Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth

Mattias T. Gebrie
Department of Control and Computer Engineering
Corso Duca degli Abruzzi 34
10138 Torino
Italy
atomattias@gmail.com

Habtamu Abie
Norwegian Computing Center
P.O.Box 114 Blindern
NO-0314 Oslo
Norway
habtamu.abie@nr.no

ABSTRACT

Health care is one of the primary beneficiaries of the technological revolution created by Internet of Things (IoT). In the implementation of health care with IoT, wireless body area network (WBAN) is a suitable communication tool. That being the case security has been one of the major concerns to efficiently utilize the services of WBAN. The diverse nature of the technologies involved in WBAN, the broadcast nature of wireless networks, and the existence of resource constrained devices are the main challenges to implement heavy security protocols for WBAN. In this paper we develop a risk-based adaptive authentication mechanism which continuously monitors the channel characteristics variation, analyzes a potential risk using naive Bayes machine learning algorithm and performs adaptation of the authentication solution. Our solution validates both the authenticity of the user and the device. In addition we evaluate the resource need of the selected authentication solution and provide an offloading functionality in case of scarce resource to perform the selected protocol. The approach is novel because it defines the whole adaptation process and methods required in each phase of the adaptation. The paper also briefly describes the evaluation case study - Smart Home eHealth.

CCS CONCEPTS

• **Security and privacy → Network security → Mobile and wireless security**;

KEYWORDS

Risk-based, Adaptive authentication, WBAN, Machine learning, IoT, Smart home, eHealth

ACM Reference format:
G. Mattias and H. Abie. 2017. Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth. In *Proceedings of ECSA'17*, September 11–15, 2017, Canterbury, United Kingdom, 7 pages.
https://doi.org/10.1145/3129790.3129801

ECSA '17, September 11–15, 2017, Canterbury, United Kingdom

ACM ISBN 978-1-4503-5217-8/17/09…$15.00
https://doi.org/10.1145/3129790.3129801

1 INTRODUCTION

The future Smart Homes are expected to deliver many kinds of services of which health care is one of these services. Integration of health care system into a Smart Home will enable the provision of high quality, low cost and easily accessible care to the ever increasing population of the world particularly the elderly suffering from age related diseases [1]. One way to implement health care system in Smart Home is the use of wearable sensor nodes, actuators nodes and wireless communication technologies, which is referred to as wireless body area network (WBAN). A WBAN is a collection of low-power and lightweight wireless sensor nodes, with limited computation, communication and storage capacity [2]. Keeping WBAN and its supporting infrastructure safe and sound is a challenging task. In heterogeneous, dynamic and interconnected environment such as the Smart Home, the resident is exposed to privacy and security risks as personal information becomes remotely accessible in a new way.

Thus implementing a security protocol needs to address varies resource capacity of the nodes in the network. Moreover, the fact that the devices involved in the network are unattended and communicates wirelessly create a large attack surface. Thus, stringent and scalable security mechanisms are required to prevent malicious interactions with the WBAN system [3].

One way of maintaining the integrity and security of such a network is authentication. It is a means to identify and verify a device or a user who it claims to be. Existing conventional high-level authentication mechanisms can only monitor a particular infrastructure unit and safeguard a particular service. These kinds of authentication solutions are platform specific and cannot protect a system against ever-changing attacks, and don't take into account the nature of constrained resources and dynamic networks. These challenges demand a risk aware and an adaptive authentication solution that is able to change and modify its authentication protocols autonomously on the fly. In addition the authentication solution must also consider the fact that the devices in the network maybe resource constrained to perform a heavy authentication task.

In an effort to overcome some of the aforementioned challenges a lot of researches have been done over the past few years on authentication solutions. Researches in [4-9] generally focused on IoT in Smart Home authentication and in [10-20] particularly focused on WSN and WBAN. While most of the researches focused on how an authentication solution efficiently utilize the limited resource on

constrained networks [5,8,16,20-24], some tried to consider authentication in dynamic environments [8,19]. Few researches begun to consider adaptation of the authentication protocol based on the context of the system [12,25]. Researchers in [26-31] attempted to measure risk in user activity and authenticate accordingly but failed to address the natures of resource constrained and dynamic network such as WBAN.

