http://dx.doi.org/10.5755/j01.eee.20.6.7285

Identification of Dependency among Energy Consumption and Wi-Fi Protocol Security Levels within the Prototype Module for the IoT

A. Venckauskas[1], N. Jusas[1], E. Kazanavicius[1], V. Stuikys[1]
[1]*Department of Computers Science, Kaunas University of Technology,*
Studentu St. 50-213, LT-51368, Kaunas, Lithuania
algimantas.venckauskas@ktu.lt

***Abstract*—In this paper, we present an approach to design the prototype module for the Internet of Things (IoT), which is based on using the Wi-Fi protocol. The aim is to investigate and identify some properties of the module such as dependency among energy consumption and security levels. The contribution of the paper is the configurable IoT prototype module enabling to provide wide-scale experiments to obtain energy-security dependencies for various modes of the IoT applications. We also present the design process, the structure and behaviour of the whole system, and a methodology for energy measurement. We compare the obtained results in two different modes: ideal (without effect of noises to functionality of the module) and real (with noises presented within real communication environment).**

***Index Terms*—Internet, wireless networks, information security, energy consumption.**

I. INTRODUCTION

The technology advances have resulted in that we already today live and work in a digital world surrounded by the modern technology infrastructure – the multiple devices integrated within networks along with computers, mobile devices, sensors networks, etc. is commodity of our lives now. In the nearest future, however, not only humans and computers but also everyday-life items will be interconnected to create the new computing infrastructure - *The Internet of Things* (IoT) [1]. The goal of the IoT is to enable things to be connected “anytime, anyplace, with anything and anyone ideally using any path/network and any service” [2]. Semantically, the IoT means a *new highly heterogeneous world-wide network* of interconnected objects uniquely addressable, based on standard communication protocols [3]. This move from “interconnected computers” to “interconnected things” is a great challenge for the Information-Communication Technology (ICT) workers, scientists and society in the whole. As a response to the challenge, an extremely wide stream of research is provided worldwide now.

From the pure technological viewpoint, this technology-based paradigm change causes the need to reconsider old communication-related problems and to solve new ones [4]–[6]. Though there are many research efforts and variety of tasks to be yet solved within this new paradigm, two major concerns, namely energy awareness and information security and privacy, remain as most crucial ones. There are many reasons for that. Internet connectivity is becoming increasingly ubiquitous and pervasive. The heterogeneous networks within the IoT (such as mobile, ad hoc, sensor networks) use batteries as a main energy resource. Diversity of possible applications may pose a quite different level of information security (from unsecure to highly secret).

Each factor (energy-awareness, security, performance) when considered separately within a communication network, is a big problem in its own. As those factors are in deep relationship also with requirements of a particular application, the problem becomes even more complicated. For example, energy-awareness depends on network topology, communication intensiveness, the IoT (network) node working mode, etc.

On the other hand, energy measurement requires some *adequate models of the IoT node* in order we could be able to reason about its behaviour in term of energy consumption in the whole. In this paper, in the context of IoT research project [7], we propose a *Prototype Module for the IoT* (further PM for short). The PM should be considered as a node of a possible IoT. The aim is first to have a node of IoT at hand that models the behaviour of IoT adequately, and then to identify the empirical dependency upon the energy consumption and security levels of the standard Wi-Fi module embedded within the prototype. To achieve the aim, we consider the following two tasks: 1) developing of a common *methodology* to design and investigate behaviour of the PM as a node of a possible IoT and 2) providing experiments for identification the dependency upon the energy consumption and security levels of the standard Wi-Fi module. By PM we mean a module to be embedded into *a node* of the Internet of Things (IoT) or a node of the IoT prototype. The PM function is to support two activities: communication and control in order to create data for the measuring sub-system.

Our contribution is the reconfigurable PM and energy-

Manuscript received December 12, 2013; accepted March 19, 2014.
This research was funded by the grant No. VP1-3.1-SMM-08-K-01-018 financed from the EU SA.

security level dependency obtained using the PM in two modes: 1) ideal case when there are practically no noises that may affect the quality of communication; 2) communication under the present of unpredictable noises within the communication environment.

