**Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 74-78 ISSN 2587-4667**
**Scientific Cyber Security Association (SCSA)**

# MODELS AND METHODS OF WIRELESS DECENTRALIZED NETWORKS FOR ENERGY MONITORING OF CRITICAL INFRASTRUCTURE FACILITIES

Yuliia Kovaleva, 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Tetiana Babenko, 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine
Vira Ignisca 1-4 Faculty of Information Technology, Taras Shevchenko National University of Kyiv, Ukraine

**ABSTRACT**: In this article, we describe the many models describing the dependence of power consumption on the operating modes of 802.15.4 / ZigBee devices at the MAC and NWK levels of the specification, it is not so much of practical interest to develop a realistic analytical model for predicting the lifetime of a system in IEEE 802.15.4 networks, taking into account the possible external impact on network, how much is the implementation of a new approach to building a reliable, fault-tolerant self-regulating autonomous decentralized network P2P architecture.

**KEYWORDS***: information security auditor, personnel evaluation, critical infrastructure facilities, Rush model, Binary selection with logistic function, artificial neural networks.*

## INTRODUCTION

Technological advances in microelectronics have enabled the mass production of miniature transceivers with extremely low power consumption that can be networked and communicated with each other using wireless communication channels. Autonomous networks of such devices are called wireless monitoring networks (WMN), which, in particular, emphasizes their main purpose - the collection of data from sensors (meters) for further analysis and transmission of control commands.

The change in the flows of active and reactive power caused by distributed generation has important technical and economic consequences for the distribution network, which makes it obvious the inconsistency of centralized approaches to the architecture of automated energy monitoring systems and actualizes the need to model processes in decentralized systems. A new approach to energy management in field equipment that takes into account the stochasticity of variables and adapts predictive models to compensate for data latency, signal latency, and disturbances in real time, allows you to create autonomous decentralized systems with a predictable lifespan and an acceptable level of service quality.

## PROBLEM DEFINITION

Smart Metering is currently being implemented in the traditional energy system with an advanced communications network to collect meter readings to update the energy billing process. The implementation of these communication infrastructures and the associated Smart Grid applications is driving the rapid increase in data transmission in information networks. This, in turn, creates new problems: connection failures, delays in information transfer, data errors, etc., which are becoming more and more critical.

Extending network lifespan is a common goal of wireless research, as a network node is usually limited by the capacity of the power supply, which determines its lifetime. In works [1, 2], the concept of the energy value of a node was introduced, defined as the ratio of the total consumed energy to the initial energy of the battery. The value of a node is the higher, the less is the ratio of the energy expended by the

node when operating in the network to its initial energy. According to this model, the total energy consumption includes the energy spent on sending and receiving packets, sleep and sensing modes.

However, the authors did not consider additional sources of energy costs, such as packet control in the GTS mode and retransmissions caused by network interference. The latter is decisive, since with heavy traffic, the retransmission of "unsuccessful" packets leads to significant additional energy consumption, leading to a reduction in the network lifetime. The model proposed in [3] eliminates this disadvantage, but does not offer an analytical method for calculating the probability of a failed transmission. In [4], a model for predicting communication delays in the GTS mode is proposed. There is a direct dependence of the lifetime of a wireless monitoring network on its security, so the issue of the system's resistance to external interference is crucial. Considering the many models describing the dependence of power consumption on the operating modes of 802.15.4 / ZigBee devices at the MAC and NWK levels of the specification, it is not so much of practical interest to develop a realistic analytical model for predicting the lifetime of a system in IEEE 802.15.4 networks, taking into account the possible external impact on network, how much is the implementation of a new approach to building a reliable, fault-tolerant self-regulating autonomous decentralized network P2P architecture.

The European Commission has created a Smart Grid Task Force (SGTF). SGTF defines smart grids as electrical grids that can effectively integrate the behavior and actions of all users connected to it - generators, consumers and potential customers - to provide a cost-effective, sustainable power system with low losses and high quality and security of supply and safety [5]. The Smart Grid Model (SGAM) architecture [6] was proposed by the European Standards Organization as a reference model for Smart Grids (Fig. 1).

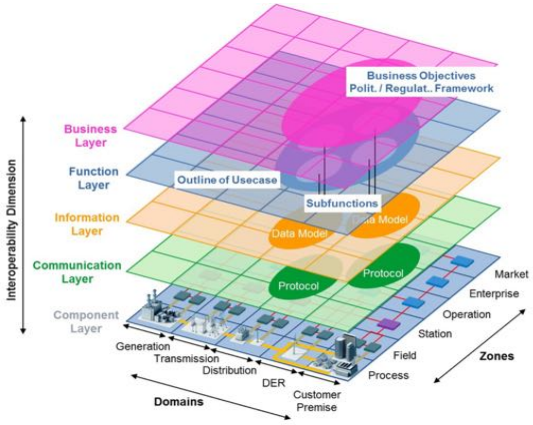


Figure 1. Reference architecture SGAM

The smart grid is transforming into an internet of energy, and blockchain technology can be a link between the smart grid and consumers, which will facilitate the active participation of end users in energy markets. The purpose of using blockchain technology in distributed control, management and verification of the implementation of demand control programs by intelligent energy monitoring grids is the need to ensure high reliability and decentralized operation by implementing instant transactions, protection against unauthorized access and demand regulation in real time. In this context, the smart grid represents peers coordinating their activities along the infrastructure chain in order to maintain decentralized demand and ensure stable network operation.

