Conference Paper

Estudio de la Seguridad en Redes de Sensores Corporales aplicadas al Ámbito Sanitario

Isabel de la Torre Díez[1], Carmen Marina Benito Alonso[1], Gema Castillo[2], and Aránzazu Berbey-Alvarez[2]

[1]Universidad de Valladolid, España
[2]Universidad Tecnológica de Panamá, Panamá

Abstract

Nowadays, the technology has become necessary in daily aspects of everyday life, included healthcare and healthy lifestyle. Thus, in the last years has taken place an important development of Body Sensor Networks (BSN) to let a continuous monitoring. Security is becoming increasingly important in all areas related to Information Technology, and becomes even more important when patient's health is involved. Confiability and privacy are necessary requirements for patients to feel secure with the sensors, but the reliability is necessary too, because if all measured data are lost or damage before reaching their destination, it cannot be made an adequate monitor or make the best diagnosis. The aim of this work is to provide a review of the security for BSN applied to the healthcare, in order to enable the development of applications to improve the patient's diagnosis and treatment with chronic diseases.

Keywords: BSN, healthcare,confiability, reliability, chronic diseases.

Corresponding Author:
Isabel de la Torre Díez
isator@tel.uva.es

Received: 15 November 2017
Accepted: 5 January 2018
Published: 4 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ESTEC Conference Committee.

Resumen

Hoy en día, la tecnología se ha vuelto necesaria en los aspectos cotidianos de la vida, incluida la asistencia sanitaria y un estilo de vida saludable. Así, en los últimos años ha tenido lugar un importante desarrollo de las Redes de Sensores Corporales (BSN) para permitir un seguimiento continuo. La seguridad es cada vez más importante en todas las áreas relacionadas con la tecnología de la información, y se vuelve aún más importante cuando la salud de los pacientes está involucrada. Confianza y privacidad son requisitos necesarios para que los pacientes se sientan seguros con los sensores, pero la fiabilidad es necesaria también, porque si todos los datos medidos se pierden o dañan antes de llegar a su destino, no puede darse un monitoreo adecuado o hacer el mejor diagnóstico. El objetivo de este trabajo es proporcionar una revisión de la seguridad de BSN aplicada a la atención sanitaria, con el fin de permitir el desarrollo de aplicaciones para mejorar el diagnóstico del paciente y el tratamiento

con enfermedades crónicas.

Palabras claves: BSN, salud, confiabilidad, privacidad, enfermedades.

1. Introducción

Las redes de sensores de área corporal (*Body Sensor Network*, BSN), son también conocidas como redes de área corporal (*Body Area Network*, BAN) o redes de sensores inalámbricas de área corporal (*Wireless Body Sensor Network*, WBSN), y el interés en la seguridad de este tipo de redes viene fomentado por el gran interés que han suscitado las nuevas tecnologías enfocadas al cuidado de la salud y a las aplicaciones médicas. El uso de las tecnologías ha facilitado mucho nuestra vida cotidiana, pero también ha fomentado una vida mucho más sedentaria. Según la Organización Mundial de la Salud (OMS) actualmente hay 41 millones de niños con obesidad, esto está llevando a que cada vez haya más personas que padezcan enfermedades cardiovasculares y diabetes. Hay 422 millones de personas en el mundo que tienen diabetes (OMS, 2016), de las cuales más del 90% son del tipo 2, además las enfermedades cardiovasculares son la principal causa de muerte en el mundo, más del 30% (OMS, 2017). Todo ello sumado al envejecimiento de la población, hace que sea necesario un sistema sanitario más eficiente y adecuado a este sector de la población, lo que está motivando el desarrollo de redes de sensores que permitan una atención más rigurosa y personalizada.

Las BSN consisten en una serie de sensores interconectados y distribuidos alrededor del cuerpo humano con el fin de recoger, procesar y analizar información para la función que han sido implementados. Se centran en sistemas de monitorización portátiles y en tiempo real con el objetivo de asegurar una continua monitorización de los pacientes, mientras les proporciona una gran libertad de movimientos.

