Personal and Ubiquitous Computing (2019) 23:793–799
https://doi.org/10.1007/s00779-018-1128-3

ORIGINAL ARTICLE

ECASS: an encryption compression aggregation security scheme for secure data transmission in ambient assisted living systems

Bacem Mbarek[1] · Nafaâ Jabeur[1] · Ansar-Ul-Haque Yasar[2]

Received: 23 December 2017 / Accepted: 1 March 2018 / Published online: 10 March 2018

Abstract

Considerable efforts are being spent worldwide to ensure comfortable living environments and decent, on-time assistance to elderly and people requiring healthcare services. Recent advances in data acquisition and communication are allowing revolutionary ambient assisted leaving (AAL) systems to be implemented, where healthcare data are collected and reported on-the-fly to dedicated medical servers for further analysis and actions. Due to the increasing rely on distributed, resource constrained sensing devices, AAL systems are being subject to large number of attacks. In addition to usual high energy consumption and communication overhead, current systems are not yet able to fully safeguard the private data of their users. To overcome these shortcomings, we propose in this paper to combine the use of cryptography, compressed sensing, and steganography into a new generic solution called Encryption Compression Aggregation Security Scheme (ECASS). While focusing on the specific case of Medical Healthcare Systems, ECASS aims to secure private data exchanges over wireless networks while achieving lower energy consumption and communication overhead. Our simulations with the NS-2.35 simulator are showing an improvement of 40 and 50% in terms of energy consumption and communication overhead respectively compared to the IBE-Lite security scheme.

Keywords Ambient assisted leaving · Security · Healthcare · Steganography · Compressed sensing · Cryptography

1 Introduction

Thanks to continuous progress in mobile and pervasive computing technologies, ambient assisted living (AAL) systems are attracting increasing attention from the research and development community. The main goal of these systems is to apply ambient intelligence technology to enable people with specific demands (e.g., handicapped or elderly) to maintain their independence regarding daily routines and with respect to outpatient and inpatient nursing and medical care. The market share of AAL systems in home health monitoring has increased from 420,000 in 2010 to around 570,000 in 2011 and estimated to hit 2.47 million in 2016, according to a recent research report ([1]). Furthermore, according to Berg Insight firm [2]), there were three million patients using connected home medical monitoring devices worldwide in 2013. The firm is expecting the estimated revenue to jump from almost 4 billion euros in 2013 to reach more than 19 billion euros in 2018. In spite of this huge interest, the security of patient data remains one of the most critical requirement to guarantee effective AAL operations. Several research works in the literature (e.g., [3]) have proposed dedicated authentication protocols for the AAL systems. In these protocols, it has been proven that the implementation of security policies (e.g., [4]) is a complex and challenging issue as it requires resources exceeding what is generally available. In addition, shortening transmission distances (e.g., [5]) would reduce the spectrum of security threats, but remains ineffective in preventing a wide range of risks, including spoofing, message altering and replaying, flooding, and wormhole attacks [6]. The deficiencies

✉ Bacem Mbarek
bacem.mbarek1@gmail.com

Nafaâ Jabeur
nafaa.jabeur@gutech.edu.om

Ansar-Ul-Haque Yasar
ansar.yasar@uhasselt.be

[1] German University of Technology in Oman (GUtech), Athaibah, Oman

[2] Transportation Research Institute Hasselt University, Hasselt, Belgium

of current approaches in effectively securing AAL systems is mainly due to the commonly limited storage, processing, and transmission capabilities of system edge devices (such as healthcare sensors) as well as their proprietary technologies. Consequently, we argue that thorough investigations are still needed to enable transmitting securely private patient data over wireless networks while guaranteeing data authenticity, freshness, replay protection, integrity, and confidentiality. Within this context, we propose a secure data transmission scheme for a three levels AAL system architecture: micro level (to collect and report data of interest about patients' health conditions and supporting medical equipment), meso level (to aggregate micro level's data), and macro level (to store and analyze data as well as instruct the meso and micro levels for further actions). In order to ensure secure communication between the three levels of our architecture, we propose a novel Encryption Compression Aggregation Secure Scheme (ECASS). Our approach is based on a Compressed Sensing (CS) approach to minimize the communication overhead and reduce power consumption, a cryptography hash algorithm to ensure data integrity, and a steganography algorithm to aggregate and hide private medical data into selected images.

