de miembros del grupo, será imprescindible su colaboración con otros miembros del grupo para conseguir información más allá de la relativa a él mismo o su patrón. Este hecho representa que es necesario modificar el mecanismo de red de confianza para poder solventar los escenarios de par único, de modo que se redistribuya la información relativa a todos los miembros del grupo en cada par.

En el caso más general, el escenario 2As, se debe considerar la posibilidad de que cualquier miembro pueda autenticar a cualquier otro. Para este caso, se puede usar la propuesta ya mencionada de Hubaux et al [6] para distribuir de manera uniforme las claves públicas firmadas de todos los integrantes del grupo, de modo que únicamente mediante el intercambio de la información de dos pares (la parte autenticada y la parte autenticadora) ya es suficiente para poder buscar un camino de confianza.

En el escenario 3As, dado que se trata de un caso más restrictivo, únicamente es necesario que los miembros de Γ^R posean toda la información necesaria para poder deducir un camino de confianza hasta la parte a autenticar. Para ello, es necesario que todos mantengan un repositorio con el mínimo necesario de relaciones de confianza backbone de modo que desde su ubicación puedan llegar a cualquier otro integrante de Γ^R (por ejemplo, mediante el algoritmo de Dijkstra). Esta opción es equivalente al mecanismo de resolución de enrutado mediante OSPF [2].

La resolución propuesta para los escenarios 2As y 3As puede ser o no factible según el número de miembros de Γ^R.

Curiosamente, el caso 4As, al ser el más restrictivo de todos, puede ser resuelto de manera trivial sin impactar en la autonomía de los pares. Esto es debido a que Γ_B^R es equivalente al conjunto de pares que generaron una relación de confianza a partir de la cual el integrante se unió al grupo (en el caso de relaciones patrón, los patrones del par). Por ello, a cualquiera de ellos le resulta fácil autenticar por si mismo a los integrantes del grupo con los que formó una relación patrón, puesto que él mismo generó la firma. Sin embargo, para limitar únicamente a Γ_B^R la capacidad de autenticación, es necesario que cada par mantenga en secreto su propia clave pública, de manera que solo él pueda validar sus propias firmas.

Respecto a los casos colaborativos, el escenario 2Ac es el que resuelve directamente tal y como se plantea el mecanismo, sin necesidad de modificación alguna.

El caso 3Ac es resoluble si los patrones se niegan a colaborar con aquellos pares que no forman parte de Γ^R (aquellos con los que no comparte relaciones backbone, sino únicamente de patrón). Dado que un miembro del grupo que no pertenece a Γ^R necesita de su patrón para poder iniciar la búsqueda del camino de confianza, si este se niega a colaborar, será incapaz de recuperar el camino de confianza hacia el miembro a autenticar.

Para el caso colaborativo más restrictivo, 4Ac, es importante remarcar que no tiene sentido si no está asociado a un escenario de registro también colaborativo (ya que por definición del escenario, ha de ser cierto que $|\Gamma_B^R| > 1$). Este caso se puede garantizar una solución mediante este mecanismo, si nuevamente, los miembros de Γ^R mantienen su clave pública en secreto y no colaboran con nadie del grupo (ni siquiera otros miembros de Γ^R) para crear caminos de confianza. A partir de este punto, en el que es imposible establecer caminos de confianza de longitud mayor a 1, la única opción que le queda a un miembro que se quiera autenticar es acudir a sus patrones, o sea, a los miembros de su Γ_B^R. Una vez establecida esta restricción, se puede establecer un protocolo de acuerdo entre los patrones (como el sistema bizantino comentado en el apartado 3) para que cada uno de ellos anuncie al resto si su relación hacia la parte a autenticar ha validado o no. Nótese que, en este caso, no se está resolviendo la misma tarea varias veces (en el caso del mecanismo de AC solo hay un único certificado a validar), sinó que se trata de tareas distintas (cada patrón valida su relación), por lo que en este caso sí que es lícito usar un protocolo de acuerdo.

En base a lo expuesto, se puede observar que los mecanismos basados en red de confianza pueden resolver todos los escenarios si se aplican las modificaciones oportunas. De hecho, para el caso específico 4As, están hechos a medida cuando, precisamente, no existe solución directa con mecanismos basados en AC.

