A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth

Kashif Habib, Arild Torjusen, Wolfgang Leister
Norwegian Computing Center
Oslo, Norway
Kashif.Sheikh@nr.no, Arild.Torjusen@nr.no, wolfgang.Leister@nr.no

***Abstract*—Patient monitoring outside the hospital environment is one case for Internet of Things (IoT) in healthcare. While remote patient monitoring may improve healthcare, patient authentication is a challenge in this scenario. Authentication mechanisms that require the user to present credentials only initially do not verify the claimed identity of the patient after the initial authentication. We propose a novel authentication framework based on biometric modalities and wireless device radio fingerprinting. The framework is capable of verifying that the monitored data belongs to the correct patient during the entire session, it also ensures the integrity and trust of the received data. We analyse our framework in view of some issues for the IoT in eHealth such as context and location awareness, resource constraints, and dynamic environment.**

Keywords—Internet of Things; eHealth; biometric authentication; radio fingerprinting.

I. INTRODUCTION

The current Internet is rapidly evolving towards the Internet of Things (IoT) environment where different objects communicate and exchange information with each other for improved functionalities and performance. While monitoring patient's health parameters with on-body sensors, the IoT may allow the patient to be at different locations such as home, office, public place, or in a vehicle but medical sensors still connected and transmitting information to the doctor's office.

The healthcare system can get many benefits by using flexible Remote Patient Monitoring (RPM) in the IoT for eHealth such as patient monitoring with chronic disease, monitoring of elderly people, and monitoring of athletes fitness [1]. The main objective of the RPM system is to assist the existing healthcare system by monitoring the vital signs of patient's health data in real time.

A. Research questions

With a RPM scenario as a basis, we address the establishment of trust in the received data in two parts: 1) how do we know that the data monitored during the entire session in the RPM system belongs to the correct patient, i.e., data origin authentication; 2) how do we ensure the *integrity* of the received data.

More specific for a health scenario, we address two parts: 1) how can we know if the patient is suffering from a heart attack or other acute conditions; 2) how can we locate a patient that is suffering from some acute incident.

B. Security challenges for the IoT in eHealth

Transferring a patient's health data to a remote medical server opens for security threats such as interception, interruption, modification, and fabrication [2]. These threats may impact on a patient's privacy, confidentiality of data transmission, integrity of received data, and data availability.

Authentication is a key aspect in terms of establishing trust in the system. Although, trust can be defined for different purposes and application areas in several disciplines [39], our criteria to determine trust in the RPM system is simple. If we establish a mechanism capable of ensuring that the received data is coming from a correct device and patient, then it can serve the purpose of trust establishment. If the sensors are used by someone else except the actual patient, the authentication mechanism should be capable of detecting the imposter at any time during the monitoring session. The capability to detect an imposter not only increases the effectiveness of system security but also maintains the trust level in the system.

C. Biometric and radio fingerprinting

The continuous RPM requires continuous verification of monitored data to establish trust. In order to ensure that the received data is coming from the correct patient and is correct, verification of data origin and integrity are important elements in the RPM system. For this purpose, one can use authentication mechanism to ensure the correctness of data origin before the data is used for medical diagnosis. Authentication mechanisms based on credentials such as secret keys, password, and tokens possess vulnerabilities for the RPM system. One of the reasons is that if a third party gets access to the credentials, then he can impersonate the actual patient causing data fabrication and data integrity issues. Also, after initial authentication using these credentials, there is no guarantee that the data is still coming from the authenticated patient throughout the session. The RPM system demands continuous monitoring of the patient which also implies that the monitored data should be validated on a continuous basis until the session ends [3] [4]. The RPM system should ensure not only that the monitored data belongs to the actual patient during the whole monitoring period but also that it is sent using the correct device. This may be achieved using biometric and radio fingerprinting since they have direct association with the user and the device.

 ISBN: 978-1-61208-363-6

D. Contribution

The goal of our work is to develop a more reliable authentication system that can prevent the misuse of the RPM for the IoT in eHealth. Our main contribution in this paper is to propose a novel authentication framework for the IoT in eHealth. More specifically, a patient is authenticated by the following tuple:

(P, B, F), where P is patient's physiological biometric, B is patient's behavioral biometric, and F is patient's smart phone radio fingerprint.