The remainder of this paper is organized as follows. In Section 2, we present works related to securing communication in the specific context of AAL, namely medical healthcare systems. In Section 3, we outline our network model and describe our proposed ECASS solution. In Section 4, we present a security analysis of ECASS. In Section 5, we provide a thorough performance evaluation.

2 Related work

Several works (e.g., [7, 8]) have attempted to provide elderly and people requiring medical assistance with convenient services to live safely, securely, healthily, and independently. To ensure personalized services, private healthcare data are collected by using physiological signals, such as blood flow, heart interval, and electrocardiography. These data are then sent to remote controllers for extended analysis, particularly because of the current limited storage, processing, and communication capabilities of sensing devices. Because of the same reasons, conveying private medical data over wireless connexions is still subject to a wide range of security attacks. In order to prevent attacks on private medical data, security schemes based on shared symmetric cryptographic keys are used to protect the transmission of health information over the wireless network. In spite of their reported performance, these symmetric schemes are still suffering from delayed authentication. They are also susceptible to DoS attacks due to late authentication [9]. As alternatives to such schemes, Tan et al. [10] have proposed a lightweight identity-based cryptography scheme, called IBE-Lite. Applied to body sensor networks, IBE-Lite has the limitation to not consider sensor-to-sink (or user) data authentication. Consequently, false medical data could be injected or treated as legitimate due to the lack of node authentication. Zhou and Chao [11] have presented a novel media-aware traffic security architecture, where four major components are highlighted, namely key management, batch rekeying, authentication, and watermarking. The authors have classified the key management according to the multimedia traffic as well as the scalability of the security scheme. They have also proposed to change the key based on synchronization and inefficiency. To ensure secure communication in wireless body area network (WBAN), Liu et al. [12] have used a bilinear pairing approach defined on the elliptic curve to design a new certificateless signature scheme. Although the preliminary results seem to be promising, the proposed scheme provides non traceability. This is because the user's identity is a constant value, which makes it easy for the adversary to trace the client by observing this value.

Very recently, Le et al. [13] suggested a mutual authentication and access control protocol (MAACE) where legitimate professionals can access their patient's data. The MAACE facilitates mutual authentication and access control, which is based on elliptic curve cryptography (ECC). Furthermore, these authors argue that their scheme is secure enough in practical attacks, e.g., replay attack, and denial-of-service attacks. Their architecture (i.e., MAACE) consists of three layers: (i) sensor network layer (SN); (ii) coordination network layer (CN); and (iii) data access layer (DA). In their architecture, the SN transmits data to the CN (i.e., PDA, laptop or cell phone), later, the data is forwarded to the DA for future record. Although, Le et al.'s protocol facilitates sufficient security against practical attacks, but their scheme is susceptible to information-leakage attacks, which could be risky for the patient's privacy. As a result, patient vital signs could be exposed to illegal users (e.g., insurance agents, media persons), which is not acceptable for real-time healthcare applications. Thus, a strong user authentication is required for the healthcare application using sensor networks.

Huang et al. [14] proposed a secure hierarchical sensor-based healthcare monitoring architecture. The proposed architecture has three network tiers (i.e., sensor network, mobile network, and back-end network) and has considered three real-time healthcare applications (i.e., in-hospital, in-home, and nursing-house) scenarios. The authors used wearable sensor systems (WSS) and wireless sensor motes (WSM) at the sensor network tier. The WSS are Bluetooth enabled and integrated with biomedical sensors; and the WSS are strategically placed on the patient's body, whereas, the WSMs are deployed within the building, and are used to collect the environmental parameters and transmit through the Zig-bee wireless network standard. WSS and WSM broadcast data securely to the upper layer. Here, WSS uses an advance encryption standard (AES)-based authentication and encryption, while WSM uses a polynomial-based encryption scheme to establish secure point-to-point communication between two WSMs. In the mobile network tier, mobile computing devices (MCDs) such as PDAs are organized as an ad-hoc network and connected to the local station. MCD has the more computational capabilities to analyze the WSS and WSM data. The back-end tier is structured with a fixed station as a server, that provides application level services for lower tiers and process various sensed data from MCDs.