5. Conclusiones

En el proceso de control de acceso a grupo se pueden clasificar un conjunto de escenarios diferentes según el grado de implicación de sus miembros. Sin embargo, no todos los mecanismos de control de acceso son capaces de resolverlos todos directamente, al presentar un conjunto de particularidades en su concepción inicial. La principal contribución del presente artículo es la propuesta de qué modificaciones son necesarias de cara a que dichos mecanismos de modo que sean capaces de resolver el máximo de escenarios posible, especialmente dado el caso que actualmente no todos ellos están resueltos. Para lograrlo, se ha tenido presente que la resolución de cada escenario no sea mediante la aplicación de políticas arbitrarias sobre la capacidad de operación de un par.

En conclusión, los mecanismos basados en red de confianza, si se modifican adecuadamente, pueden llegar a proporcionar un gran grado de flexibilidad y disponibilidad a la hora de resolver los escenarios de registro, sin que una baja en el grupo reporte un gran impacto en el sistema. En contraposición a los basados en AC, están mucho más orientados a la autenticación colaborativa, aspecto a tener muy en cuenta a la hora de hacer una elección. A pesar de ello, ambos casos pueden llegar a adaptarse al máximo de escenarios posibles con las modificaciones expuestas.

Referencias

[1] Napster. `http://www.napster.com`.

[2] Rfc2328: Ospf v2. `http://www.ietf.org/rfc/rfc2328.txt`.

[3] Joan Arnedo-Moreno and Jordi Herrera-Joancomartí. Identifying different scenarios for group access control in distributed. *Actas de la IX Reunión Española sobre Criptologia y Seguridad de la Información (IX - RECSI)*, 2006.

[4] Joan Arnedo-Moreno and Jordi Herrera-Joancomartí. Providing collaborative mechanism for peer group acces control. In *Proceedings of the Workshop on Trusted Collaboration*. IEEEPress, 2006.

[5] Tuomas Aura and Silja Mäki. Towards a survivable security architecture for adhoc networks. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *Security Protocols, 9th International Workshop*, volume 2467 of *Lecture Notes in Computer Science*, pages 63–73. Springer-Verlag, Berlin, 2002.

[6] S. Capkun, L. Buttyán, and J.P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing 2 (2003)*, pages 52–64, 2003.

[7] CCITT. The directory authentication framework. recommendation, 1988.

[8] B. Cohen. Incentives build robustness in bittorrent. *1st Workshop on the Economics of Peer-2-Peer Systems*, 2003.

[9] S. Garfinkel. *Pgp: Pretty good privacy.* O'Reilly and Associates Inc., 1994.

[10] Amir Herzberg, Markus Jakobsson, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung. Proactive public key and signature systems. In *CCS '97: Proceedings of the 4th ACM conference on Computer and communications security*, pages 100–110, New York, NY, USA, 1997. ACM Press.

[11] G. Hoeper, K. amd Gong. Models of authentications in ad hoc networks and their related network properties. Technical report, Waterloo, 2004.

[12] J.P. Hubaux, L. Buttyán, and S. Capkun. The quest for security in mobile ad hoc networks. *MobiHoc'01: Proc. of the 2nd ACM int'l symposium on Mobile ad hoc networking & computing*, pages 146–155, 2001.

[13] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, pages 382–401, 1982.

[14] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, and Lixia Zhang. Self-securing ad hoc wireless networks. In *ISCC '02: Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02)*, page 567, Washington, DC, USA, 2002. IEEE Computer Society.

[15] Sun Microsystems. Project JXTA. `http://www.jxta.org`.

[16] S. Yi and R. Kravets. Moca: Mobile certificate authority for wireless ad hoc networks. *The 2nd Annual PKI Research Workshop (PKI 03)*, 2003.

[17] Yuqing Zhang and Dehua Zhang. Authentication and access control in p2p network. In Qianni Deng et al. Minglu Li, Xian-He Sun, editor, *Grid and Cooperative Computing: Proceedings of Second International Workshop, GCC 2003*, pages 468–470, Berlin, 2003. Springer-Verlag. Lecture Notes in Computer Science Volume 3032.

[18] L. Zhou, F.B. Schneider, and R.V. Renesse. Coca: A secure distributed online certification authority. *ACM Transactions on Computer Systems*, pages 329–368, 2002.

[19] Lidong Zhou and Zygmunt Haas. Securing ad hoc networks. Technical report, Ithaca, NY, USA, 1999.