One of the main obstacles faced by smart metering today is data privacy and security, which in the case of blockchain is addressed using distributed block ledger functions. A distributed blockchain database is built and managed at the smart grid level. Each node is equipped with IoT-based meters that record controlled data in blocks within the blockchain. Thus, any node is a peer-to-peer distributed energy network node and can maintain a copy of the database that is automatically updated when new energy

consumption data is logged. The blockchain database consists of many blocks connected in a peer-to-peer chain and is held by the participants who decide to include data in the registry. The network is built by combining computers according to the principle of the same functions. That is, a computer receiving information is a server, and by transmitting information to the network it performs the function of a client. Networks of this kind operate on a peer-to-peer basis (originally peer-to-peer or P2P) and are called peer-to-peer or decentralized. Successful operation of WMN applications requires coordinated operation and management of a large number of distributed and loosely coupled field smart devices that identify and trust each other. Decentralization of the WMN infrastructure provides benefits, including a reduction in the amount of data transmitted to the Internet for processing and analysis, and improved security and confidentiality of information. Ensuring the validity of these operations means achieving a distributed consensus across the WMN field devices.

One of the biggest challenges in integrating blockchain into IoT is scalability. Due to the large number of devices and resource constraints, blockchain deployment in the IoT is particularly challenging. An optimal blockchain architecture must scale to many I / O devices (they become peers on the blockchain chain) and it must handle high transaction throughput.

Decentralization of the WMN infrastructure provides benefits, including a reduction in the amount of data transmitted to the Internet for processing and analysis, and improved security and confidentiality of information. Ensuring the validity of these operations means achieving a distributed consensus across the WMN field devices. Now three fundamentally different approaches to solving the problem of transferring and processing information by various platforms of existing solutions have been formed - the IBM Research solution based on Hyperledger Fabric technology [7], the IOTA consortium solution based on the Tangle protocol, which is based on DAG (Directed Acyclic Graph), and Qubic technology [8] and the advanced approach of the Radix project based on Tempo Ledger technology [9]. These approaches combine the ability to run on a wide variety of hardware, and a functional programming language allows for simpler analysis to prove code is correct and emphasizes parallelism, which means that different parts of a larger program can run concurrently to take advantage of multiple processors or even multiple processors. devices.

Proof-of-work (PoW) - The consensus mechanism is considered a highly energy-intensive technology. Given the importance of (PoW) - the consensus mechanism, IBM Research is developing a new method for implementing this mechanism using the computing power of devices of the Internet of Things
[10]

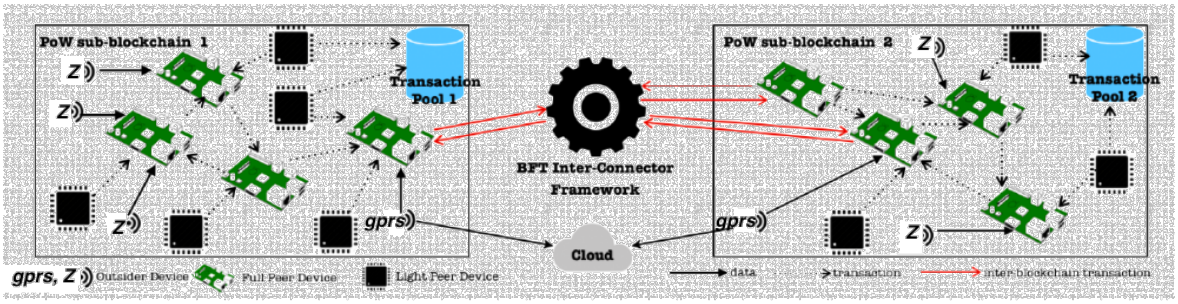


Figure 2. Hybrid WMN blockchain [8]

One of the biggest challenges in integrating blockchain into IoT is scalability. Due to the large number of devices and resource constraints, blockchain deployment in the IoT is particularly challenging. An optimal blockchain architecture must scale to many I / O devices (they become peers on the blockchain chain) and it must handle high transaction throughput. Hybrid-IoT, a platform developed by IBM Research, uses both PoW block diagrams and Bytantine Fault Tolerant (BFT) protocols to achieve

scalability. First, PoW block diagrams provide a distributed consensus among many IoT devices, peers on the blockchain in a clustered sub-blockchain. Hybrid-IoT uses the BFT inter-cluster interconnect framework to ensure mutual understanding between blockchains.

The chosen structure of virtualized I / O devices represented by Hybrid-IoT peers with different roles within a separate PoW blockchain proves the effectiveness of the PoW blockchain design, which also prevents security vulnerabilities.