3 Data secure transmission protocol in AAL

Our system architecture includes sensor nodes, each of which consisting of a set of sensors for the collection of medical-related data. Depending on current communication coverage, which is affected by nodes' capabilities as well as indoor settings, a variable number of routing nodes may be needed. Sensor nodes will be sending their data on regular basis, on-demand, or depending on sporadic assistance needs (e.g., heart attack requiring immediate assistance) to dedicated data collectors for further processing and actions. For example, if we assume that a number of patients are being admitted in the same room and each patient is holding a sensor node, then a data collector entity will be a room controller (RC). In addition to collecting, processing, and aggregating data from related sensor nodes, a RC is responsible of conveying the collected data to a dedicated server where further actions will be performed. As our focus is on securing data communications, the actions performed on data by any RC or by the dedicated server are out of the scope of this paper. Without loss of generality, we will be explaining our approach based on the system architecture depicted in Fig. 1 and including the following levels: micro level, meso level, and macro level.

- **Micro level** – This level consists of wireless sensor nodes (SNs). Each SN has several sensors connected to the patient's body to measure medical information pertaining to the current health condition of that patient. We assume that a SN has the following common components: sensor hardware, a power unit, a micro-controller, an external memory, and a transceiver [15]. Because of privacy issues as well as needs for real-time action during emergency situations, SNs must be endowed with appropriate mechanisms to convey the

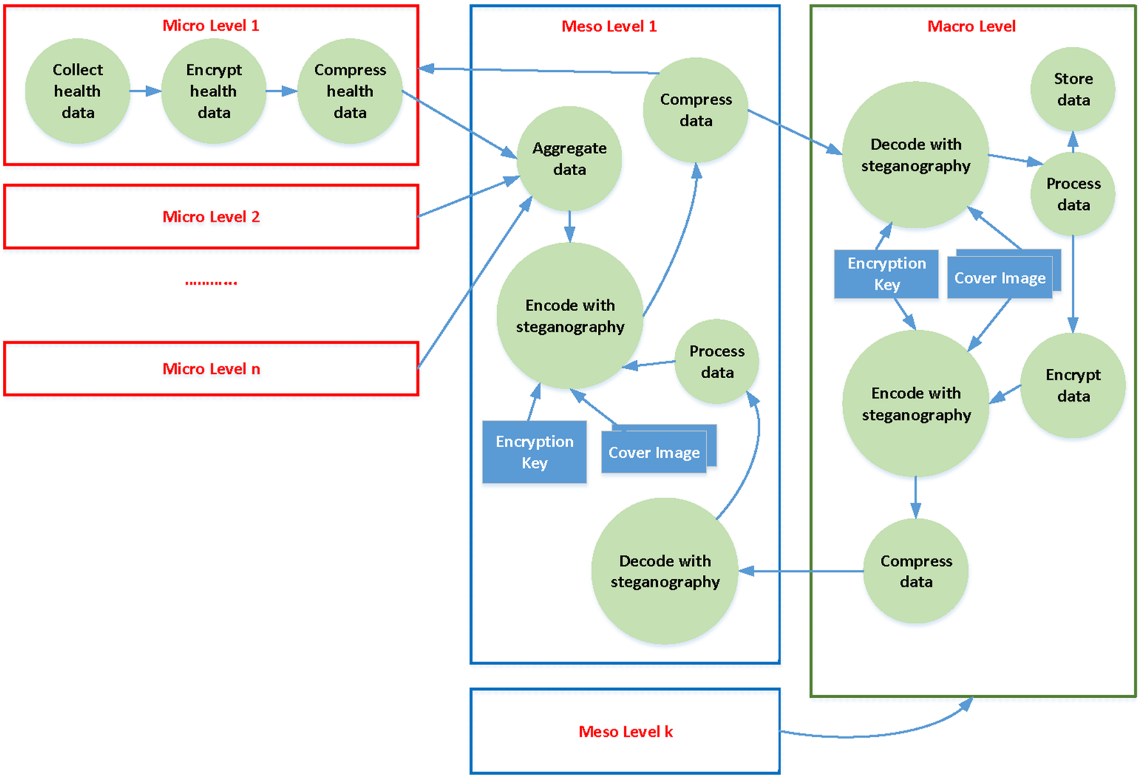

Fig. 1 Hiding steganography method

collected data to the meso level over secure communication channels.

