Analysis of wireless network security systems problems and those solutions

https://doi.org/10.31713/MCIT.2020.31

Didmanidze Ibraim
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia
ibraimd@ukr.net

Beridze Zebur
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia

Zaslavski Vladimir
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

Didmanidze Didar
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia

Abstract – **In the people's lives wireless networks play a big role. It is necessary to understand the basic concept of wireless networks, to consider the security issues related to them, and then observe how they work and what benefits they can bring in different cases. In this regard the given research paper presents the fundamental principles of security as well as related open questions. It reviews the security issues of the wireless networks. Security of protocols of wireless network routing has become an urgent necessity to stimulate the network launching and expand the area of its usage. Therefore, the presented research paper proposes and defines different solutions and concepts for security.**

Keywords – Wireless network security, wireless technologies, information transfer area, wireless global network, wireless networks.

INTRODUCTION

Today, the popularity of wireless technology has several reasons. A significant reduction in the prices of wireless devices allows a service provider to significantly reduce the cost of wireless service and make it more accessible to a user. Like usual networks, based on the use of wires, the wireless networks provide information between computer devices as well. This information can be presented in a variety of ways: by e-mail, WEB-page, database records, video stream or voice message. In most cases wireless networks transmit data through e-mail and files. In connection with the improvement of wireless networks' quality, it is possible to transfer video signals as well as to provide a telephone connection.

Organizations avoid using wireless networks without an adequate security. Security issues in wireless networks represent an important obstacle for the widespread adaptation of such networks. Appropriately, the corresponding wireless network security is an important area, which requires a response in the case of the networks extensive usage. It is necessary for the researchers of the given sphere to identify the open issues and provide appropriate solutions for these problems. Such attempts would make the wireless network safer.

Security is a very important issue for wireless networks, because communication signals can be easily received in an environment. Therefore, companies and individual customers have to recognize the potential problems and take appropriate measures.

Main part. Wireless networks like transmitters, that ensure interaction between users, servers, and databases, use radio waves of infrared range. This area of information transfer is invisible to humans. Today, most manufacturers integrate the Network Interface Cards (NIC), known as network adapters, and antennas into computer devices so that they are invisible to consumers. All this makes the wireless device more convenient to use. The tendency regarding the wide-scale usage of wireless networks is more and more being experienced. Different wireless interfaces available in nowadays reality give the possibility to use network services. For example, the user can work with email and surf websites independently from where the one might physically be. Wireless networks provide the users with possibility to expand the working space and relevantly get much preferences. Majority of users can easily use common internet connections without installing any cabling systems, via personal computers and notebooks [1].

Any system, which needs protection, has its weaknesses or deficiencies, which partially or all together can be chosen as a target by an attacker. Accordingly, one of the approaches of security mechanism development is an analysis of all the threats and alleged attackers, which are facing the system with shortcomings. The security mechanism should provide the system security, considering all the threats, attackers and shortcomings [2].

An attack is an attempt to circumvent a security control mechanisms of a computer. The attack may be resulted in leakage, change or cancel data. The examples of attacks are: a data leakage from a transferred environment and devices, an acceptance of illegal privileges, wrong data entry, data modification, analysis of network flow, etc.

Recently the security and the quality of service in wireless networks have become the issues of outmost interest and the

subjects of active investigation, that is conditioned by the increasing demand of support for data package transfer. Organizations will avoid using wireless networks unless adequate security is insured. Security issues tend to be the critical obstacle in the process of wide range adaptation of these networks. Relevantly the security of the types of networks is an important aspect that require response if the networks are widely used. It is necessary open questions to be identified and properly solved by the researchers in the given field. Each such attempt makes wireless network slightly more secured. The objective of the presented research paper is to elaborate a number of measures that will increase the security level of wireless networks and manage remote jobs.

Wireless network security is significantly different from their wired analogue security, that is caused by the nature of the physical environment. During the process of establishing the connection with wireless environment the transmitted and received signals travel in the air. Appropriately, any node, that is located in the sender node transmission range and knows the operating frequency and other physical-level attributes (modulation, coding, etc.), is potentially able to decipher the signal in such a way that the sender or an expected recipient would know nothing about the intrusion. Often, when the effective protection mechanisms are activated in an access point, an existing threat is posed by the possibility of switching the Access Point (rogue access point). This point is considered to be an unauthorized access point connected to the network.

The safety and service quality of wireless networks has become a subject of considerable and active research over the past few years, what is caused by a growing requirement for supporting the transfer of data packages. Any node which is located in the transmission range of a delivery node and which knows the operating frequency and other physical attributes (modulation, encoding, etc.) can potentially encrypt the signal so that a sender or an alleged recipient will not know anything about that interference. However, such interference in cable networks can occur if an attacker has an access to physical means of transmission (wires, fibers, etc.) what requires the accession to the facility. As wireless networks are not dependent on infrastructure based resources, such as power stable source, high frequency, continuous connection or unchanging routing, they can be easily attacked.

For example, an experienced hacker or accidentally snooper (a person who likes spying) can easily track the unwanted packages and open the data in it, using the software means. For example, snoopers located hundreds of miles away from the building, where a wireless local area network is functioning, are capable of looking for all transactions in a wireless network. Of course, the main danger is the fact that as a result of such an attack, some people can have access to important information such as usernames and passwords, credit card numbers and other.

CONCLUSION

An experienced hacker or accidentally snooper can easily track the unwanted packages and open the data in it, using the software means. Of course, the main danger is the fact that as a result of such an attack, some people can have access to important information such as usernames and passwords, credit card numbers and other.

The solution to this problem at least refers to the encryption of information that should be transferred between wireless devices and base stations. During the encryption process, data bits are changed with the help of secret keys. As the keys are secret, the hacker cannot decrypt data. Therefore, due to the use of effective encryption mechanisms, the data protection can be strengthened.

Wireless network, also, can be protected from outside radio signals by ensuring the ability to resist them in a building.

The research deals with the all above mentioned issues.

REFERENCES

[1] Didmanidze I., Beridze Z., Geladze N. Routing Security Enchantement in Wireless Local Area Networks. XXX international conference PROBLEMS OF DECISION MAKING UNDER UNCERTAINTIES (PDMU-2015). ABSTRACTS. August 14-19, 2017, Vilnius, Lithuania. p. 39.

[2] Didmanidze I., Beridze Z. The Analysis of Wireless Network Security. 12th International Conference THEORETIKAL AND APPLIED ASPECT OF PROGRAM SYSTEMS DEVELOPMENT. TAAPSD'2015. Proceeding. 23-26 December 2015 y. Kiev. p. 206-207.