La monitorización y el control de las enfermedades se realizan, por lo general, dentro de los hospitales bajo un entorno clínico y donde todo está esterilizado. Un ambiente muy alejado del entorno real de los pacientes en su vida diaria. Las BSN hacen posible que el médico pueda llevar un control más fiable de sus pacientes permitiéndoles realizar su día a día con total normalidad

Este documento es un estado del arte basado en la recopilación de información y la evolución a lo largo de los años de un tema relevante y con mucho recorrido en el campo de las telecomunicaciones enfocadas a la telemedicina. Todo lo aquí expuesto

está apoyado en información recogida de artículos de diferentes bases científicas, libros especializados en el tema, páginas web, además de valoraciones propias.

2. Seguridad

A pesar del control estricto de los datos sanitarios a los que están sujetos los aparatos de telemedicina suministrados por los hospitales, el abuso está a la orden del día. Y cuando esto ocurre, los datos y la información no pueden cambiarse como si de una cuenta bancaria se tratase puesto que muchas enfermedades son para toda la vida. Los datos médicos, personales e intransferibles, son muy codiciados por los hackers, se paga por ellos diez veces más que por los datos de las tarjetas de crédito. Por otro lado, desde el momento en el que son recogidos y almacenados o enviados a otro nodo receptor los datos son expuestos a todo tipo de violaciones. Lo fundamental que debe ser tenido en cuenta a la hora de realizar un buen diseño de una BSN son los mecanismos de seguridad.

No es una tarea sencilla proporcionar todos estos requerimientos debido a la limitación de la potencia de procesamiento, la energía y la memoria, además, hay que tener en cuenta la vida útil de los dispositivos, la itinerancia de los nodos sensores y algo fundamental, que la mayor parte de los usuarios no son expertos en el uso de estas redes de sensores.

2.1. Criptografía

Desde que los datos médicos son recogidos por los sensores, la seguridad y la privacidad se convierten en elementos fundamentales de una BSN debido a que los datos se asocian directamente a un paciente en particular, además, los datos deben ser fácilmente accesibles ante una emergencia por el personal cuyo acceso esté permitido. Todo esquema que proporcione cualquiera de las características fundamentales frente a la seguridad como son la autentificación, la confidencialidad o la encriptación debe ser diseñado de manera que asegure una baja carga computacional y un bajo consumo de potencia, minimizando el número de mensajes intercambiados y utilizando el menor número de operaciones computaciones criptográficas posibles. Dentro de estos requerimientos se encuentran:

- Proteger la privacidad del paciente desde el lugar de almacenamiento de los datos. No solo porque los datos puedan ser borrados, sino que también se intente aprender el contenido de los datos de los pacientes.

- Que la tolerancia de los sensores de una BSN no se vea comprometida. Ya sea por un sensor perdido o robado, un sensor de una de BSN no debería permitir que alguien no autorizado obtenga datos del paciente.
- Prevenir el acceso no autorizado a la información. El mismo doctor debería poder acceder únicamente a los datos a los que está autorizado y no a todos. Además, debe asegurar que los datos recibidos vengan de un sensor real y no sea un señuelo ya que los tratamientos y decisiones médicas están basadas en información recibida de esos nodos.
- Asegurar la integridad de los datos. Esto permite la verificación de los datos. Los datos no deben ser alterados ni modificados durante la transmisión ya que una alteración no autorizada de los datos puede provocar un diagnóstico erróneo.
- Flexible en la concesión de permisos. El paciente puede decidir permitir el acceso a sus datos a distintas personas y generar distintas claves para cada acceso.

2.1.1. Autenticación

La autenticación es una parte fundamental de una BSN ya que es una garantía que asegura la identidad a los nodos en los que se produce la comunicación. Ya en el 2005, Bao *et al*., (Bao *et al.,*2005), propusieron un esquema de autenticación basado en señales biométricas, en el que se utiliza la información extraída de las señales fisiológicas para proporcionar una verificación e identificación mutua entre los sensores de una BSN. En concreto, y debido a que las señales fisiológicas como la huella dactilar o el patrón del iris utilizadas en otros sistemas de encriptación no son válidas ni seguras para las BSN ya que no varían con el tiempo, en este estudio se utiliza la variación del ritmo cardiaco como señal fisiológica. Las características únicas y totalmente aleatorias de estas señales proporcionan una comunicación segura. En esta misma dirección surgió la idea de utilizar el electrocardiograma (ECC) como señal biométrica (Ramli *et al*, 2013), debido a su naturaleza más estable en un largo periodo de tiempo, a que no requiere un esfuerzo computacional adicional y a sus características únicas de robustez que combinan factores simpáticos y parasimpáticos del cuerpo humano. Una autenticación segura y eficiente debe constar de una serie de fases. Inicialización, registro, identificación y autenticación mutua (See Li *et al*, 2015), (Sarvabhatla, 2015). Shi *et al.,* (Shi et al, 2015) consiguieron reducir la tasa de falso positivo. Con su esquema integrado en la capa física y que se basa en los movimientos corporales se reduce el hardware subyacente mejorando su simplicidad.