In response to the preceding challenges, we propose a novel risk based adaptive authentication method for WBAN in Smart Home eHealth environment. The method involves continuously monitoring and analyzing the user and devices activities and selecting its authentication/re-authentication protocols based on the security risk involved. It further compares the selected authentication protocols' resource need with the available resource of the authenticating device to decide to offload or not the authentication process.

The rest of the paper is structured as follows. Section 2 discusses the background and state of the art. Section 3 presents the proposed risk-based adaptive authentication framework. Section 4 describes the validation case study, and finally, Section 5 offers conclusions and future work.

2 BACKGROUND AND STATE OF THE ART

In this section, we discuss background concepts on adaptive authentication and risk based authentication, a review of related work on authentication solutions for constrained network and a brief state of the art in naïve Bayesian network.

2.1 Authentication

The authentication problem is simple to describe but hard to solve. Two parties are communicating, and one or both wish to establish their identity to the other. Authentication is thus the process of verifying the physical identity of a person, i.e. user authentication and the digital identity of a process/computer. Authentication is the gatekeeper for other security tasks such as confidentiality–restricting data access to authorized persons, integrity–ensuring data modification by authorized persons, non-repudiation–conclusively tracing an action to an individual and availability–ensuring availability of data to authorized persons. Thus user authentication is a central component of any security infrastructure. Users can be authenticated in many different ways, by using something a user knows, something a user has, something a user is, something a user does, where a user is, and combinations of any of these as illustrated in Table 1.

Table 1: Authentication Types

Authentication	*Types*
Something you know	*Password, PIN, Personal number, Phone number, date of birth, etc.*
Something you have	*Tokens, Smartcards, Bank Card, Passport, Driving license, etc.*
Something you are	*Biometrics: Physiological biometrics such as fingerprint, facial recognition, iris-scan, hand geometry, retina scan, etc., and Behavioral biometrics such as voice recognition, keystroke-scan, signature-scan, gaits, etc.*
Something you do	*User behaviors patterns, bank transactions, travelling, calls, social media logs, etc.*
Combinations	*Any combinations of the above (aka multifactor authentication, e.g. PIN-enabled bank card)*

As the last factor indicates for each of these authentication types a lot of solutions have been developed with varying factors, single factor (e.g. user name and password) to multi-factor (using two or more distinct and different types of authentication mechanisms). The focus of this study is to adapt authentication mechanisms dynamically according to contextual changes in order to increase the flexibility of authentication and level of security.

2.2 Adaptive Authentication

Adaptive security is a security model that changes its behavior autonomously by monitoring and regulating the situations or changes under observation to safeguarding systems against threats over a network. There exists a body of work on adaptive security for IoT in eHealth. In [36] a risk-based adaptive security framework for IoTs in eHealth has been presented, which estimates and predicts risk damages and future benefits using game theory and context-awareness techniques. Savola et al. [33] analyzed security objectives of eHealth IoT applications and their adaptive security decision-making needs, and proposed a high-level adaptive security management mechanism based on security metrics to cope with the challenges. Following this, on one hand Savola and Abie [34] argue that adaptive security solutions need security metrics to be able to adapt the relevant security parameters according to contextual and threat changes, which are typical for patient-centric IoT solutions. The authors developed a context-aware Markov game theoretic model for measurably evaluating and validating the run-time adaptivity of IoT security solutions. On the other hand, Torjusen et al. [35] argue that the integration of run-time enablers into an adaptive security framework could lead to a sustainable security framework for IoT in eHealth. A brief survey and comparison of adaptive security with their special features and benefits categorized according to their types of adaptation can be found in [32].

The main focus of this paper is specifically on adaptive authentication. Adaptive authentication refers to an authentication solution that continuously monitors and analyzes the changing environment and adapts its solution dynamical based on system requirement to thwart a system against unknown threats [36,37]. In a static authentication a system user provides identity and gives proof of this identity when first accessing a service and will be valid throughout the full session whereas an adaptive authentication takes a different view from this conventional authentication mechanism. Instead of locking the door and hoping for the best, it focuses on observing for threats and attacks and reacting to them dynamically head-on.