In contrast to existing techniques that use only biometric modalities, our approach binds together the biometric modalities and radio fingerprinting technique as a unique identifier to not only authenticate the patient but also the device transmitting health parameters. However, biometric and radio fingerprinting used separately for authentication in the RPM pose some shortcomings. For example, using radio fingerprinting only, the device can be authenticated but not the patient. Using biometric only, the patient can be authenticated but the authenticity of the transferring device may be questioned. We therefore propose a novel authentication framework that binds them together for the said purpose. The authentication method comprised of biometric modalities and radio fingerprinting has not been investigated to date.

In order to incorporate the issues and concepts discussed earlier, Section II discusses authentication techniques using biometric and radio fingerprinting. Section III presents the proposed authentication framework. Related work is highlighted in section IV. Section V analyses our authentication framework. Section VI concludes the paper and addresses future work.

II. AUTHENTICATION TYPES

A. Biometric Techniques

Authentication is a necessary requirement in any information system to ensure the availability of information to authorized users only. The authentication mechanisms are developed using passwords, secret keys, tokens, and biometric features. The verification is performed based on credentials such as something we know (password, passphrase, personal identification number), something we have (tokens, cryptographic keys), something we are (physiological and behavioral characteristics such as fingerprints, face, iris, palm prints, voice, hand geometry, Deoxyribonucleic acid (DNA), Electrocardiography (ECG), keystroke dynamics, gait, and signature).

Authentication systems may require use of one of these factors (knowledge, possession, and inherence) when an entity presents evidence for its identity. A common solution to reduce the risk of an entity presenting false evidence is to use different factors in combination, yielding multi-factor authentication. Biometric authentication is considered much stronger when compared to password or token based authentication [5] because the biometric characteristics of every human are uniquely identifiable, non-transferable, and non-reproducible. Multi-factor authentication is considered stronger than single factor authentication. Authentication mechanisms can be divided into two categories: static and continuous authentication methods [6]. Static authentication mechanisms authenticate the user initially but do not monitor post authentication session to detect if it is the same user accessing the system [7]. However, some systems can use periodic static authentication as well for re-authentication using same static credentials. Continuous authentication methods monitor a system during the lifetime of a session to detect if it is the same user accessing the system [8].

Continuous authentication mechanisms are an obvious choice for the RPM scenario because they have the potential to answer the fundamental question of patient verification during the entire session of remote monitoring. We can also use more than one biometric trait or use static and continuous simultaneously to verify the patient and increase the trust level on the received data.

B. Radio Fingerprinting Technique

The radio fingerprinting technique uses the hardware properties of the wireless devices and their signal characteristics for the purpose of unique identification. The radio fingerprints are generated by analysing the properties of radio signal and are determined by extracting device specific features that are caused by hardware impairments. The radio fingerprints are extracted by analysing the received radio signal for specific properties such as frequency, amplitude, and phase [14] [15] [16]. Radio fingerprinting is comprised of pre-processing, detection, feature extraction, and classification processes phases [9]. The purpose of radio fingerprinting is to uniquely identify the transmitter independently of any identifier in the data payload that can be forged easily. Radio fingerprinting can be used to identify cellular phones or other wireless devices, and to prevent fraud and cell phone cloning [10] [11]. The successful identification of wireless devices can potentially allow other applications such as intrusion detection system and forensic data collection to use radio fingerprinting [12] [13].

Radio fingerprints allow us to compare and distinguish different wireless devices with each other [17] and can be used in an authentication mechanism similarly to human biometric authentication. The radio fingerprinting method is composed of enrolment and verification operations [18] [19] [20]. Radio fingerprinting can be used in message authentication because it helps against message replay attacks [16].

III. PROPOSED AUTHENTICATION FRAMEWORK

We assume a mobility scenario where the patient does not need to stay at static locations. Hence, the patient can be at various locations including (i) at home, nursing home, or office; (ii) at public places such as library, café, playing sports; (iii) in transport such as car, ambulance, bus, and train; (iv) hospital that includes waiting room, intensive care unit, and surgery room. The RPM scenario for the IoT in eHealth is depicted in Fig. 1. We base the mobility scenario on previous work [40].

We propose an authentication framework composed of three phases to ensure the correctness of patient's physiological characteristics, patient's device, and patient's behaviour on continuous basis. Note that medical sensor to smartphone authentication is an important issue that is not treated here.