2.1.2. Integridad

La integridad de los datos asegura la originalidad de los datos cuando viajan a través de una comunicación inalámbrica entre los nodos de una BSN. La importancia de la privacidad en estas redes radica en que al ser información médica personal es necesario proteger estos datos fisiológicos de escuchas indebidas, inserción de información no autorizada y modificaciones. Algunos autores apuestan por un concepto conocido como esteganografía para las redes BSN (Sankari *et al*, 2012) (Rekha *et a*l., 2014), en el que el mensaje es encubierto en el medio de transmisión, por ejemplo, en una imagen. Por otro lado, Miao *et al* (Miao *et al*, 2009) propusieron un diagrama de bloques en el que se utiliza el modo de cifrado de flujo del estándar de encriptación avanzada (AES) generando un código de autentificación de mensajes (MAC).

Sin dejar de tener en cuenta los nuevos sistemas de almacenamiento en la nube que han surgido en los últimos años algunos autores. He *et al* (He *et al*., 2015) proporcionaron una solución efectiva para chequear la integridad de los datos de forma remota en la nube sin necesidad de descargarlos.

2.1.3. Encriptación

Inicialmente se desarrollaron nuevos sistemas de encriptación debido a que los que existían para las redes inalámbricas de área personal (WPAN) y las WSN no cumplían los requisitos para las BSNs, en cuanto a seguridad, tamaño y peso. Según la HIPAA (la ley de responsabilidad y de la portabilidad de la seguridad de la salud), la encriptación puede ser opcional en las comunicaciones con una red segura, sin embargo, cuando la información es transmitida por una red abierta como Internet debe ser encriptada.

Existen dos tipos de encriptación y ambos son estudiados para su utilización en las redes BSN, la criptografía simétrica y asimétrica. En la mayoría de los esquemas en los que la distribución de la clave se produce de manera simétrica los sensores necesitan pre compartir secretos, lo que no es nada conveniente cuando los secretos necesitan ser actualizados. Por otro lado, aunque se pueden utilizar la criptografía asimétrica en las redes de sensores es complicado distribuir las claves públicas de forma segura.

La criptografía de curva elíptica (ECC) surgió como una opción viable para la criptografía de clave pública gracias a su rápida computación, a su pequeño tamaño y a su baja carga computacional. Sin embargo, más tarde se vio que no era la mejor opción para las BSN debido a que los requerimientos de energía necesarios eran mucho más

altos que los sistemas simétricos (Sil Lee et al., 2015), aunque gracias a su alta seguridad se sigue implementando para la autenticación, generación y mantenimiento de la clave. El esquema Fuzzy Vault (véase Figura 1) es el más utilizado por su simplicidad y a la vez su alto grado de seguridad basado en señales biométricas. En Miao *et al* (Miao *et al*, 2010) se propuso una modificación en el que la información transmitida contiene versión transformada pero nunca una copia exacta de la señal biométrica, lo que impide escuchas indebidas. Consiguió reducir la tasa de error de falsa aceptación y de falso rechazo a costa de reducir el nivel de seguridad, algo que según se trata en Cao *et al.,* (Cao *et al*, 2011) es inaceptable cuando se trata del cuidado de la salud. En Lu et al, (Lu et al., 2014) se muestra un método de reconocimiento de nodos para mejorar la seguridad de una BSN, en el que el diseño del vault se realiza en el espacio de dos dimensiones con codificación en código Gray. En Zheng *et al*., (Zheng *et al*., 2015) se compara el esquema Fuzzy Vault, en el que la biométrica utilizada es directamente el valor IPI, con el esquema *Fuzzy Commitment*, en el que la señal biométrica se obtiene de la generación de secuencias binarias aleatorias de los valores IPI de un ECG. El esquema PSKA utiliza el esquema fuzzy vault para la codificación de la clave y generación del polinomio mientras que utiliza su propio esquema para el intercambio del vault y confirmación de las fases, lo que complica la obtención de la clave a los adversarios (Cao *et al*, 2011) (Lu et al., 2014) (Zheng et al., 2015) (Venkatasubramanian *et al*., 2010). VLC es una avanzada tecnología de comunicación óptica inalámbrica que utiliza el espectro de luz visible como medio de transmisión de los datos. VLC es menos peligroso para la salud de los humanos y proporciona una mayor seguridad puesto que la luz no puede atravesar las paredes, y además no necesita intercambiar secretos pre compartidos (Cahyadi *et al.,* 2015) (Huang *et al.*, 2015). El esquema ABE es muy adecuado para encriptar los mensajes cuando no se conoce con exactitud la identidad del receptor, proporciona un control de acceso detallado, en el que los datos médicos son encriptados por atributos (identidad) y únicamente los atributos que satisfagan la estructura de acceso de la clave podrá descifrarlos (Tian *et al*., 2014) (Shanthi *et al.,* 2015).