2.3 Risk-based Authentication

Risk-based authentication uses contextual and historical information to calculate the risk score associated with the user's current activity. The risk score is calculated on real time basis according to a set of rules that can be used to make authentication decisions. The overall goal of risk-based authentication is to gather available information from the user environment, compare it with a known user profile, and

determine if that user needs to step through an additional identification process. In [28] Hintze et al. consider geographical location as authentication factor to evaluate the risk and to make authentication decision for mobile devices. Their method uses location-based risk in combination with multi-modal biometrics to adjust the level of authentication necessary to a risk situation. Adam and Hurkala [29] proposed a context risk aware authentication. They used user IP address, time of access, device cookie, device profiling and number of failed authentication attempts to study the risk related to the user identity. Traore et al. [27] proposed a Bayesian network model for analyzing and evaluating the keystroke and free mouse movement of user's to calculate the risk in web sessions. Researches in [30,31] considered the evaluation of fingerprint movement for learning the behavior of the smartphone user. However, to the best of our knowledge, none of the work published so far has taken into account the evaluation of risk in a resource constrained network such as the WBAN. In this study, we use the resource constrained devices in WBAN and the dynamic network environment of Smart Home in designing risk-based adaptive authentication solution. The channel characteristics variations among the communicating devices are used to uniquely identify devices validity. The validation of the devices is based on the naïve Bayes network.

2.4 Authentication Mechanisms Review and Comparison

In this section we present a brief overview authentication mechanism and the evaluation of some of user/devices authentication methods proposed in the literature. We evaluate each method based on its resources use (energy, memory, computation and communication) efficiently, and/or adapt its method to the available resource and risk as illustrated in Table 2.

In [15], the reduction of memory overhead, computational overhead and network transmission overhead has been claimed. In [15] a delegation architecture that offloads the expensive Data Transport Layer Security (DTLS) handshake when employing public-key cryptography for peer authentication and key agreement purpose, proposed. In [38], biometric-based user authentication mechanism for wireless sensor networks proposed, which uses one-way hash function and symmetric secret session key shared between the user and a sensor node so that the secret session can be used latter. Caparra et al. [25] proposed authentication process with anchor node involvement in the authentication process to estimate the channel of the source node to concentrator node. The solution is energy aware. It considers the energy level of the anchor before letting them involve in the authentication process.

Spooren et al. [39] proposed authentication adaptation that continuously monitors the battery charge level of the device and keep track of how battery charges are distributed throughout the day to check the authenticity of the device. Han et al. [8] proposed node authentication and key exchange protocol for Smart Home Environment that supports the dynamic nature of the Sensor node by introducing a concept known as Neighbor sink link that helps store the neighbor identity detail in order to reduce computation and communication overhead. Nan et al. [17] used the RSSI signal variation between communicating nodes and user physiological pattern to solve authentication problem which as they claimed, resulted in a prolonged battery life of the WBAN sensors. Hamdi and Abie [40] proposed a novel game-based adaptive security model for IoT in eHealth, which uses energy consumption, channel bandwidth, memory capacity, and nearby node intrusion to determine whether or not to authenticate the sender node. The model uses the trade-off between security effectiveness and energy-efficiency to evaluate adaptive authentication strategies. A comprehensive survey of authentication protocols for IoT under 4 environments, machine-to-machine communications (M2M), Internet of Vehicles (IoV), Internet of Energy (IoE), and Internet of Sensors (IoS) can be found in [41]. Table 2 compares closely relevant authentication solutions

Table 2: Comparison of Authentication Solutions

Ref	Energy		Memory		Computation		Communication	Risk aware
	Battery efficiency	Battery level adaptation	Memory efficiency	Memory size adaptation	Overhead	Overhead adaptation	Overhead optimization	Adaptation
[15, 38]			X		X		X	
[40]		X		X			X	
[25, 39]		X						
[8]					X		X	
[17, 20, 42]	X							
[11, 14]			X		X			
[43]	X		X					
[27-31]								X

2.5 Channel Characteristics

There is a wide array of information that is available to be considered when evaluating the validity of devices and users in authentication. For the purpose of this study, channel characteristics variation between the sensor nodes and the gateway of the WBAN are the preferred means to validate devices identity. That is because channel characteristics in WBAN exhibit unique properties according to the movement of the user, the posture of the user, surrounding environment, the position of the antennas and the location of the node [17,44-46]. Yin et al. [53] have demonstrated that the accuracy of the measurement and thus the identification probability can be maintained above 98%, which is sufficient for this purpose since it is not possible to achieve 100% security.

