Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 3, March 2019, pg.91 – 96

The Analysis of Authentication Methods of Satellite Communication Channels

Dr. Khaldoun Bsoul, Computer Science Department, Faculty of Science and Arts/Tanomah Campus
King Khalid University, Abha, KSA, Kbesoul@kku.edu.sa

Ayman Nayef ALhalaybeh, Computer Science Department, Faculty of Science and Arts/Tanomah Campus
King Khalid University, Abha, KSA, Aalhalaybeh@kku.edu.sa

Abstract: In this paper, the analysis shows that construction of systems of information security, transmitted by radio satellite communication channels, it is widely used: first of all cryptographic methods of information security, which ensure the integrity of the authentication and the confidentiality of transmitted information.
The used techniques in satellite communication systems radio channels dependent on the limitations, impose an information system, first of all in terms of the interaction protocols, ways and means of transmitting information commands.
Keywords: Communication systems, Authentication radio channels, Encryption method, Protocols, Implementation.

Introduction:

It is currently becoming more common communication system, operating by satellite communication channels.

In connection with a small satellite communication channels protectiveness great importance is the task of ensuring the confidentiality transmitted through this information channel.

Threat model analysis, acting on satellite radio communication system, possible to identify the following authentication problem:

1. Command and other information authentication radio channels transmitted in satellite communication systems [1, 2].

2. Users, have to establish the authenticity of the correspondent, which establishes a control channel.
3. Authentication program, files, stored in database, while simultaneously checking the integrity of the object of protection, perhaps the solution to these problems based on the method of block symmetric encryption, asymmetric encryption block, stream encryption methods.

The problem and solution:

Used of the techniques in satellite communication systems radio channels dependent on the limitations, impose an information system, first of all in terms of the interaction protocols, ways and means of transmitting information commands.

To date, the solution of authenticity problems associated with the development and implementation of a variety of block encryption algorithms.

To them, first of all, you must include standard DES (USA), and algorithms, based on asymmetrical transformation with public keys.

The main advantage of modular algorithms is their adaptability and ease of use in communication networks.

When you use strong data each unit received is encrypted using one and the same key. This allows you to organize as virtual, and data gram transmission, and when the block encryption is necessary provide synchronization to within the boundaries of the package.

Depending on the possible cargo is used a symmetrical, and asymmetric encryption algorithm. In the case of the using of symmetric cryptographic algorithms sources (transmitter) and the receiver must fully trust each other. In asymmetric systems transmitter and receiver many by parties, don’t trust each other [3, 4].

Regarding encryption speed (decryption) it is more preferred symmetric cryptosystem. In a hardware implementation, they provide a speed of several tens Mgb/s, and when the program – units Mgb/s.

In the class of asymmetric encryption algorithms to use of a foreign element base can be achieved within a speed of tens or hundreds Kbit/s.

In a stream cipher system, direct conversion is carried out using the ration:

$$C_i = M_i \oplus r_i \qquad (1)$$

Where: M_i – Element information sequence open a message.

r_i- The element encoding sequence.

The inverse transformation is performed on the receiving side according to the rule

$$M_i^* = (C_i^* - r_i)(mode\ _P) \qquad (2)$$

Where: $* - i$ - indicates possible presence in the resulting distorted message, effect of transfer over the communication channel or storage in characters carriers.

$P -$ Conversion module.

The founded application system produced binary conversion information (p=2). In this case the expressions (1) and (2) have the form:

$$C_i = M_i \oplus r_i \qquad (3)$$

$$M_i = C_i \oplus r_i \qquad (4)$$

The analysis showed, what and to provide theoretical or practical non decrypted Gamma-line conversion r_i it must meet the following requirements:

- Period L sequence r_i to realize theoretical non decrypted should be infinity, but to implement practical non decrypted L>L$_{pr}$ where L$_{pr}$ – limit the period L;
- The type implementation sequence r_i it should clearly defined key K$_i$ chosen from a full set of keys {K};
- According to its structural properties of sequence r_i should in limit the limit of approach to sequence, formed randomly sensor;
- The possibility of formation of one and the same implement r_i at various sets of equipment for in-line conversion under certain keys K$_i$;

The main advantage of the method are in –line conversion [5, 6, 7]:

a) The possibility of construction a theoretical and practical non cryptic system;

b) The possibility of implementing fast conversion speed (up 10 mb/s) and, as consequence, working in real time,

c) The ability of automatic rejection of false information by error propagation.