2.2. Tolerancia ante fallos

Cuando ocurre un fallo en una BSN, la mayoría de las aplicaciones esperan que una buena fiabilidad les permita seguir operando con normalidad. El sistema debe tener la capacidad de seguir recogiendo información y, más tarde, enviar el aviso al nodo correspondiente para solucionar el fallo. Si por el contrario los datos no pueden ser

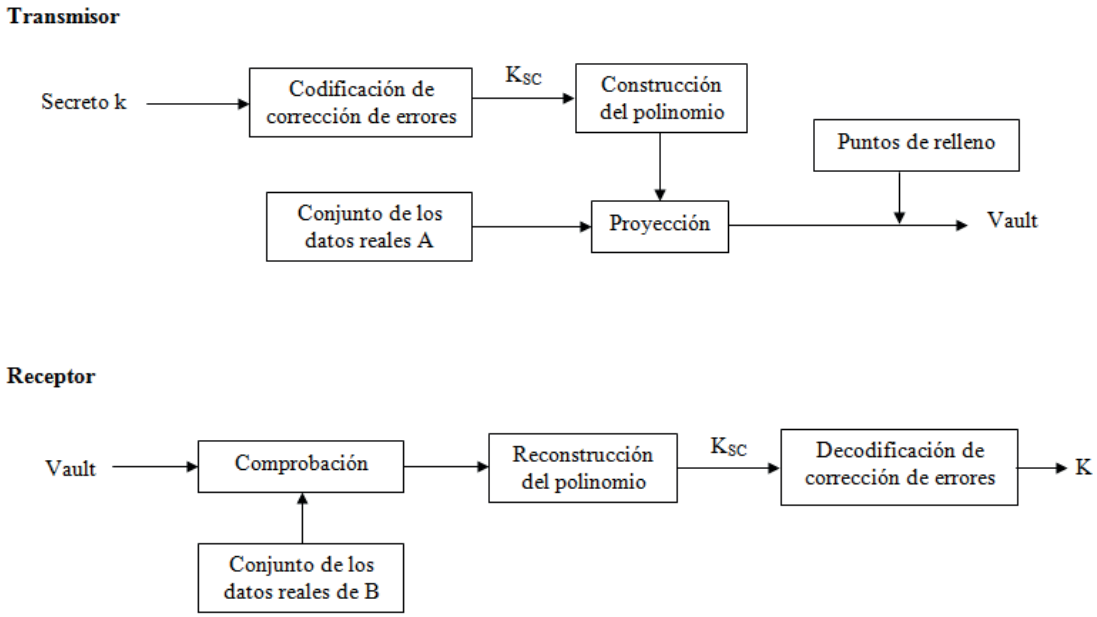

Figura 1: Diagrama de bloques del esquema Fuzzy Vault

enviados, debido a una congestión en la red o a un cambio en la topología, el sistema debe ser capaz de tomar una rápida decisión y redirigir la información por un camino seguro.

Por otro lado, nodos tan pequeños implican baterías de menor tamaño que los sensores utilizados habitualmente en otros tipos de redes, lo que provoca estrictas limitaciones de la energía que se consume en el procesamiento de los datos, en el almacenamiento y en los recursos de la comunicación. El resultado de la pérdida de paquetes en la trasmisión de datos, debido a que la capacidad de almacenamiento de un biosensor suele ser muy limitada, implica que los datos a menudo tengan que ser reenviados, algo que consume mucha energía y provoca que el nodo comience a fallar. Todo ello hace que en algunos casos los datos críticos no puedan ser transmitidos a los nodos de control a tiempo, lo que posiblemente provocará fallos en el diagnóstico.