In the Smart Home scenario of WBAN communications, signal propagation can experience fading due to different reasons, such as energy absorption, reflection, diffraction, shadowing by body, multipath due to the environment around the body and body posture.

The channel characteristics variation between communicating devices can be obtained by studying the property of the signal travelling from the transmitter node to the receiver node. We have identified RSSI (Received signal strength indicator), Channel gain, Temporal link

signature, and Doppler measurement as means to model the channel characteristics variation exhibited due to the unique environmental setup of the Smart Home and the unique physiological pattern of mobility of the user wearing the sensor nodes.

Received signal strength indicator (RSSI): is an indication of the power level being received by a client device in a wireless environment. RSSI is often expressed in decibels (db), or as percentage values between 1 up to 100, and can be either a negative, or a positive value. In [17,47-49] RSSI variation is analyzed to assist authentication solution.

Channel gain: When a radio signal is transmitted from a transmitter to a receiver, the different carrier waves experience different gains in the wireless channel due to the multipath characteristics. A vector of these channel gains can serve as a link signature which can be used to verify the authenticity of a transmitter [50].

Temporal link signature: A radio signal from a transmitter to a receiver takes many paths and each path has a different length. A wave propagating as such takes a different amount of time to arrive at the receiver resulting to a unique temporal link signature. Patrawi [51] proposed the use of channel impulse response generated temporal link signature for each device in the wireless channel to uniquely identify the link between a transmitter and a receiver. The author argues that temporal link signature is useful for efficient location estimation in WSN, physical security for managing objects, and prevention of impersonation in wireless networks.

Doppler measurements: Doppler is the frequency shift caused by the velocity of a transmitter. It involves in measuring the carrier frequency deviation of the moving emitter, in order to calculate its velocity. Doppler measurements, detect motion while the device is moving [52].

2.6 Naïve Bayes

The Bayesian Classification represents a supervised probabilistic learning method as well as a statistical method for classification. It calculates explicit probabilities for hypothesis and it is robust to noise in input data. The probabilities of an event A may well depend on the previous or simultaneous occurrence of an event B and A is said to be conditioned on B. The basic idea of Bayes rule is that the outcome of an event A can be predicted based on some evidences (x) that can be observed. A Naïve Bayes Classifier is a simple probabilistic statistical classifier based on applying Bayes probability theorem. Bayes theorem can be described as follows:

$$Posterior\ probability(c/x) = \frac{Class\ prior\ probability(c) * likelihood(x/c)}{evidence(x)}$$

The posterior probability, in the context of a classification problem can be interpreted as what is the probability that a particular object belongs to class C given its observed feature values?

The naïve Bayesian algorithms used for training the model and to make classification is implemented using Rapid Miner software suite, to collect results of the classification and for further processing another application has been developed that uses Rapid Miner API.

3 ARCHITECTURE OF RISK BASED ADAPTIVE AUTHENTICATION

In this chapter, we propose the overall design of risk-based adaptive authentication architecture as depicted in Fig. 1. After describing Bootstrapping process of the network, the section describes the main components of the framework, monitor, analyze and adapt in detail.