II. Related Work

Though there is an extremely large amount of literature on various aspects of the IoT, we have selected [1]–[3] to outline the context of our paper. According to [2], the future communication infrastructure is seen as the *Future Internet* at the top and the *Internet of Things* at the bottom to create smart environments. Those environments will include eight smart applications: Smart Cities, Smart Transport, Smart Living, Smart Health, Smart Buildings, Smart Industry, and Smart Planet. Thus, the arrival of the IoT indicates on the paradigm change in communication technology now. The paradigm change exacerbates the old communication problems and poses new ones such as security, privacy, energy, performance [1]–[3].

Security problems are common for both various communication networks and IoT [4]–[6], where the standard communication protocols are at the focus [3] (see [7], for more extensive analysis). In recent years with the expansion of mobile technologies, the interest to security and energy awareness problems has grown significantly. Due to their importance and complexity, in most cases authors consider them separately. The paper [8] provides security levels as applied to different types of applications (we use those levels in our paper too). In [9], authors present an extensive study on energy measurements methodologies (both at device and application levels). The papers [10], [11] present some investigation results on efficiency and energy consumption using cryptographic algorithms.

III. Description of the Approach

The approach describes the *design process*, the *structure* and the *behaviour* of the system within which the developed IoT nodes are integrated to provide experiments for achieving our aims. The approach includes six interrelated stages: 1) Statement of the requirements to design PM and measurement environment; 2) Design of PM hardware (HW); 3) System integration: PM with the measurement module (MM); 4) software (SW) integration into the system and testing; 5) Development of the measurement methodology; 6) Providing experiments to obtain empirical data for the dependency (energy-security) identification.

The main requirements (stage 1) are as follows: a) the use of the standard protocol Wi-Fi to support communication with PM; b) the use of standard hardware in the mode ‘plug-in-and-pay”; c) hardware should be small enough in size, reliable, easy to connect and test the system; d) the use of standard software platform to enable various modes; e) re-configurability to adapt the PM to various modes of use; f) the module should model the essential features of the IoT node and at the same time to contain capabilities to provide the prescribed experimentation.

To implement the PM at Stage 2, we have selected the GHIelectronics HW platform [12] that consists of a set of kits *(FEZ Spider Starter Kit)*. As the PM has to perform two activities (bi-directional communication and control), there two modules within the prototype are needed. The first is the communication module (CM). The second is the control and processing module (CPM).

At Stage 3, we need first to devise the measurement hardware, and then to integrate it into the system. Figure 1 outlines the architecture of the whole system as a result of implementing Stages 2 and 3.

At Stage 4, we aim at ensuring the correct functioning of the system. For that, we perform the following actions: 1) Loading the SW part into the CPM module and 2) system testing. We use the *.NET Gadgeteer* tools developed by Microsoft for the purposes to support small electronic projects [12]. As practically all components are standard, the testing procedure of the whole system is simple. During the procedure, user learns on how to work with the system to be prepared for experimentation.

At stage 5, we plan the scope, time, place and sequence of activities to be performed during the experimentations. To ensure reliability, we need also to anticipate the possibility to repeat of experiments. Finally, at stage 6, processing of the collected measured data takes place.

In Fig. 1, we present the system’s architecture. It consists of three components: PM and Wi-Fi access point and MM. The first is the *information source* to be transferred, while the second is treated as *a sink (user)* of this information.

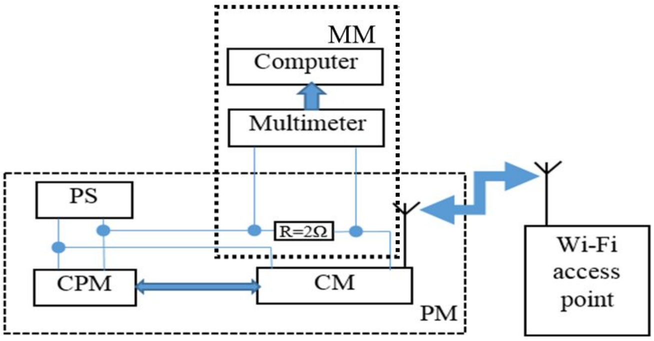


Fig. 1. Architecture of the system. PS – power supply, CMP – Control and processing module, CM – communication module, PM – prototype module, MM – measurement module.

