UDC 004.043

V. Buriachok , V. Sokolov
Borys Grinchenko Kyiv University
v.buriachok@kubg.edu.ua
v.sokolov@kubg.edu.ua

SAFE MONITORING SYSTEM FOR WIRELESS NETWORKS BASED ON THE MERKLE TREE

Abstract—The Merkle tree, which is proposed in this report for use in the creation of wireless networks, is a special data structure that contains summary information about a certain amount of data and is used to verify the integrity and reliability of the data and their individual nodes transmitted between the nodes.

Keywords—monitoring system, blockschain, Merkle tree.

I. Introduction

Internet communication standards, as well as service applications, provide data delivery to network users in order to:

• Organization of work with hypertext pages

• Provision of the necessary resources on request of web-clients

• Access to distributed databases that is a chain of transaction blocks (blockschains), in which each block contains a timestamp and a link to the previous hash tree block [1, 2].

II. Ensuring the Integrity and Reliability of Data and Resources

To increase the stability of wireless networks, we introduce an external negative feedback, the role of which we offer a subsystem with spectrum analyzers.

Incorporating it into a schematic solution for the creation of monitoring systems for wireless networks using the Merkle tree will provide the opportunity to save limited resources of sensors used for processing and storage of data in computers, as well as the transfer of such data between the PC. This is due to the fact that the functions of hashing in contrast to the encryption functions, require for this much less resources.

Considering that the wireless subscribers of an enterprise or organization can be divided into three categories:

• Mobile (mobile phones, tablets, etc.).
• Conditional mobile (laptops).
• Stationary (PC).

Connect spectrum analyzers can only conditionally mobile and landline subscribers (see Table 1). We select mobile subscribers in a separated group [3, 4] with different algorithms for embedded systems (see Table 2).

Table 1.

Software and hardware list

Hardware	Software
Access point (AP) & clients: Raspberry Pi OLED SSD1306 TFT ILI9341 LED HDMI LCD HID Sensors: Pololu Wixel (CC2511-F32) OLED SSD1306	AP: OS Raspbian Lite (Linux) dnsmasq hostapd cmtg v.3 (COMonitoring) Python 3 OLED libraries Clients: OS Linux cmtg v.3 Sensors: C# firmware OLED visualization library

Table 2.

Justification of the algorithm choice

Classic version	Embedded systems
Encryption Key infrastructure Complete mixing hash algorithm	MD5-hashing [5] Lack of key infrastructure HP HashFusion [6]

II. Prototype Implementation

This algorithm allows you to apply hash functions of any length and works fairly quickly even on weak processors (see Fig. 1).

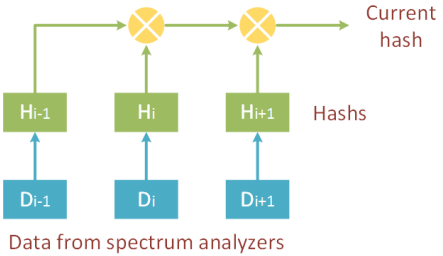

Fig. 1. Subsystem using the Merkle tree

A general view of the monitoring system prototype of wireless networks with a spectrum analyzer subsystem is presented on Fig. 2.

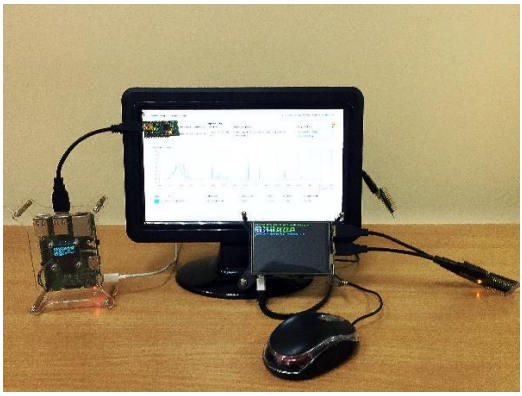

Fig. 2. General view of the prototype

III. Future Work

- Testing the system in real conditions.
- Increasing the number of sensors.
- Determining the optimal number of clients with sensors.
- Use of other OS (Windows, iOS) and other sensors.

IV. Conclusions

Situation monitoring centers for wireless infrastructure:

- Collect information about the status of the frequency range
- Centralized data processing and rapidly AP reconfiguring.
- Automatic and semi-automatic control on the wireless network.
- Ensuring the integrity of packets with telemetry from sensors.

References

1. Buryachok, V. L. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range / V. L. Buryachok, V. Yu. Sokolov // World Science. — #3 (31). — Vol. 1. — Warsaw : RS Global, 2018. — P. 9–16. DOI: 10.5281/zenodo.2528801.

2. Astapenya, V. M. Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane / V. M. Astapenya, V. Yu. Sokolov // Proceedings of the XI International Conference on Antenna Theory and Techniques, 24 May, 2017: abstracts. — Kiev : IEEE, 2017. — P. 389–391. DOI: 10.1109/ICATT.2017.7972671.

3. Sokolov, V. Yu. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network / V. Yu. Sokolov, A. Carlsson, I. Kuzminykh // Proceedings of the IV International Scientific and Practical Conference Problems of Infocommunications. Science and Technology, 10 Oct., 2017: abstracts. — Kharkiv : IEEE, 2017. — P. 564–568. DOI: 10.1109/INFOCOMMST.2017.8246463.

4. Bogachuk, I. Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers / I. Bogachuk, V. Yu. Sokolov, V. Buriachok // Proceedings of the V International Scientific and Practical Conference Problems of Infocommunications. Science and Technology, 9 Oct., 2018: abstracts. — Kharkiv : IEEE, 2018. — P. 581–585. DOI: 10.1109/INFOCOMMST.2018.8632151.

5. Rivest, R. The MD5 Message-Digest Algorithm, RFC 1321 / R. Rivest. — MIT Laboratory for Computer Science and RSA Data Security, 1992. DOI: 10.17487/RFC1321.

6. Monahan, B. HashFusion — a Method for Combining Cryptographic Hash Values / B. Monahan, L. Chen, S. Haber. —Hewlett Packard Labs, 2017. — 12 p.