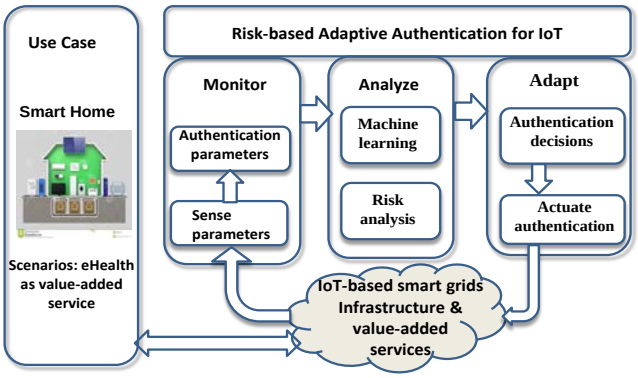

Figure 1: Risk-based adaptive authentication model for IoT

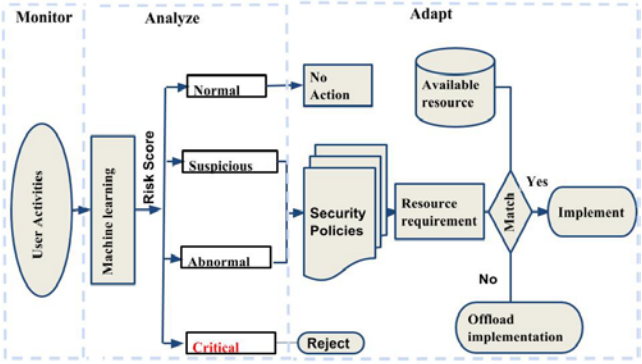

Figure 2: Detailed architecture diagram with offloading

3.1 Bootstrapping of the Network

In this phase, we register patterns on channel characteristics of devices and behavior of users to train the Bayesian network. During training, the probability of each class is computed by counting how many times it occurs in the training dataset. This is called the prior probability. The bootstrap process is described as follows.

1. RSSI, Channel gain, Temporal link signature, and Doppler measurements between each sensor node and the gateway are used to register the position of the node and behavioral patterns of the user. For each attribute, since all the features are continuous we define a range of values and compute the probability of each range.

2. A naïve Bayes classification algorithm is applied on the registered pattern to build a knowledge base for each sensor node. Sleeping, Walking, Sitting, and Eating are the selected daily routines that are used as a target class to classify the features selected in step 1. A signal value out of the range of a known value is classified as Unknown. During training, the probability of each class is computed by counting how many times it occurs in the training dataset. From the training data we populate the frequency of occurrence of each feature and calculate the likelihood probability value using Table 3.

Table 3: Feature Frequency

Target class	Feature				Total Probability
	[Range 1] frequency	[Range 2] frequency	[Range 3] frequency	[Range 4] frequency	
Walking					
Sitting					
Eating					
Sleeping					
Unidentified					
Total Probability					

3.2 Monitor

The monitor phase gathers information from the connected sensor nodes. It uses a continuous cycle to monitor activities of a user and the device channel characteristics thereof, which are then utilized to reveal an adaptation need. These collected input signals are filtered and relevant set of channel characteristics; the same as listed in the bootstrapping stage are selected. These selected features are used as parameters to build user behavioral patterns. Later at the analyze stage the pattern generated in this stage will be compared with historical patterns of the corresponding device to see if any deviation exists.

3.3 Analyze

The analyze module computes the monitored features and evaluate a security risk in that particular instance. Privacy and security risks such as risk associated with a log-in attempt, loss of data, hacking, impersonation, eavesdropping, extraction of data, patient endangerment, etc. can be analyzed.

The naïve Bayes machine learning algorithm is once again used to evaluate the changes in the individual device/user characteristics given the knowledge base build in the bootstrapping stage. The result of the evaluation is a classification of the user activity and a probability score related to the classification. The probability score is used to indicate if there is a security risk and identify the level of the risk.

Once the risk level is established, decision will be made on to choose which authentication method is suitable. We use a naïve Bayesian network classifier to classify the user pattern related to a particular device. The classes used to classify those collected features are the same classes used in bootstrapping stage 2.

3.4 Adapt

The Adapt model plans how to adapt to the authentication level for the observed risk. It is a decision whether to elevate the authentication level and to select the suitable authentication protocol for the selected authentication level. If the risk score of a given user behavioral pattern exceeds normal risk threshold, authentication level is automatically elevated and the user/device maybe required going through a higher level of authentication method. Each of the method is assigned authentication strength. The initial authentication strength for a user is zero. Each time the user/device performs some activity its activity will be classified and a risk level assigned to it. This may rank through Normal, Suspicious, Abnormal and Critical. Authentication decision is performed according to the risk levels as depicted in Table 4.

If the risk level is Normal no action is needed, if the risk level is abnormal a node is requested to authenticate again, if the risk level is suspicious a node is held in Time out and requested to re-authenticate with one of the higher level of authentication types listed in Table 1, Section 2.1 such as PIN or token, and finally if the risk level is critical the user/device is rejected.