Figure 2 describes the behaviour (processes) of the system. Process 1 models the data collecting and processing by CPM for transferring. Process 2 identifies the needed characteristics (volume of data, security level, etc.). Process 3 initializes the data transfer. The remaining Processes (4 and 5) identify the transferring session: its duration and ending.

IV. A Methodology to Provide Experiments

The proposed methodology includes the following stages:

1. Identification of the location to provide experimentations in the *ideal mode* using the created environment (when there are no noises that could affect the provided measurements).
2. Identification of the location to provide experimentations under the real mode conditions using the created environment (when there are noises that really affect measurements).

3. Identification of the parameters to provide measurements, the number of trials for each measurement, identification of the interval between trials taking into account the capabilities the multimeter, etc.
4. Automatic fixing of measured data and storing them into the file within PC for the further processing.
5. Processing of measured data to obtain the required characteristics using MATLAB.

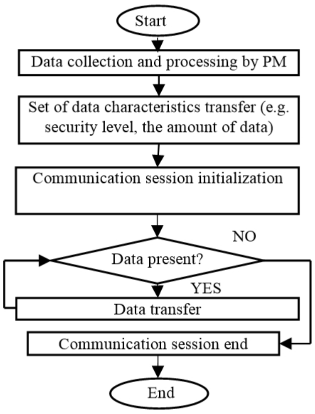

Start
Data collection and processing by PM
Set of data characteristics transfer (e.g. security level, the amount of data)
Communication session initialization
NO
Data present?
YES
Data transfer
Communication session end
End

Fig. 2. Behaviour model of the PM.

We have selected the rural location (Stage 1), which we have been identified as an ideal place to provide our experiments because there were no evident radio signals that might make the interference with the measured ones. On contrary, the large organization with the well-developed communication infrastructure within the urban area (city) has been treated as a location (Stage 2) to create the real conditions for experiments. At stage 3, there were identified the following parameters: (i) the distance between the PM and Wi-Fi access point was about 10 m for both ideal and real cases; (ii) the interval between the measurement trials was 0.5 s (it was predefined by multimeter characteristics); (iii) the number of trials to measure the same characteristics was 10; the volume of information to be coded/decoded and transferred was equal to 0.5 MB and the volume of buffer was (512 and 1024 bits) (the same for each trial and each mode). All 7 possible modes of standard Wi-Fi protocol have been applied [3] see also (Fig. 3) (Unsecure, WEP_64, WEP_128, WPA-AES, WPA_TKIP, WPA2_AES, and WPA2_TKIP_AES). At Stage 4, the measured voltage has been fixed automatically and its value has been repeatedly stored. The results of processing (Stage 5) we have presented in Section V.

V. Experimental Results

In Fig. 3, we provide the view of the implemented system for our experiments. One can identify the links between the structural components presented in Fig. 1 and those presented here.

In Fig. 4, we present the measured voltage waveforms recalculated to power units. Figure 4(a) shows the signal form for ideal mode Figure 4(b)–Fig. 4(d) shows the real mode. In the real mode, the signal forms differ significantly. Practically all 10 trials were different (only 3 variants are given in Fig. 4(b)–Fig. 4(d) to illustrate that); whereas in the real mode each trial practically had the same waveform (it is why we present the only one instance in Fig. 4(a)). Thus, the signal forms obtained approved the assumption that the selected locations (rural and big organization in the city with well-developed communication infrastructure) can be seen as *ideal* and *real* ones.

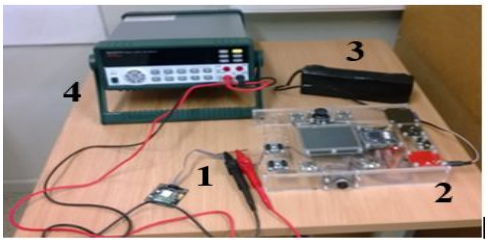
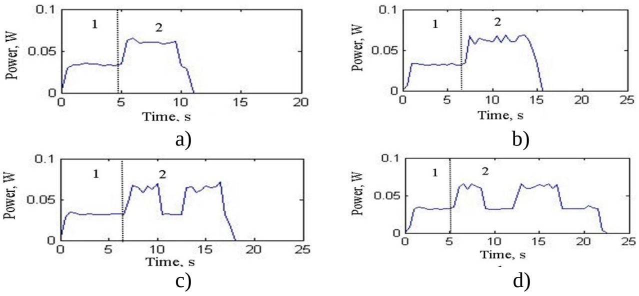


Fig. 3. Implementation view 1 -CM, 2 – CPM, 3 – PS, 4 – multimeter.



a)

b)

c)

d)

Fig. 4. Data transfer waveforms a – ideal mode; b, c, d – real environment.