 ISBN: 978-1-61208-363-6

We assume that the medical sensors are paired with the patient's smartphone earlier during an issuing procedure. Hence, the patient uses only such medical sensors that have already been paired with the smartphone. The pairing procedure can ensure that the smartphone only connects with pre-approved medical sensors. Beyond this, the three phases of authentication are:

- Patient to smartphone authentication
- Smartphone to network authentication
- Patient to remote medical server authentication

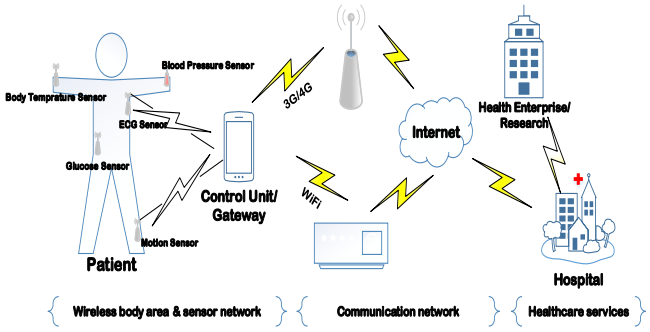

Figure1. Remote Patient Monitoring (RPM) Scenario

A. *Patient to smartphone authentication*

This phase ensures that the smartphone collects the data from a correct patient or the patient uses correct device to transfer medical data. We propose to use built-in sensors in the smartphone to authenticate the patient, e.g., smartphone biometric fingerprint identification sensors, face recognition using camera, voice recognition using microphone, and gait recognition using accelerometer. The authentication process for this step is depicted in Fig. 2.

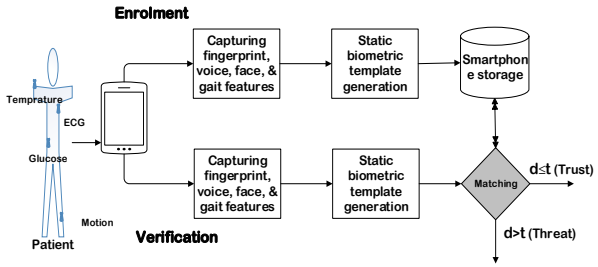

Figure 2. Patient to smartphone authentication process

The patient to smartphone authentication phase based on static biometric is composed of enrolment and verification processes. During the enrolment process patient's fingerprints, voice, face, or gait features are extracted to create a biometric template that is stored in smartphone for future comparison. Later on, the template is used for authentication. During the verification process, the patient's biometric characteristics are captured and verified against the stored template. A distance *d* indicates the tolerance of variation for the matching. The predefined trust threshold *t* indicates the limit for accepting or rejecting the authentication. If ($d \leq t$) the patient is authenticated and trust is established. Otherwise ($d > t$) the user will be required to try again. Repeated failures will be treated as a possible threat. In an adaptive security setting [41], the trust threshold *t* might be varied dynamically depending on the current user environment and risk level.

B. *Smartphone to network authentication*

We propose this authentication phase to incorporate the idea of using an authenticated device. The process is depicted in Fig. 3.

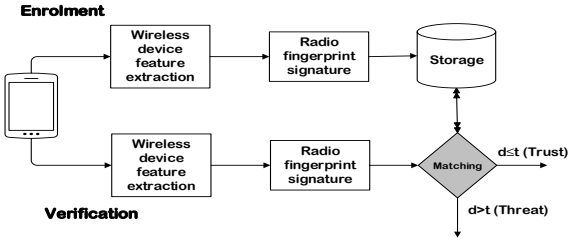

Figure 3. Smartphone to network authentication process

The device to network authentication phase based on radio fingerprints is comprised of enrolment and verification. The device specific features are extracted in the enrolment process to create the radio fingerprint of smartphone. The signatures are stored at wireless access point and mobile operator end for future comparison. Later on, when smartphone wants to access the medical server, first the radio fingerprint is checked at the access point or at the mobile operator end. A match will allow the connection but the request will be blocked on a mismatch. Our solution assumes that the access point and mobile operator network are configured to only let through traffic from matching devices. Note that the mobile network operators do not provide such service to date.