Table 4: Risk Level and Related Security Policy

Risk Level	Authentication Decision			
	Level 1	Level 2	Level 3	Level 4
Normal	No Action			
Suspicious		Re-authentication		
Abnormal			Time out and Re-Authentication	
Critical				Reject

The last step in the adaptation stage is the implementation of the authentication decision. However, before executing the selected authentication protocol the system must compare the resource need of the authentication protocol with the available resource of the device performing the client authentication task. In a situation where the device implementing the authentication protocol is a resource constrained to perform the authentication task, the system will search for a node with available resource to perform the task (offloading) as depicted in Fig. 2.

4 CASE STUDY: eHEALTH IN SMART HOME

The term “Smart Home” is generally used to refer to a home equipped with electronically controlled devices with security and convenience. These wide arrays of devices are interconnected to form a network, which can communicate with each other and with the user to provide service and create an interactive space. One of the services in Smart Home is eHealth and WBAN is one of the means to provide health

services in Smart Home. Health monitoring system in Smart Home is depicted in Fig. 3.

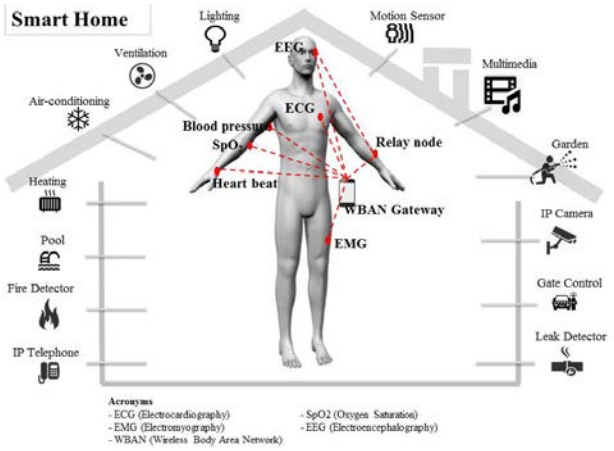

Figure 3: eHelath in Smart Home

A WBAN system contains a set of physiological and environmental monitoring sensor nodes. These sensors are capable of collecting body vital signs and contextual information at a certain interval and send them to concentrator node for further processing. In this paper we assume that all sensors in WBAN can send data through wireless channel.

At the physical and network layer, devices in WBAN will typically organize in a star topology where each node directly communicates with a network hub. This is the traditional approach in most WBANs, with the network hub being a dedicated network controller or, more recently, a smartphone. The hub will also act as the gateway for accessing external services (i.e., the Internet, other devices inside the smart home or device in proximity of the WBAN).

All Sensor nodes in WBAN system needs to get authenticated in order to establish a communication channel with the gateway. In this paper the focus is the authentication of sensor node to the gateway. In this case study, and as mentioned earlier, the risk associated with a log-in attempt, loss of data, hacking, impersonation, eavesdropping, extraction of data, patient endangerment, etc. will be analyzed.

5 CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a novel risk-based adaptive authentication model for IoT in Smart Home eHealth to identify the activities of the user and to verify the validity of the sensor nodes. The model uses a naïve Bayes machine learning algorithm to classify the channel characteristics variation between sensor nodes and their gateway. According to the observed variation of channel characteristics, the model assess the risk to determine the probability of the device in question being compromised, Based on the risk score obtained from the assessment the model selects an authentication decision suitable for the particular risk score. Furthermore the selected authentication decision resource need is compared with the available resource of the authenticator device and incase of scarcity in the available resource, the authentication process is offloaded to a device with available resource.

Our future work includes further development of the model for calculating the channel characteristics and to validate the model by predicating risks using the naïve Bayes classification.

ACKNOWLEDGMENTS

This work has been supported by the research project IoTSec - Security in IoT for Smart Grids, with number 248113/O70 part of the IKTPLUSS program funded by the Research Council of Norway.

REFERENCES

[1] O. Ojo and O. Adigun, "A Grid Enabled Framework for Ubiquitous Healthcare Service Provisioning," in *Advances in Grid Computing*: InTech, 2011.