IoT network devices have an extremely wide range of computing power and energy resources, and some of them cannot solve the complex problems provided by PoW. Dividing nodes into groups allows the algorithm to decide what proportion in each group should mine, depending on the amount of energy used by each node. In this model, only some of the nodes (nodes) implement full PoW. IBM found that when placing nodes in clusters of 250 units, only 7% of these sub-blockchains performed PoW, achieving the best results in terms of economy, scalability, and security.

IOTA, designed with scalability in mind, introduced the concept of a dedicated smart contract platform called Qubic, running on top of the core IOTA protocol. Individual Qubics are essentially quorum-based distributed computing tasks. Qubic uses the IOTA Tangle to package and distribute cubes from their owners to the oracles who will handle them. Technically, the Tangle method is an acyclic graph - it is a looping method where loops can be executed in parallel. Cubes can live on Tangle while dormant. When specific inputs become available or changed, they are "awakened" and processed, which can cause a cascade of other cubes to wake up as new results appear. This allows you to create a very dynamic programming environment that allows you to add new cubes at any time and bind them to any input. After the cube has been processed, the quorum reached, and the results sent to the Tangle, two things happen: 1) qubic goes to sleep again, waiting for the next input change, and 2) the cascade effect is triggered so that the dependent qubic unfolds and starts processing with new inputs. The technology assumes an economical mode of operation and is optimized for low power consumption and small amount of memory in field devices, which does not exclude large-scale calculations, especially those that can be parallelized and distributed over a large number of processors.

RADIX has proposed a peer-to-peer network of nodes with logical clocks to generate temporary evidence of the chronological order of events. Radix has achieved a solution to both problems in such a way that it does not need PoW (mining), it does not need PoS (proof of stake), and it does not need master nodes to confirm transactions. The system is secure by providing nodes with a historical record of the generated temporary evidence. RADIX DLT has linear scalability. This means that the more nodes added to the network, the more it will scale. Unlike current solutions, each node added increases the throughput of the Radix network. Radix will allow even resource-limited devices to participate as nodes on the network. The Radix node can be run on a device with a 16MB memory and a 100 MHz processor. This will make decentralization even more perfect.

Radix Tokens (RAD) uses decentralized leger technology (DLT) to record transactions. RadixDLT offers a system that improves, albeit different, blocking technology in terms of scalability. RadixDLT stores all transactions and orders in a protocol in a global distributed ledger called Tempo Ledger. This book consists of three main components: a network cluster of nodes, a global register database distributed across nodes, and an algorithm for generating a cryptographically secure record of temporarily ordered events.

## CONCLUSION:

As blockchain technology develops, the most promising solution seems to be RadixDLT, since it is devoid of IOTA's drawbacks in terms of the cumbersome mechanism for implementing smart contracts and is not as demanding on hardware resources as IBM Hyperledger. In terms of hardware solutions, the most likely is the use of productive "light" nodes on low-power devices such as the Raspberry Pi, which are controlled by a Radix-based master node. This implementation does not imply the installation of the

central server of the system, and its synchronization is carried out by the master nodes, dispersed geographically. This increases the overall performance of the network, optimizes its power consumption and provides guaranteed resilience to various types of cyber attacks.

**REFERENCE:**

[1] Sofiane Ouni, Zayneb Trabelsi Ayoub/ Predicting communication delay and energy consumption for ieee 802.15.4/zigbee wireless sensor networks.- International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013. Pp. 141-152

[2] Eduardo Casilari, Jose M. Cano-García, Gonzalo Campos-Garrido/ Modeling of Current Consumption in 802.15.4/ZigBee Sensor Motes.- Sensors 2010, 10, 5443-5468; doi:10.3390/s100605443

[3] Bruno Bougard, Francky Catthoor, Denis C. Daly, Anantha Chandrakasan, Wim Dehaene/ Energy Efficiency of the IEEE 802.15.4 Standard in Dense Wireless Microsensor Networks: Modeling and Improvement Perspectives. - Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05)

[4] Jefferson Antonio Zeni Trevisan, Andre´ Augusto Mariano, Eduardo Parente Ribeiro/ Average Power Consumption Model For Wireless Sensor Networks.- Universidade Federal do Paraná. Av. Coronel Francisco Heráclito dos Santos, 210. Curitiba - PR - 81531-970 - Brazil. 1jtrevisan@ufpr.br. Доступ: www.inatel.br/.../82-averagepowerconsumptionmodelforwir...

[5] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture; 2012. [Online] Available at: http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[6] Smart Grid Task Force - EG1 Report, Interoperability, Standards, and Functionality Applied to Large Scale Smart Metering Deployments, October 2015.

[7] Gokhan Sagirlar, Barbara Carminati, Elena Ferrari, John D. Sheehan, Emanuele Ragnoli. Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains.- IEEE International Conference on Blockchain (Blockchain-2018), July 30 - August 03, 2018 Halifax, Canada https://arxiv.org/abs/1804.03903