C. *Patient to remote medical server authentication*

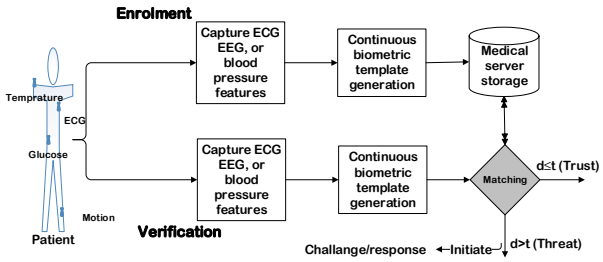

Figure 4. Patient to medical server authentication process

The process for continuous biometric authentication consists of enrolment and verification as depicted in Fig. 4.

During the enrolment process the patient's ECG, or blood pressure features are extracted to create a biometric template that is stored at medical server for future comparison. Later on, the template is used for authentication. During the authentication process, the patient's biometric char-

acteristics are captured and verified against the stored template. If the comparison verifies the patient based on matching score, then the patient is authenticated and trust is established. Otherwise in case of a non-match, the server will keep receiving data marked with reduced trust level.

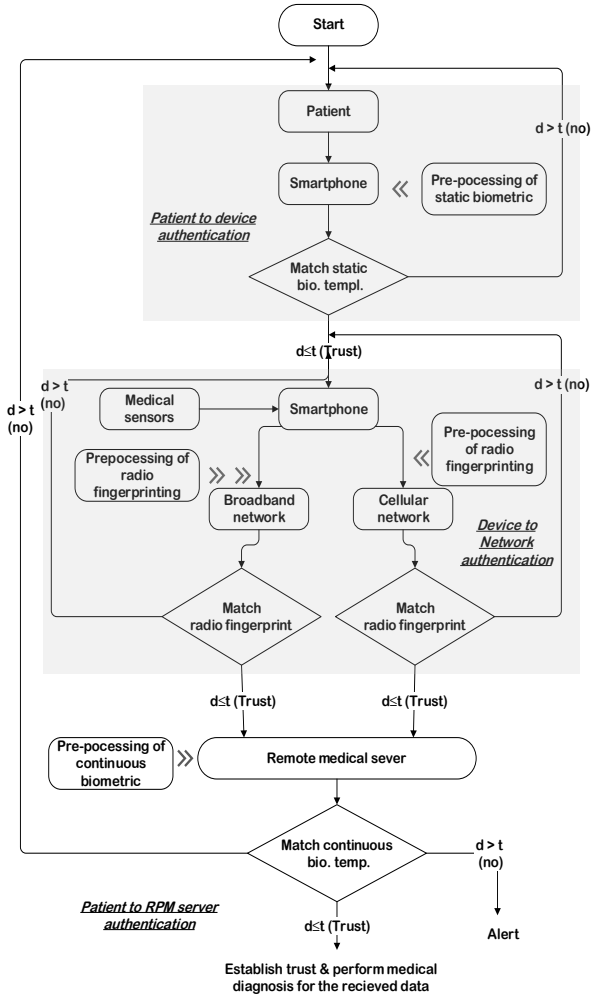

Figure 5. Authentication framework

As mentioned earlier, the overall authentication framework is composed of three phases depicted in Fig. 5. The three phases are combined to provide the required level of authentication. At first, the preprocessing of the static biometric template is performed and the signature is stored in the smartphone. The patient to device authentication phase ensures that the correct patient access the smartphone. The process is repeated when non-match occurs, otherwise patient is verified as a genuine user when match occurs and the next phase—device to network authentication—starts. Once the patient has been authenticated, the smartphone starts to collect data. Based on the patient's current location, either a wireless access point or the mobile network operator first verifies smartphone fingerprint signature against preprocessed stored template. The patient's data is forwarded to the medical server when the template is matched, otherwise the phase is repeated. During the next phase—patient to medical server authentication—apart from medical diagnosis the received data is used for feature extraction to create template that is matched against a preprocessed stored template. If the templates match the patient's data it is used for medical diagnosis, otherwise either the overall process is repeated or an alert is generated to initiate a response mechanism from medical staff. Table 1 summarises the phases of the authentication framework. The marks indicate the locations involved in the corresponding phases.