The next table summarizes the data transferred each of the above methods.

The method of appointment	Resistance method	Conversion speed	Implementation
Symmetric block transform method	Computationally fortitude	To 10 mb/s	Software hardware
Asymmetric block transform method	Computationally fortitude	100 kb/ s	software
Stream encryption method	Practically non – cryptic	Up 10 mb/ s	Software hardware

Analysis of the table shows, that give the nature and functioning of the satellite communication systems.

(The need of work in real time with the start – stop serial transmission methods and processing of nouns and restriction of the length of transmitted information block). The most suitable method, which can be used to convert the special information, it is the method of in –line conversion.

Application only by flow conversion team on the radio channel satellite communication systems, as studies have shown, make it infective because most of the information block long.

The most commonly used system with information packet, it is a method based on the formation of a secure message authentication code.

The essence of the message authentication code formation method is that for information unit joins an additional unit (authentication code) formed participation and information bit of the previous blocks, as well as time varying system parameters.

The results:

In this way, optimal terms of maximum security transmitted by satellite radio channels information, as well as the speed is a method of block line conversion with the subsequence an additional of authentication code.

Finally the analysis shows that construction of systems of information security, transmitted by radio satellite communication channels, it is widely used: first of all cryptographic methods of information security, which ensure the integrity of the authentication and the confidentiality of transmitted information.

The used techniques in satellite communication systems radio channels dependent.

References:

1. Satellite Communications, Dennis Roddy, Fourth Edition.
2. Fundamentals of Satellite Communication, k. N. Raja Rao, 2004.
3. Everyone Communicates, Few Connect: What the Most Effective People Do Differently, *by John C. Maxwell, 2010.*
4. Essential Interviewing: A Programmed Approach to Effective Communication, *by David R. Evans, Margaret T. Hearn, Max R. Uhlemann and Allen E. Ivey, 2010*.
5. Mastering Communication at Work: How to Lead, Manage, and Influence, *by Ethan F. Becker and Jon Wortmann, 2009.*
6. Communication: The Key to Effective Leadership, *by Judith A. Pauley, 2009*
7. The Art and Science of Communication: Tools for Effective Communication in the Workplace, *by P. S. Perkins and Les Brown, 2008*.
8. Safwan Al Salaimeh, Mohammad Bani Younes, 2014// Functional Structure of Special Computerized Information System. Journal of Environmental Science, Computer Science and Engineering & Technology. December 2014-February Sec. B; Vol.4.No.1, 52-56. 2012,
9. Mohammad Bani Younes, Safwan Al Salaimeh, // The Optimal Allocation of Simulation Resource in Logistics Information Systems. International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 2, February 2015.
10. Safwan al Salaimeh, Zeyad Al Saraireh, Jawad Hammad Al Rawashdeh, // Design a Model of Language Identification Tool . International Journal of Information & Computation Technology. Volume 5, Number 1 , pp. 11-18. 2015.
11. Khaled Batiha, Safwan Al Salaimeh, (2016)// Development sustainable algorithm optimal resource allocation in information logistics systems. International journal of computer applications (IJCA), March 2016 edition. USA.

12. K. J. Astrom, Computer Aided Modeling, Analysis and Design of Control Systems-A Perspective, Department of Automatic Control, Lund Institute of Technology, S-220.
13. H. Raza, Zhigang Xu., Bingen Yang, Modeling and control design for a computer-controlled brake system, IEEE Transactions on Control Systems Technology (Volume: 5, Issue: 3, May 1997),
14. Christian Schmid, COMPUTER-AIDED CONTROL SYSTEM ENGINEERING TOOLS, CONTROL SYSTEMS, ROBOTICS, AND AUTOMATION – Vol.XXI - Computer-Aided Control System Engineering Tools –
15. Ivane Gorgidze, Tamar Lominadze, Maka Khartishvili and Ketevan Makhashvili, Information and Computer Technology, Modeling and Control, Nova Science Publishers, 2017.