[2] J. Y. Khan and M. R. Yuce, "Wireless body area network (WBAN) for medical applications," *New Developments in Biomedical Engineering. INTECH*, 2010.

[3] R. V. Sampangi, S. Dey, S. R. Urs, and S. Sampalli, "A security suite for wireless body area networks," *arXiv preprint arXiv:1202.2171*, 2012.

[4] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Consumer Electronics (ICCE), 2011 IEEE Int. Conference on*, 2011, pp. 787-788.

[5] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254-264, 2016.

[6] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "3-level secure Kerberos authentication for Smart Home Systems using IoT," in *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on*, 2015, pp. 262-268: IEEE.

[7] S. Z. Reyhani and M. Mahdavi, "User authentication using neural network in smart home networks," *International Journal of Smart Home*, vol. 1, no. 2, pp. 147-154, 2007.

[8] K. Han, T. Shon, and K. Kim, "Efficient mobile sensor authentication in smart home and WPAN," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 2, 2010.

[9] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 IEEE Fifth International Conference on*, 2013, pp. 88-93.

[10] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)," in *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, 2013, pp. 998-1001: IEEE.

[11] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, 2016.

[12] Y.-P. Kim, S. Yoo, and C. Yoo, "DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things," in *Consumer Electronics (ICCE), 2015 IEEE International Conference on*, 2015, pp. 196-197: IEEE.

[13] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, 2006, vol. 1, p. 8 pp.: IEEE.

[14] Q. Chang, Y.-p. Zhang, and L.-l. Qin, "A node authentication protocol based on ECC in WSN," in *Computer Design and Applications (ICCDA), 2010 Int. Conference on*, 2010, vol. 2, V2-606-V2-609: IEEE.

[15] R. Hummen, H. Shafagh, S. Raza, T. Voig, and K. Wehrle, "Delegation-based Authentication and Authorization for the IP-based Internet of