TABLE 1. AUTHENTICATION FRAMEWORK PHASES

	Locations			
Authentication type	**Patient**	**Smartphone**	**Network**	**Medical server**
Static biometric	✓	✓		
Radio fingerprint		✓	✓	
Cont. biometric	✓			✓

IV. RELATED WORK

The proposed authentication framework integrates static biometric, wireless device fingerprinting, and continuous biometric to provide an overall authentication solution. In this section, we briefly present related work to show that research in these domains is promising and that it is viable to these mechanisms for identification and verification in our scenario.

Biometric modalities such as voice, face, and fingerprinting recognition are emerging as an alternative authentication choice for smartphone users [21]. Also, some researchers have developed algorithms for voice and face recognition on mobile phones [22] [23]. Mobile phones with biometric fingerprint identification capability are already available in the commercial market.

The viability of authentication using wireless device fingerprinting has been proposed and demonstrated by some authors in different settings such as distributed ad hoc networks [24], infrastructure type networks [12] [25], and sensor networks [16]. A recent Internet draft [26] discusses the scope of radio fingerprinting for wireless device authentication. The identification for source of transmission by cellular operators has been addressed in the literature [16] [27]. Ureten et al. [9] demonstrated the use of radio fingerprinting to enhance the security of the 802.11 standard communications. Moreover, identifying wireless devices through fingerprinting technique has been published by various authors such as identifying unique devices through wireless fingerprinting [28], using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks [29], secure authentication in wireless networks using RF fingerprints [30], forensic identification of GSM mobile phones [14], practical RF fingerprints for wireless sensor network authentication [31], and AGC-based RF fingerprints in wireless sensor networks for authentication [32].

Patient authentication using ECG in biometric recognition has been presented in many recent studies [33] [34] [1]. The authors not only demonstrated the ECG data collection while the patient is at rest but also during the different activities phases. The RPM system utilizing sensors such as ECG, Electroencephalography (EEG), and Electromyogra-

phy (EMG) attached to a patient's body, aiming to collect signals and then transferring them to a remote medical server is also explained in the literature [35] [2]. The use of a patient's physiological or behavioural characteristics in body area sensors network to solve identification and verification problem [4], physiological biometric for continuous authentication in ubiquitous environment [36] [5], and physiological characteristics of the patient for identity recognition have also been published in the literature [37] [38].

V. DISCUSSION

Some characteristics of the devices in the IoT environment are resource constraints, heterogeneity, distributed environment, uncertainty, context and location awareness, and ubiquity. In this section, we analyse our proposed mechanism in the context of these characteristics.

A. Resource constraints

Resource constraints such as limited power in sensor nodes are an important factor in the RPM system. Increased activity beyond the necessary collection and transmission of patient's data may drain the power of sensor nodes. An authentication mechanism for such environment should not consume significantly more resources than what is already the case. The proposed mechanism impose only minor extra processing burden on devices during different phases of authentication. For instance, patient to device authentication using static biometric requires only the patient's physical characteristics template to be locally stored at smartphone consuming little storage. Similarly, device to network authentication requires the wireless device fingerprint template to be stored either at the wireless access point or at the mobile network operator consuming no storage at the device. Patient to remote medical server authentication utilise the continuous biometric technique where the matching template is stored at the server end. The received data is used at the hospital site to authenticate the patient without requiring sensors to do any extra processing. Thus, devices with limited energy are not required to perform any extra processing. The framework does not impose any extra burden in terms of storage, processing, and power. In fact, the patient's own physiological and behavioural characteristics, the device specific characteristics, and the monitored data that is to be collected anyhow serve the authentication purpose.

B. Distributed/heterogeneous/dynamic environment

The devices in the IoT imply a distributed environment. As discussed in the scenario, the patient may be present at various locations but medical sensors can still send data to the medical server. We propose to use wireless device fingerprinting for broadband and cellular network infrastructures. Therefore, our framework is usable in such environments.

C. Context and location awareness

The proposed framework uses patient's behavioural characteristics for continuous biometric authentication. The patient behaviour can change when he is suffering from a heart attack. While authenticating a patient during a heart attack, the biometrically received data will not match the stored template. The non-match will trigger an alarm at the medical server requiring a response. For example, the response may include calling the patient on the smartphone, where in case of no answer an ambulance will be dispatched. In this case, radio device fingerprinting can serve another useful purpose. Since there can be uncertainty about the patient's current location, the device fingerprints and location service at that point of time can help in locating the patient.