Se pueden encontrar diferentes tipos de fallos:

- Fallo en el diagnóstico. Existen tres tipos de escenarios que deben tenerse en cuenta en el estudio de la seguridad de toda BSN.
- Diferentes movimientos del cuerpo humano no tienen por qué tener el mismo desplazamiento ni consumir la misma energía, los diferentes tipos de datos fisiológicos tienen diferentes requerimientos de fiabilidad, además en un momento determinado unos nodos pueden tener una actividad muy baja mientras que otros sean altamente activos. Una forma eficaz de solventar estos escenarios es

obtener dos tipos de señales fisiológicas distintas y sus relaciones para evitar un diagnóstico erróneo.

- Fallo en los sensores. Las salidas erróneas procedentes de nodos que han fallado pueden llevar a una interpretación equivocada o a falsas alarmas innecesarias. Se pueden producir fallos provocados por la presencia de nodos defectuosos, la pérdida de la comunicación inalámbrica o por una batería agotada, o fallos causados por un ruido excesivo provocado por un mal contacto o mal funcionamiento de los componentes de un sensor. En sistemas reales, el 80% de los fallos son fallos intermitentes. Son debidos a que el software o el hardware es defectuoso, después de su primera aparición suelen volver a producirse con cierta frecuencia, e incluso llegan a ser permanentes.

- Pérdida de datos. Lo principal es preservar la integridad computacional, esto se realiza gracias a las copias de seguridad de los datos cuando el enlace que ha fallado restablece la comunicación. A nivel de consumo de energía almacenar los datos de forma local implica un gasto menor que de forma inalámbrica. Se pueden encontrar dos tipos de fallos. Fallos de corto alcance, que pueden ser resueltos por los nodos locales sin que sea necesario transmitir ningún tipo de dato a la red de almacenamiento, y los fallos de largo alcance, que los nodos locales no pueden tratar y es necesario reenviar una copia de seguridad de los datos a un destino alternativo para preservar la integridad de los datos.

- Fallo en el medio de transmisión. En Wang *et al.,* (Wang et al., 2015) se demuestra que se puede aislar los sensores implicados en la transmisión con una cierta probabilidad, dependiendo de si la energía restante puede permitir al nodo transmitir directamente al dispositivo encargado de recoger toda la información medida de los sensores, también conocido dispositivo de acumulación. Al igual que en Wang *et al.,* (Wang *et al.,* 2015) en Mahapatro *et al.,* (Mahapatro et *al,* 2015) se demuestra como los fallos están sujetos a una cierta probabilidad. La diferencia en este caso está en que toma el intervalo de tiempo transcurrido entre dos muestras para calcular la probabilidad de detectar si la transmisión ha fallado o no. En Wu et al., (Wu *et al.,* 2010) se propone un esquema adaptativo llamado en el que estudia una estrategia para la reserva del ancho de banda del canal cuando se produce un fallo en el canal de transmisión y así mantener la fiabilidad en la trasmisión de los datos.

3. Conclusiones

Tras realizar el estudio de la seguridad en las redes BSN es importante destacar la gran diferencia de soluciones propuestas de cara a la criptografía respecto a la tolerancia ante fallos, siendo las primeras mucho más numerosas. Dentro de la encriptación de la red, el principal objetivo es buscar esquemas de comunicación en los que los datos del paciente solo sean accesibles para las personas autorizadas, y en cuanto a la funcionalidad del sistema, la seguridad pasa por una buena recuperación del sistema cuando se producen fallos que provocan que los datos no lleguen a su destino.

Referencias

[1] Bao, S. D. Y. T. Zhang and L. F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems", Proc. 27th IEEE Conference on Engineering in Medicine and Biology, pp. 2455-2458, 2005

[2] Cahyadi, W. A. T. Jeong, Y. H. Jim, Y. H. Chung and T. Adiono, "Patient Monitoring Using Visible Light Uplink Data Transmission", International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS) pp 9-12, 2015

[3] Cao, C. Z.; He, C. G., Bao, S. D. and Li, Y. "Improvement of fuzzy vault scheme for securing key distribution in body sensor network, "Proc. Annual Conference of IEEE-EMBS, 2011, pp. 3563-3567

[4] He, D., Zeadally, S. and Wu, L. "Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks", IEEE Systems Journal, pp 1932-8184, 2015