Things," in *Sensing, Communication, and Networking (SECON), 2014 Eleventh Annual IEEE Int. Conference on*, 2014, pp. 284-292: IEEE.
[16] S. Gerdes, O. Bergmann, and C. Bormann, "Delegated Authenticated Authorization for Constrained Environments," in *Network Protocols (ICNP), 2014 IEEE 22nd Int. Conference on*, 2014, pp. 654-659: IEEE.
[17] N. Zhao, A. Ren, M. U. Rehman, Z. Zhang, X. Yang, and F. Hu, "Biometric Behavior Authentication Exploiting Propagation Characteristics of Wireless Channel," *IEEE Access*, vol. 4, pp. 4789-4796, 2016.
[18] N. Zhao *et al.*, "Double threshold authentication using body area radio channel characteristics," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2099-2102, 2016.
[19] R. Fantacci, F. Chiti, and L. Maccari, "Fast distributed bi-directional authentication for wireless sensor networks," *Security and Communication Networks*, vol. 1, no. 1, pp. 17-24, 2008.
[20] P. Banerjee, T. Chatterjee, and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN," in *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, 2015, pp. 2126-2132: IEEE.
[21] B. Mbarek, A. Meddeb, W. B. Jaballah, and M. Mosbah, "A secure authentication mechanism for resource constrained devices," in *Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of*, 2015, pp. 1-7: IEEE.
[22] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500-528, 2006.
[23] J. Han and D. Kim, "A back-end offload architecture for security of resource-constrained networks," in *Network Computing and Applications (NCA), 2016 IEEE 15th Int. Symposium on*, 2016, pp. 383-387: IEEE.
[24] M. Mana, M. Feham, and B. A. Bensaber, "SEKEBAN (secure and efficient key exchange for wireless body area network)," *International Journal of advanced science and technology*, vol. 12, pp. 45-60, 2009.
[25] G. Caparra, M. Centenaro, N. Laurenti, S. Tomasin, and L. Vangelista, "Energy-based anchor node selection for IoT physical layer authentication," in *Communications (ICC), 2016 IEEE International Conference on*, 2016, pp. 1-6: IEEE.
[26] K. Renaud, "A process for supporting risk-aware web authentication mechanism choice," *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1204-1217, 2007.
[27] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Online risk-based authentication using behavioral biometrics," *Multimedia tools and applications*, vol. 71, no. 2, pp. 575-605, 2014.
[28] D. Hintze, E. Koch, S. Scholz, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 85-88: ACM.
[29] A. Hurkała and J. Hurkała, "Architecture of Context-Risk-Aware Authentication System for Web Environments," 2014.
[30] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior," in *Sicherheit*, 2014, pp. 1-12.
[31] L. Li, X. Zhao, and G. Xue, "Unobservable Re-authentication for Smartphones," in *NDSS*, 2013.
[32] H. Abie, R. M. Savola, J. Bigham, I. Dattani, D. Rotondi, and G. Da Bormida, "Self-healing and secure adaptive messaging middleware for business-critical systems," *International Journal on Advances in Security*, vol. 3, no. 1&2, 2010.
[33] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health IoT applications," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 276-281: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[34] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in *Proceedings of the International Workshop on Adaptive Security*, 2013, p. 6: ACM.
[35] A. B. Torjusen, H. Abie, E. Paintsil, D. Trcek, and Å. Skomedal, "Towards run-time verification of adaptive security for IoT in eHealth," in *Proceedings of the 2014 European Conference on Software Architecture Workshops*, 2014, p. 4: ACM.
[36] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 269-275: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[37] R. Hulsebosch, M. Bargh, G. Lenzini, P. Ebben, and S. Iacob, "Context sensitive adaptive authentication," *Smart Sensing and Context*, pp. 93-109, 2007.
[38] M. Sarvabhatla and C. S. Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN," in *Emerging Applications of Information Technology (EAIT), 2014 Fourth International Conference of*, 2014, pp. 367-372: IEEE.
[39] J. Spooren, D. Preuveneers, and W. Joosen, "Leveraging Battery Usage from Mobile Devices for Active Authentication," *Mobile Information Systems*, vol. 2017, pp. 1-14, 2017.
[40] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Communications (ICC), 2014 IEEE International Conference on*, 2014, pp. 920-925: IEEE.
[41] M. A. Ferrag, L. A. Maglaras, H. Janicke, and J. Jiang, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *arXiv preprint arXiv:1612.07206*, 2016.
[42] S. Prameela and P. Ponmuthuramalingam, "A robust energy efficient and secure data dissemination protocol for wireless body area networks," in *Advances in Computer Applications (ICACA), IEEE International Conference on*, 2016, pp. 131-134: IEEE.
[43] M. Rizk and M. Mokhtar, "An efficient authentication protocol and key establishment in dynamic WSN," in *Information Communication and Management (ICICM), Int. Conference on*, 2016, pp. 178-182: IEEE.
[44] M. Särestöniemi, T. Tuovinen, M. Hämäläinen, K. Y. Yazdandoost, and J. Iinatti, "Channel modeling for UWB WBAN on-off body communication link with finite integration technique," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 235-241: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[45] S.-H. Han and S. K. Park, "Performance analysis of wireless body area network in indoor off-body communication," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 2, 2011.
[46] A. Taparugssanagorn, C. Pomalaza-Ráez, R. Tesi, M. Hämäläinen, J. Iinatti, and R. Kohno, "UWB Channel Characteristics in the Proximity of a Dynamic Human Body for WBAN Medical Applications," in *Submitted to Int. Symp. on Medical Information and Communication Technology (ISMICT)*, 2010.
[47] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803-1816, 2013.
[48] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 331-344: ACM.
[49] A. Scannell, A. Varshavsky, A. LaMarca, and E. De Lara, "Proximity-based authentication of mobile devices," *International Journal of Security and Networks*, vol. 4, no. 1-2, pp. 4-16, 2009.
[50] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*, 2006, pp. 33-42: ACM.
[51] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, 2007, pp. 111-122:
[52] A. Domazetovic, L. J. Greenstein, N. B. Mandayam, and I. Seskar, "Estimating the Doppler spectrum of a short-range fixed wireless channel," *IEEE Communications Letters*, vol. 7, no. 5, 227-229, 2003.
[53] X. Yin, J. Chen, M. Tian, N. Zhang, Z. Zhong, S. X. Lu, Personal authentication using the fingerprints of intra-body radio propagation channels, 2013 7th Int. Symp. on Medical Information and Communication Technology (ISMICT), 6-8 March 2013