D. Security

We analyse the security of our proposed framework from availability, integrity, and confidentiality aspects. The biometric and radio fingerprints templates are vulnerable to theft. At first, the patient can always report immediately for such an instance. However, if the imposter uses the stolen device for sending data to the medical server, while the patient to device authentication and device to network authentication may succeed, the continuous biometric authentication template will not match. The non-match will trigger an alarm at the medical server implicating that either it is an imposter or the patient is suffering from an attack. The authentication mechanism triggers an alarm that requires response by medical staff. Also, if someone gets access to the biometric templates and tries to use them for sending fabricated data to the medical server, then the imposter will not be able to compromise the system because biometric features of every human are unique and non-transferable. During the transfer of data to the medical server there is a risk of data interception which may impact the patient's privacy and confidentiality. We recommend using lightweight cryptography to prevent clear text data transmission to the medical server.

VI. CONCLUSION & FUTURE WORK

Our proposed authentication framework comprised of three phases ensures that the received data at remote medical server belongs to correct patient and identifies the fabricated data. The framework is resource and energy efficient requiring no extra processing for authentication purpose except the initial pre-processing of biometric and radio fingerprinting templates. While suffering from a heart attack or other extraordinary medical condition during the remote monitoring session, the patient's location can be determined using smartphone radio fingerprints.

In future, we want to evolve our framework towards adaptive and context aware authentication mechanism. The framework will be validated using simulation scenarios [40]. Incorporating context awareness and adaptive security in our framework are challenges because a non-match between stored and given templates always can not be treated as a threat to the system, rather there can be situations where environmental or system's context can assist us in decision making. Adaptive security can make template matching more flexible and we can adjust security level instead of blocking transmission during no-match due to the changed context. Thus, we will develop models of context awareness and adaptive security for our proposed authentication framework.

 ISBN: 978-1-61208-363-6

ACKNOWLEDGMENT

The work presented here has been carried out in the research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway.