- **Meso level** – This level includes several room controllers (RCs). Every RC is responsible of collecting data from SNs and conveying them to the macro level after performing some actions (e.g., aggregating data). Appropriate mechanisms are needed to enable a secure communication between a RC and the macro level as between a RC and the micro level. In our architecture, every RC is acting as a cluster head for a group of SNs falling within its communication range. As our focus is on security issues, the management of handover between clusters is out of the scope of this paper. Also, we suppose that patients are not mobile. Mobility is out of the scope of the current paper.
- **Macro level** – This level includes a Health Management Server (HMS) that receives all data packets from all RCs of the Meso Level. The HMS has the responsibility to process and store the data received from all RCs as well as make the necessary data analysis to identify and convey appropriate actions to the right SN through the right RC, at the right time. Our focus in this work is to enable a secure communication between the HMS and any RC.

3.1 Encryption compression aggregation-based security scheme (ECASS)

This section provides an overview of our proposed security scheme, ECASS. Our scheme is essentially based on three distinctive phases: data encryption, data compression, and data aggregation based on a steganography approach. We explain in what follows each of these steps.

3.1.1 Encryption phase

The encryption phase of our solution is using an encryption protocol based on key pre-distribution [16]. Our choice is motivated by the capability of this protocol to provide a robust and efficient security model based on dynamic key updating. Our choice is also motivated by the use of a XOR logical operation between the hash value of the medical information and the individual key of each SN to prevent adversaries from inferring the shared key. In our proposed solution, we use the HMS server for generating, storing, and distributing the security parameters. The encryption protocol is executed as follows. During the deployment phase, every SN is initially loaded with a polynomial share $g(Sid_i, c)$, whereas every RC is initially charged by $g(Rid_i, c)$, where Sid_i is the identity of the SN, c is the compressed data, Rid_i is the identity of the RC, and g is a symmetric function . Furthermore, the HMS holds two keys, K_j and K_i. The key K_j is used to protect the data transmitted over wireless connections between SN and RC. The key K_i can be used to secure communications between the HMS and any RC. The individual key of node N_j is calculated as follows.

$$K_i^j = K_i^{j-1} \oplus h(data_i^j) \tag{1}$$

Every sensor node (N_i) generate the encrypted text c_i^r it is willing to send using the key K_i as follows:

$$c_i^j = E(\{data_i^j, j\}, K_i), h(data_i^j, K_i) \tag{2}$$

$data_i^j$ is the compressed data by the node N_j at round r, and $(h(data_j^j, K_j)$ is a hash value computed and forwarded with $data_i^j$.

After being encrypted, the medical information is compressed (as explained below) and sent by the sensor node N_i to the RC to which it belongs. The RC can decrypt the ciphertext by using $g(Rid_i, c)$. Hence, for correct and positif test, the RC can be sure that the received message is coming from node N_j and the data have not been modified by an attacker.

3.1.2 Data compression phase

In healthcare applications, sensing health data may be comparable with, or even greater than, that of radio communication [17]. It has been proven that the Compressing Sensing theory could solve these limitations [18]. Indeed, by compressing the signal throughout, the energy consumption overhead of communications could be reduced by up to 30% while keeping a very high performance of the signal [19]. Compressed Sensing (also known as compressive sensing, compressive sampling, or sparse sampling) is a processing technique to efficiently acquire and reconstruct signals, by finding solutions to underdetermined linear systems [20, 21].

The compressing sensing message c is constructed as follows:

$$c = \Phi v \tag{3}$$

where c is the compressed data and v is the original data. The CS is a new data compression paradigm, is compressed by a full row-rank random matrix, denoted by Φ. A simple and practical method used to complete the sparse solution and to avoid the convex optimization problem. The compressing sensing algorithm uses Φ and c at the RC end to reconstruct the original data v.

$$v \epsilon R^L min||v||l_1 \; subject \; to \; c = \Phi\Psi v \tag{4}$$

where, Ψ is a basis $N \times L$ matrix used to construct the data and decompress the compressed data.

The recovered data is then $f = \Psi x^*$, where x^* is the optimal solution to 4.