Note that each presented signal represents two phases: 1 (meaning the power consumed for the search of remote Wi-Fi access point and linking to it) and 2 (meaning the power consumed for data transfer).

As it was mentioned above, for the ideal case, signal waveforms practically were the same for each out of 10 made measurements. But in the real mode, waveforms differ significantly. Such kind of disparities could influence the noisy environment where is a lot of different Wi-Fi signals. By identifying the delay differences (duration of among waveforms) we are able to model performance of the PM.

Table I shows the relationship among the Wi-Fi standard protocol modes and security levels, which were identified as proposed in [8]: Unclassified (U), Sensitive but Unclassified (SU), Restricted (R), Confidential (C), Secret (S), and Top Secret (TS) are introduced. Note that security levels are more relevant to characterize applications, whereas protocol modes are usually used to specify security in cryptography.

TABLE I. MATCHING BETWEEN WI-FI MODES AND SECURITY LEVELS.

Wi-Fi mode	Unprotected	WEP 64	WEP 128	WPA AES	WPA TKIP	WPA2 AES	WPA2 TKIP AES
Security Level	U	SU	SU	R	C	S	TS

In Fig. 5, we present some results of solving the second task, i.e. the identification security level-energy dependencies. The results were obtained using the MATLAB facilities. Here, the following dependencies one can see: the modes WPA_64 and WPA_128 have very small or no impact for the energy consumption as compared with the unprotected connection, whereas WPA and WPA2 increase energy consumption is about 25 %. The biggest impact on energy consumption has the environment.

Depending on security level, the energy consumption increase is between 30 %–95 %.

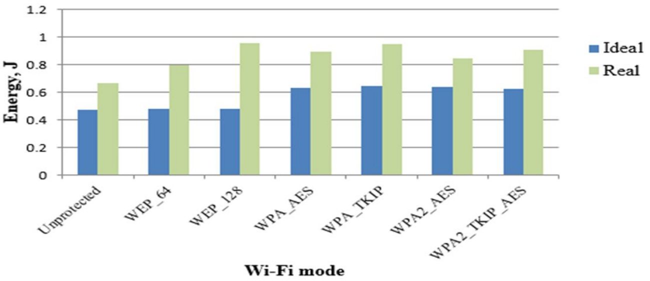


Fig. 5. Energy-security mode dependency in ideal and real modes.

In Table 2, we summarize the results in more compact way. To evaluate the energy consumption dependences on the used Wi-Fi modes, we have calculated the following energy consumption estimates: average, standard deviation and prediction interval [13].

TABLE II. ENERGY-WIFI MODE-ENVIRONMENT DEPENDENCY.

Wi-Fi mode	Ideal mode (no noises)				Real mode (with noses)			
	Average	Standard deviation	Prediction interval		Average	Standard deviation	Prediction interval	
			min	max			min	max
Unprotected	0.475	0.028	0.446	0.503	0.664	0.038	0.626	0.702
WEP_64	0.481	0.008	0.473	0.488	0.799	0.122	0.677	0.921
WEP_128	0.481	0.008	0.473	0.488	0.956	0.196	0.759	1.152
WPA_AES	0.636	0.030	0.607	0.666	0.895	0.116	0.779	1.011
WPA_TKIP	0.648	0.030	0.618	0.678	0.948	0.163	0.785	1.111
WPA2_AES	0.637	0.030	0.607	0.667	0.848	0.117	0.732	0.965
WPA2_TKIP_AES	0.626	0.005	0.622	0.631	0.906	0.104	0.802	1.010

