El prototipo de Red de Distribución Cuántica de Claves UPM-TID

D. Lancho[1], J. Martínez[1], D. Elkouss[1], D. Menéndez[2], M. Soto[2] y V. Martín[1]

[1] DLSIIS. Fac. De Informática, U. Politécnica de Madrid. Campus de Montegancedo, 28660 Madrid. vicente@fi.upm.es

[2] Departamento de Seguridad en Redes y Servicios. Telefónica Investigación y Desarrollo. C/ Emilio Vargas 4, 28043 Madrid.

El objetivo de esta contribución es presentar el estado actual y algunos de los resultados del prototipo de red de distribución cuántica de claves* que estamos construyendo, con la finalidad de acercar esta tecnología a un servicio real con posibilidades comerciales. QKD se presenta como un método de alta seguridad para transmitir secretos: con él se puede hacer que dos usuarios conectados por un canal cuántico y uno clásico autenticado compartan una clave y acoten el máximo conocimiento que de ésta pueda tener un hipotético espía. Es decir, salvo por errores en la implementación, se puede establecer una comunicación demostrablemente segura. La implementación de los protocolos de QKD no está exenta de problemas. El principal escollo es la necesidad de producir, detectar y transmitir cuantos de manera individual y bajo demanda. Su rendimiento está muy limitado en alcance y en velocidad de generación de clave por la ineficiencia de los detectores, la incapacidad de generar fotones de manera individual bajo demanda y las pérdidas en el canal cuántico. La inexistencia de repetidores cuánticos y la dificultad de establecer un canal cuántico con un satélite hacen que en la actualidad cualquier red QKD sea necesariamente de ámbito metropolitano [1,2].

Si nos planteamos la viabilidad de su adopción como tecnología de uso generalizado es inevitable una reducción de costes a través del uso compartido de infraestructuras. Es poco realista pensar en que una compañía vaya a construir una red de fibra óptica paralela a la ya existente con el único objetivo de destinarla al canal cuántico necesario para hacer QKD. Las tecnologías de fibra óptica para redes convencionales usadas en la actualidad permiten un uso compartido, aunque evidentemente limitado, de la misma fibra para transportar uno o varios canales cuánticos conjuntamente con otros canales convencionales.

Las limitaciones que nos encontramos vienen impuestas, por un lado, porque estas redes no están diseñadas para pulsos débiles, por lo que las pérdidas que se consideran aceptables en el ámbito clásico son muy grandes desde el punto de vista de la QKD. Por otro, la convivencia de canales cuánticos y convencionales en una misma fibra óptica induce ruido en los cuánticos debido a efectos de dispersión e intermodulación.

Basándonos en tecnologías ópticas pasivas de uso común, hemos creado un prototipo de red para estudiar los límites y problemas de la integración de la QKD en redes de telecomunicaciones. Puesto que se necesita una red fácilmente desplegable, sin enormes costes adicionales, y que dé servicio a la mayor cantidad de usuarios posible, se han usado en la medida de lo posible equipos de comunicaciones de suministradores habituales en telecomunicaciones sin modificar. Por esta misma razón, la estructura de la red está dividida en anillo metropolitano y red de acceso. La integración de red convencional con QKD y el hecho de contemplar explícitamente la red de acceso hacen único a este prototipo.

En la actualidad, el anillo metropolitano está compuesto por tres nodos ROADM† con tecnología CWDM‡. En cada uno podemos inyectar o extraer canales cuánticos. En este es-

* A partir de ahora usaremos su acrónimo inglés: QKD, por *Quantum Key Distribution*.

† Acrónimo del inglés *Reconfigurable Optical Add and Drop Multiplexer*.

‡ Acrónimo del inglés *Coarse Wavelenght-Division Multiplexer*.

cenario, usando líneas de 6 km uniendo los nodos 1 y 2 y de 3,5 km uniendo los nodos 2 y 3, tenemos pérdidas de 5 dB entre nodos contiguos y de 10 dB en una vuelta completa, con lo que obtenemos velocidades de transferencia del orden de 10 Kb/s de clave bruta entre nodos contiguos y de unos 5 Kb/s. en el anillo completo. En el primer caso se obtienen tasas de error de menos del 5% con un canal clásico poblado. Esto con los sistemas QKD instalados en la actualidad, cuyo límite máximo de pérdidas tolerable se sitúa en torno a los 20 dB. Esta velocidad se incrementará notablemente con los nuevos sistemas, cuyo límite de pérdidas es superior a 35 dB.

Los nodos ROADM están a su vez conectados a través de una red de acceso a los usuarios finales. Tenemos dos redes de acceso distintas, con las dos tecnologías que se espera que sean las más utilizadas en un futuro próximo y que ya se están desplegando en muchos países.

La primera de ellas es GPON[§]. Físicamente un nodo en la central de la compañía (en nuestro caso, junto al ROADM) usa una fibra óptica compartida hasta un divisor de señal instalado cerca de los clientes. Del divisor al cliente hay una fibra de uso privado. El ancho de banda se comparte con multiplexación por división en el tiempo entre la central y los nodos de los clientes, a la vez que se usan varias longitudes de onda. Esto tiene como consecuencia que el canal cuántico queda dividido entre todos los clientes, conllevando una pérdida importante en la señal y dividiendo el ancho de banda de claves entre todos los usuarios. Este escenario de grandes pérdidas impone limitaciones muy importantes a la distancia máxima a la que se puede llegar y al número de usuarios finales a los que la red puede dar servicio. Con cuatro usuarios finales, una longitud de línea de pocos kilómetros y el uso de un algoritmo de estados señuelo (que se hace imprescindible) se pueden obtener claves en los extremos, aunque a una baja velocidad con los sistemas utilizados en nuestro prototipo.

El segundo tipo de red de acceso instalada es WDM-PON. Físicamente tiene la misma estructura que GPON, excepto que el divisor es ahora un AWG[¶] y cada usuario tiene asignada una longitud de onda. En este caso las pérdidas son mucho menores y el número de usuarios no supone una penalización para QKD. Este escenario todavía no ha sido completado ya que se hacen necesarias modificaciones específicas en los sistemas de QKD que estamos llevando a cabo.

Los autores agradecen la financiación del Ministerio de Ciencia e Innovación del Gobierno de España a través del Centro para el Desarrollo Tecnológico Industrial, CDTI, y del proyecto Segur@ CENIT-2007, así como del proyecto UPM 178/Q06 1005-127.

Referencias

[1] R. Alléaume et al., "SECOQC White Paper on…", arXiv:quant-ph/0701168, 2007.
[2] C. Elliott et al, "Current status of...", BBN Technologies, arXiv:quant-ph/0503058, 2005.

§ *Gigabit Passive Optical Network*, estándar definido en el documento ITU-T G.984.
¶ *Arrayed Waveguide Grating*.