3.1.3 Steganography-based data aggregation

As mentioned earlier in this paper, medical data are being sent from the micro level (sensor nodes) to the meso level (room controllers) where they undergo some processing according to some predefined schemes. It is expected from each RC to aggregate the data received and convey it to the macro level. Several options are possible. One of these options is to encrypt all the encrypted data received from the micro level, aggregate them into a medical report, encrypt this report, and then send the resulting file to the HMS. In this paper, we are opting for the use of steganography to secure and encode the scattered medical data into a cover image . This image is then sent to the HMS. steganography is the art and practice of communication using hidden messages. These messages are often disguised within something else where one would not expect a message to be contained in.

After the reception of the compressed and encrypted data from the sensor nodes, the cluster head uses steganography method to aggregate the data packets received into a single image, which is transmitted to the sink. Figure 1 shows a simple representation of the generic embedding and decoding process in steganography. In this example, a secret compressed encrypted message is being embedded inside a cover image to produce the stego image [22]. The first step in embedding and hiding information is to pass both the compressed encrypted message message and the cover image into the encoder. Inside the encoder, the steganography function uses a secret key (for example, converts the first received data to ASCII code and change only one Bit per Pixel) to embed the secret information into the cover message. Second, The CH saves the new picture and sends it to the receiver. The receiver can decode the received picture and discover the received message by get/select from the received picture all of bit changed in the different pixels. The size (width and hight) of the image pre-defined an all nodes in the phase of deployment. The receiver is able to decompressed first and then decrypt all of data collected from the cover image by using its private key because they are crypted by its public key.

4 Security analysis

In this section, we present the security model and present the different services guaranteed by our proposed architecture.

Confidentiality An attacker may try to access the medical care environment without authorization with the aim to falsify assistance needs and/or endanger patients' lives. In order to prevent such threats, we are proposing to send encrypted medical information based on symmetric cryptographic key sharing. In addition to guaranteeing confidentiality, this security scheme allows for encrypting and generating illegible messages. It has been proven (e.g., [22]) that these messages are only accessible by authenticated parties. For additional confidentiality, steganography is used alongside with cryptography.

Data integrity and authentication An attacker may attempt to inject, replay, disorder, or modify the authentication headers in the message packets to ultimately harm the medical system functionalities (e.g., responding to assistance demands, managing patients' electronic reports, and billing). In order to prevent such attacks, we apply hash algorithms to each original data, where the private hash key is only known by the source. More specifically, we are using the class SHA- 1 which is a member of the class of universal hash functions [23]. Thus, in our implementation, we have selected SHA- 1. It has been proven (e.g., [6]) that using such algorithm enable to prevent malicious modifications of encrypted messages.

Scalability In our approach, key generation and maintenance is performed at the macro level (HMS), which is assumed to have extended processing and storage capabilities. Some related operations could be delegated to the meso level (e.g., RC), which is also assumed to have extended processing and storage capabilities. At the edges of our system (micro level), cryptography operations requiring limited processing overhead are performed by the SNs. These operations as well as the operations performed at the meso and macro levels are unlikely to be affected by the network size. It could then be concluded that the micro level and the meso level could be extended with any additional number of healthcare SNs and RCs respectively.

5 Performance evaluation

We used the NS-2.35 simulator [24] to analyze the performance of the MWSN scheme in terms of energy consumption and memory overhead. We run our simulations on a large scale network of 1000 nodes. We assume that all nodes have a fixed position throughout the period of simulation, with the settings provided in Table 1. Note that we also have one base station (HMS server) that collects the information from the cluster heads. In all simulation scenarios, we have six cluster heads.

We compared our proposed approach with IBE-Lite protocol that provide security and privacy protections while allowing flexible access to stored data. While IBE has been actively studied and widely applied in cryptography research.

Table 1 Simulation parameters

Parameter	Value
Simulation area	(500 × 500)m
MAC type	802.15.4
Run times	50 times
Simulation time	100 s
Number of nodes	1000
Number of cluster heads	6

5.1 Energy consumption

Figure 2 illustrates a comparison of energy consumption between our proposed scheme and the IBE-Lite [25] protocol. We note that the ECASS curve shows a clear decrease in energy consumption compared to the IBE-Lite curve. For example, at time of 2 h, IBE-Lite uses about 220 (j) whereas ECASS consumes only 140 (j). This may be explained by the fact that IBE-Lite uses asymmetric key encryption (known to be costly in terms of energy [26]) to secure communications in wireless medical systems. Conversely, thanks to the use of a secure data aggregation scheme based on symmetric function and deploying compressed sensing (CS), our ECASS solution is able to reduce communication overhead and consequently reduce energy consumption.