[5] Huang, X. X. Gao, and Z. Yan, "Security protocols in body sensor networks using visible light communications", International Journal of Communication Systems, 2015

[6] Lu, Y. and S. D. Bao, "Efficient Fuzzy Vault Application in Node Recognition for Securing Body Sensor Networks", IEEE International Conference on Communications (ICC), pp 3648 - 3651, 2014

[7] Mahapatro, A. and Mohan Khilar,P. "Fault Diagnosis in Body Sensor Networks", International Journal of Computer Information Systems and Industrial Management Applications. V 5, pp. 252-259, 2012

[8] Miao, F. Bao, S.-D. and Li, Y. "A modified fuzzy vault scheme for biometrics-based body sensor networks security", Proc. IEEE Global Telecommun. Conf. GLOBECOM, pp. 1-5, Dec. 2010

[9] Miao, Fen, Jiang, Lei Ye Li and Yuan-Ting Zhang, "A Novel Biometrics Based Security Solution for Body Sensor Networks", IEEE, 2009

[10] OMS. Organización Mundial de la Salud. ¿Qué son las enfermedades cardiovasculares?" 2017. http://bit.ly/1DH8jUT (Último acceso 25/04/2015).

[11] OMS. Organización Mundial de la Salud. Informe mundial sobre la diabetes http://bit.ly/22esx2d. Abril 2016. (Último acceso 25/04/2017).

[12] Ramli, S.N. R. Ahmad, M.F. Abdollah, E. Dutkiewicz," A Biometricbased Security for Data Authentication in Wireless Body Area Network (WBAN)," Advanced Communication Technology (ICACT), pp. 998-1001, Jan. 2013.

[13] Rekha, R. T. Gayathri Mathambigai, and Dr.R. Vidhyapriya, "Secure Medical Data Transmission in Body Area Sensor Networks Using Dynamic Biometrics and Steganography", Bonfring International Journal of Software Engineering and Soft Computing, 2012

[14] Sankari, V. and K. Nandhini, "Steganography Technique to Secure Patient Confidential information using ECG Signal", International Conference on Information Communication and Embedded Systems (ICICES), 2014

[15] Sarvabhatla, M. and C.S. Vorugunti, "An energy efficient mutual authentication scheme for secure data exchange in health-care applications using wireless body sensor network", Future Information Security Workshop, COMSNETS, 2015

[16] Shanthi, A. V. K "FINE-GRAINED ACCESS OF PERSONAL HEALTH RECORD IN CLOUD COMPUTING", ARPN Journal of Engineering and Applied Sciences, Vol 10, no. 22, 2015

[17] Shi, L., J. Yuan, S. Yu and M. Li, "MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, pp 52-62, 2015

[18] Sil Lee, Y. B. Ndibanje, E. Alasaarela, T. Y. Kim and H. Lee, "An Effective and Secure User Authentication and Key Agreement Scheme in m-Healthcare Systems", 7th IEEE International Symposium on Cyberspace Safety and Security (CSS), 2015

[19] Sil Lee, Y. B. Ndibanje, E. Alasaarela, T. Y. Kim and H. Lee, "An Effective and Secure User Authentication and Key Agreement Scheme in m-Healthcare Systems", 7th IEEE International Symposium on Cyberspace Safety and Security (CSS), 2015

[20] Tian, Y. Y. Peng, X. Peng and H. Li, "An Attribute-Based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2014

[21] Venkatasubramanian, K. K, A. Banerjee, S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks, " IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, 2010, pp. 60-68

[22] Wang, Y., Li. Xing, H. Wang and G. Levitin, "Combinatorial analysis of body sensor networks subject to probabilistic competing failures", Reliability Engineering & System Safety, V 142, pp 388-398, 2015

[23] Wu, G.; J. Ren, F. Xia and Z. Xu, "An Adaptive Fault-Tolerant Communication Scheme for Body Sensor Networks", Sensors, 2010

[24] Zheng, G., G. Fang, M. A. Orgun and R. Shankaran, "A Comparison of Key Distribution Schemes Using Fuzzy Commitment and Fuzzy Vault within Wireless Body Area Networks", 26th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): Services Applications and Business, pp 2120-2125, 2015

Authorization and Disclaimer

Authors authorize ESTEC to publish the paper in the conference proceedings. Neither ESTEC nor the editors are responsible either for the content or for the implications of what is expressed in the paper.