VI. EVALUATION AND DISCUSSION

The prototype module has been designed for the investigation of functionality of the IoT node with the focus on a variety of the requirements in terms of energy and security issues for different IoT-based applications. In our experiments, we have modelled the possible applications by the level of security, which can be expressed by the standard modes of Wi-Fi protocol. Also the ideal and real modes of using prototypes define the boundaries of environments of possible applications. The following features of the prototype module are of the great importance: (i) the prototype has a modular structure based on standard components, thus it is reliable and easy to construct; (ii) the prototype is reconfigurable in terms of easiness to change the communication protocol (e.g. along with Wi-Fi we also were using Bluetooth protocol; the latter results are beyond of the scope of this paper) and in terms of flexible change of mode within the selected protocol; (iii) the prototype is able to model the behaviour of IoT node well because of its structure contains the essential features needed for communication and processing. It was identified the decrease of performance about twice in the worst case (real case with intensive use communication devices that create noises) as compared to the ideal case (compare the right part of the form in Fig. 4(a) with the adequate parts in Fig. 4 (b).)

The distinguishing feature of the approach as compared to others (e.g. [9]), we measure the energy consumption needed for communication module only. This enables ensuring higher accuracy. The configurability features enables to extend applicability of the module for different application with different requirements for energy, security and performance. The proposed approach has some limitations too. As the approach uses restricted space of the predefined data for modelling, the use of other data may shape the results in somewhat way. Also it would be difficult to measure the energy consumption in high frequency communication protocols, without the introduction of some improvements in the methodology.

VII. CONCLUSIONS

1. The proposed measuring methodology enables to measure energy needed only for communication (data transferring), thus we are able to achieve higher accuracy because measuring errors of information processing are eliminated.

2. The proposed prototype module models the IoT node's structure and behaviour well in terms of the identified configurability (easiness to change protocol and its mode of use and portability).

3. Experiments have shown that the Wi-Fi modes WPA and WPA2 increase the energy consumption about 25 % as compared to the unprotected modes WEP_64 and WEP_128. The biggest impact for the energy consumption was the environment, which increases energy by 30 %–95 % depending on security level. In addition, this increase is less predictable because it depends more on the environment and less on the security levels.

REFERENCES

[1] L. Atzori, A. Iera, G. Morabito, "The internet of things: A survey", *Computer Networks*, vol. 54, pp. 2787–2805, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

[2] I. G. Smith, *The Internet of Things 2012: New Horizons*. Halifax, UK, 2012.

[3] L. Houda, H. Afifi, C. De Santis, *Wi-Fi, Bluetooth, Zigbee and WiMAX*. Springer, 2007.

[4] X. Chen, K. Makki, K. Yen, N. Pissinou, "Sensor network security: a survey", *IEEE Trans. Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009. [Online]. Available: http://dx.doi.org/10.1109/SURV.2009.090205

[5] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, S. Meissner, *Enabling things to talk: designing IoT solutions with the IoT architectural reference model*. Springer, 2013. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40403-0

[6] E. Kazanavicius, V. Kazanavicius, A. Venckauskas, R. Paskevicius, "Securing web application by embedded firewall", *Elektronika ir Elektrotechnika*, no. 3, pp. 65–68, 2012.

[7] A. Venckauskas, V. Stuikys *et. al.* "Analysis and development of security models of energy-efficient communication protocols", Kaunas, Report of project No. VP1-3.1-SMM-08-K-01-018, 2013.

[8] M. Pastore, M. A. Pastore, E. Dulaney, *CompTIA Security+ Study Guide: Exam SY0-101*. Wiley. 2006.

[9] R. Damasevicius, V. Stuikys, J. Toldinas, "Methods for measurement of energy consumption in mobile devices", *Metrology and measurement systems*, no. 3, pp. 419–430, 2013.

[10] A. Michalkovic, E. Sakalauskas, A. Venckauskas, "New asymmetric cipher based on matrix power function and its implementation in microprocessors efficiency investigation", *Elektronika ir Elektrotechnika*, vol. 19, no. 10, pp. 119–122, 2013.

[11] M. D. Cano, G. Domenech-Asensi, "A secure energy-efficient m-banking application for mobile devices", *Journal of Systems and Software*, vol. 84, no. 11, pp. 1899–1909, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.jss.2011.06.024

[12] S. Monk, *Getting started with .NET gadgeteer*. O'Reilly Media, 2012.

[13] W. Navidi, *Statistics for engineers and scientists*. New York: McGraw-Hill, 2011.