5.2 Communication overhead

Figure 3 illustrates the maximum communication overhead of the two protocols, ECASS and IBE-Lite. We notice that ECASS has a significantly lower communication overhead than IBE-Lite. In fact, ECASS uses a Meso Level (i.e., RCs) to aggregate different medical data received from the micro level. By compressing the data and sending a single compressed file over the network, ECASS is able to reduce communication exchanges between the meso level and the macro level as well as within the meso level if RCs are used as routers to convey data to the HMS. In contrast, with IBE-Lite, the controller sends all detected values separately.

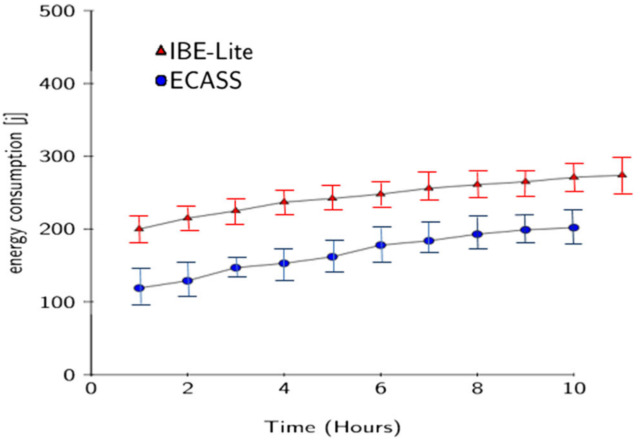

Fig. 2 Energy consumption as function of time (95% confidence interval)

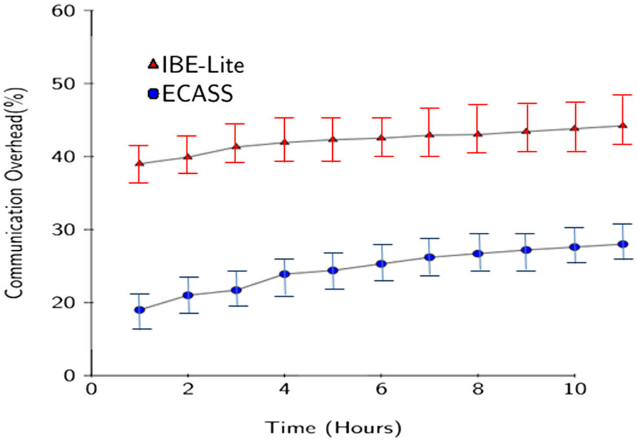

Fig. 3 Communication overhead as function of time (95% confidence interval)

6 Conclusion

The ever increasing use of distributed sensing devices is enabling ambient assisted leaving (AAL) systems to collect in situ data of interest and propose customized healthcare services within acceptable window frames. However, because of their constrained resources, these sensing devices are being subject to a large number of attacks during private data exchanges over wireless networks. In order to prevent these attacks, we presented in this paper a three-level network model where medical data are securely exchanged between peers from micro level (i.e., sensor nodes), meso level (i.e., room controllers or more generally cluster heads), and macro level (i.e., Health Management Server). To meet our goals, we proposed a novel Encryption Compression Aggregation Security Scheme (ECASS). ECASS is based on effective approaches for symmetric cryptographic keys, compressed sensing, and steganography to safeguard private healthcare data. Compared to the IBE-Lite security scheme, we confirmed with NS2 simulations that ECASS reduces energy consumption and lowers communication overheads by 40 and 50%, respectively. In the future, we are planning to compare our solution to additional security schemes (such as MAACE [13]). We are also planning to measure the effect of interchanging the steps of encryption, compression, and aggregation on the performance of our security scheme (i.e., use compression encryption aggregation, aggregation encryption compression).