REFERENCES

[1] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ECG-based patient authentication for remote health monitoring," ICMI-MLMI '09, ACM, 2009, pp. 297-304.
[2] Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," Wireless Communications, IEEE vol. 17, no.1, February. 2010, pp. 59-65.
[3] S. Bao, Y. Zhang, and L. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," IEEE-EMBS'05, 2005, pp. 2455-2458.
[4] M. A. Chowdhury, J. Light, and W. McIver, "A framework for continuous authentication in ubiquitous environments," WCSN'10, 2010, pp. 15-19.
[5] H. Saevanee, N. Clarke, and S. Furnell, "Multi-modal behavioural biometric authentication for mobile devices," Springer Berlin Heidelberg, 2012, pp. 465-474.
[6] E. Alsolami, "An examination of keystroke dynamic for continuous authentication", PhD thesis, Queensland University of Technology, 2012.
[7] J. Liu, F. R. Yu, C. Lung, and H. Tang, "Optimal combined intrusion detection and biometric based continuous authentication in high security mobile ad hoc networks," IEEE Transactions 8(2), February. 2009, pp. 806-815.
[8] R. H. C. Yap, T. Sim, G. X. Y. Kwang, and R. Ramnath, "Physical access protection using continuous authentication," In technologies for homeland security, IEEE conference, 2008, pp.510-512.
[9] O. Ureten, and N. Serinken,"Wireless security through RF fingerprinting," Can.J. of el. & com. eng., vol.32(1), 2007, pp.27-33.
[10] M. B. Frederick, "Cellular telephone anti-fraud system," google patent, 1995.
[11] K. D. Hawkes, "Transient analysis system for characterizing RF transmitters by analysing transmitted RF signals," google patent, 1998.
[12] I. O. Kennedy et al., "Radio transmitter fingerprinting: A Steady State Frequency Domain Approach," VTC, 2008, pp.21-24.
[13] R. Gerdes, T. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting," A matched filter approach, NDSS'06, 2006, pp. 1-11.
[14] J. Hasse, T. Gloe, and M. Beck, "Forensic identification of GSM mobile phones," IH&MMSec '13, 2013, pp.131-140.
[15] K. B. Rasmussen, and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," SecureComm'07, 2007, pp. 331-340.
[16] V. Brik, S. Banerjee, and M. Gruteser, "Wireless device identification with radiometric signatures," MobiCom, 2008, pp. 14-19.
[17] D. A. Knox, and T. Kunz, "RF fingerprints for secure authentication in single-hop WSN," WIMOB '08, 2008, pp. 567-573.
[18] S. Banerjee, and V. Brik (Ed.), "Wireless device fingerprinting," Encyclopedia of Cryptography and Security, Springer-Verlag Berlin Heidelberg, 2011.
[19] K. L. Talbot, P. R. Duley, and M. H. Hyatt, "Specific emitter identification and verification," Technology review journal, 2003, pp. 113-133.
[20] P. Tuyls, and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems," Lecture notes in computer science, Springer, Berlin, 2004, pp 158-170.
[21] S. Trewin et al., "Biometric authentication on a mobile device: a study of user effort, error and task disruption," ACSAC '12, 2012, pp. 159-168.
[22] Y. Ijiri, M. Sakuragi, and S. Lao, "Security management for mobile devices by face recognition," MDM'06, 2006, pp.49-49.
[23] S. Kurkovsky, T. Carpenter, and C. MacDonald, "Experiments with simple iris recognition for mobile phones," ITNG'10, 2010, pp, 1293-1294.
[24] K. Hoeper, and G. Gong, "Pre-authentication and authentication models in ad hoc networks", Wireless Network Security, Part II, Springer Verlag, December. 2006, pp. 65-82.
[25] J. Hall, M. Barbeau, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," MADNES, Springer-Verlag LNCS, Vol. 4074, 2006, pp. 80-95.
[26] J. Yu, and H. Jie, "RF fingerprint authentication of wireless device," Internet Draft, December 19, 2013.
[27] H. Mustafa, M. Doroslovacki, and H. Deng, "Automatic radio station detection by clustering power spectrum components", ICASSP'02, volume 4, IEEE, May 2002, pp.4168-4168.
[28] L. Chin, C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying unique devices through wireless fingerprinting", WiSec '08, 2008, pp.46-55.
[29] B. Sieka, "Using radio device fingerprinting for the detection of impersonation and Sybil attacks in wireless networks," security and privacy in ad-hoc and sensor networks, Springer Berlin Heidelberg, Vol. 4357, 2006, pp. 179-192.
[30] D. A. Knox, and T. Kunz, "Secure authentication in wireless sensor networks using RFfingerprints,"EUC'08, 2008, pp.230-237.
[31] D. A. Knox and T. Kunz, "Practical RF fingerprints for Wireless Sensor Network authentication," IWCMC, 2012, pp.531-536.
[32] D. A. Knox, and T. Kunz, "AGC-based RF fingerprints in wireless sensor networks for authentication," WoWMoM'10, 2010, pp.1- 6.
[33] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," EURASIP'08, 2008, pp. 1–6.
[34] C. Chiu, C. Chuang, and C. Hsu, "A novel personal identity verification approach using a discrete wavelet transform of the ECG signals," MUE'08, 2008, pp.201–206.
[35] E. Monton et al., "Body area network for wireless patient monitoring," Communication, IET, vol.2, no.2, February. 2008, pp. 215–22.
[36] T. G. Roosta, "Attacks and defenses of ubiquitous sensor networks," PhD thesis, University of California, Berkeley, 2008.
[37] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," Pattern Recognition, science direct, Vol. 38 (1), 2005, pp. 133-142.
[38] M. Guennoun, N. Abbad, J. Talom, M. Rahman, and K. El-Khatib, "Continuous authentication by electrocardiogram data," TIC-STH'09, 2009, pp. 40-42.
[39] W. Leister, and T. Schulz, "Ideas for a trust indicator in the Internet of Things", SMART' 12, 2012, pp. 31-34.
[40] W. Leister, M. Hamdi, H. Abie, and S. Polsad, "An evaluation scenario for adaptive security in eHealth", PESARO'14, 2014, pp. 6-11.
[41] H. Abie, and I. Balasingham. "Risk-based adaptive security for smart IoT in eHealth," BodyNets '12, 2012, pp 269-275.
[42] Y. Berhanu, H.Abie, and M. Hamdi "A testbed for adaptive security for IoT in eHealth", ASPI '13, 2013, pp. 1-8.

 ISBN: 978-1-61208-363-6