References

1. Dolan B 2.2m people using remote patient monitoring at the end of 2011. available online: http://mobihealthnews.com/15487/berg-2-2m-patients-remotely-monitored-globally (accessed on 18 november 2013). Tech. Rep.
2. Berg insight. mhealth and home monitoring. berg insight's m2m research series 2014. in http://www.berginsight.com, accessed November 15, 2015, p. 305 pages
3. He D, Zeadally S (2015) Authentication protocol for an ambient assisted living system. IEEE Commun Mag 53(1):71–77
4. Yeh C-K, Chen H-M, Lo J-W (2013) An authentication protocol for ubiquitous health monitoring systems. Journal of Medical and Biological Engineering 33(4):415–419
5. Li M, Lou W, Ren K (2010) Data security and privacy in wireless body area networks. IEEE Wirel Commun 1:17
6. Li X, Niu J, Kumari S, Liao J, Liang W, Khan MK (2016) A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Security and Communication Networks 9(15):2643–2655
7. Sahaa S, Tomar SK (2013) Issues in transmitting physical health information in m-healthcare. Int J Curr Eng Technol 3:411–413
8. Pu Q, Wang J, Zhao R (2012) Strong authentication scheme for telecare medicine information systems. J Med Syst 36(4):2609–2619
9. Mbarek B, Meddeb A, Jabalah W, Mosbah M (2016) A broadcast authentication scheme in iot environments. In: IEEE/ACS 13th international conference on computer systems and applications (AICCSA). IEEE, Piscataway, pp 1–6
10. Tan CC, Wang H, Zhong S, Li Q (2009) Ibe-lite: a lightweight identity-based cryptography for body sensor networks. IEEE Trans Inf Technol Biomed 13(6):926–932
11. Zhou L, Chao H-C (2011) Multimedia traffic security architecture for the internet of things. IEEE Netw 3:25
12. Liu J, Zhang Z, Chen X, Kwak KS (2014) Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Trans Parallel Distrib Syst 25(2):332–342
13. Le XH, Khalid M, Sankar R, Lee S (2011) An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. J Networks 6(3):355–364
14. Huang Y-M, Hsieh M-Y, Chao H-C, Hung S-H, Park JH (2009) Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. IEEE J Sel Areas Commun 4:27
15. Zhang Z-K, Cho MCY, Wang C-W, Hsu C-W, Chen C-K, Shieh S (2014) Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, Piscataway, pp 230–234
16. Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, Yung M (1992) Perfectly-secure key distribution for dynamic conferences. In: Annual international cryptology conference. Springer, Berlin, pp 471–486
17. Chen F, Chandrakasan AP, Stojanovic VM (2012) Design and analysis of a hardware-efficient compressed sensing architecture for data compression in wireless sensors. IEEE J Solid State Circuits 47(3):744–756
18. Yang G, Tan VY, Ho CK, Ting SH, Guan YL (2013) Wireless compressive sensing for energy harvesting sensor nodes. IEEE Trans Signal Process 61(18):4491–4505
19. Li S, Da Xu L, Wang X (2013) A continuous biomedical signal acquisition system based on compressed sensing in body sensor networks. IEEE Trans Ind Inf 9(3):1764–1771
20. Baraniuk R, Davenport MA, Duarte MF, Hegde C et al (2011) An introduction to compressive sensing, Connexions e-textbook
21. Eldar YC, Kutyniok G (2012) Compressed sensing: theory and applications. Cambridge University Press, Cambridge
22. Hamid N, Yahya A, Ahmad RB, Al-Qershi OM (2012) Image steganography techniques: an overview. Int J Comput Sci Secur (IJCSS) 6(3):168–187
23. Ostlin A, Pagh R (2003) Uniform hashing in constant time and linear space. In: Proceedings of the Thirty-fifth annual ACM symposium on theory of computing. ACM, New York, pp 622–628
24. Downard IT (2004) Simulating sensor networks in ns-2, DTIC Document, Tech Rep.
25. Kamilaris A, Tofis Y, Bekara C, Pitsillides A, Kyriakides E (2012) Integrating web-enabled energy-aware smart homes to the smart grid. International Journal On Advances in Intelligent Systems 5(1):15–31
26. Amin F, Jahangir A, Rasifard H (2008) Analysis of public-key cryptography for wireless sensor networks security. World Acad Sci Eng Technol 41:529–534