საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 11, №2, 2017
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 11, no. 2, 2017

Informatics

Automatized Design of the Logic and Structured Process of Wireless Local Area Networks Monitoring

Otar Shonia*, Ioseb Kartvelisvili*, Zebur Beridze*, Ibraim Didmanidze, Levan Kolbaia***

* *Faculty of Informatics and Control Systems, Georgian Technical University, Tbilisi, Georgia*
** *Faculty of Physics and Mathematics, Batumi Shota Rustaveli State University, Batumi, Georgia*

(Presented by Academy Member Archil Prangishvili)

ABSTRACT. Components and systems of the wireless local area networks are presented in the study. Most common threats related to the use of the wireless local area networks are described. In order to increase the safety of routing in the wireless local area network a new method is elaborated. The wireless local area network is presented schematically where certain connections between the authentication server and network devices are used. *© 2017 Bull. Georg. Natl. Acad. Sci.*

Key words: Wireless local networks, monitoring of network security, access points, routers

The wireless local area networks fully satisfy the requirements, which are set towards the wireless connections for provision of communication within the building. The wireless local networks consist of the same components as the traditional local wire ethernet networks, and their protocols are similar to the Ethernet protocols. The difference is only that at arrangement of the local area networks, it is not necessary to use the wires. The users of the wireless local area networks work with many devices – PC, notebooks etc. Usage of wireless local area networks for interconnection of devices is effective for the PC because it excludes the necessity of laying the wires. The main components of the wireless local area networks are: radio card of the network interface, access points, routers and transponder. Radio card of the network interface is realized at 802.11 standards. These radio-boards work at one physical level – 802.11a or 802.11b/g. The radio card which is compatible with the wireless local area network will realize the version of the standard. The radio-boards of the wireless local area network, which provide and realize different versions of the mentioned standard and have high level capacity of interaction, become more and more distributed.

The access point consists of the radio card and provides connection between the certain user device and wire board of the network interface, which provides the interaction of the distributed system, such as Ethernet. System software of the access

points conditions the interaction between the parts of the wireless local area network and distributive system of the access points. It differentiates the access points by the management quality and safety functions.

Router, as the name shows, sends information packets from one network to another, and select the next best channel in the nearest point to the transmission packet. The routers use the titles of Internet Protocol (Internet Protocol, IP) packets and routing tables. Also, they use the internal Protocols to define the best route for transmission of each packet. The router of the wireless local area network enables the Ethernet multiport router to function as built-in access point allowing combination of the Ethernet and wireless networks. The typical router of the wireless local area network has 4 ports, therefore it can function as a server printer. All above mentioned allows the wireless network users to receive and send packets to multiwire networks as if they are connected to one of them [1].

The routers use the Network Address Translation (NAT), which allows number of networking devices simultaneously to use one IP address, presented by the Internet Service Provider (ISP). The routers also use the dynamic host configuration protocol (DHCP) for services of all devices, which can give individual IP addresses to every device. NAT and DHCP together enable several network devices (such as PC, notebooks and printers) to work in Internet by using one IP address.

To expand the range of action in the current infrastructure, the transponder, simply regenerates the signals which are distributed in the network. The transponder of the wireless local area network does not have a physical contact to any part of the network. It receives the radio signals from the access point and transmits the frames of received data repeatedly. All these, gives the opportunity to the transponder, which is located between the access point and the remote user to function as frame retranslation that transmits from user to the access point and vice-versa. Therefore, wireless transponders are the effective solution for elimination of problems of signal degradation due to the radio disturbances.

Safety is the issue of key importance for the wireless local area networks, since the communication signals distributed in the environment are available to be intercepted. Therefore, the companies and individual users must be aware of potential problems and take relevant measures. Any system, which needs the protection, has its weaknesses and malfunction, which will be selected partially or entirely as an object by the cyberpunk. Accordingly, one of the approaches for creation of the system security is to analyze those threats and expected attacks the system faces, taking into consideration that the system has failures. The security mechanisms must provide the safety of the system taking into consideration given threats, attacks and malfunction [2].

For instance, any intruder, using different software facilities, can easily find the unsecured packets of the wireless network and fully open the data existed in it. For example, unauthorized persons, being in distance of several hundred meters from the building, where the wireless local area network functions, are able to find all transactions that are made in the part of wireless network. The main risk is that via attacks, someone can obtain such important information as names and passwords of users, numbers of credit-cards etc.

Similarly, any person who is near the building is able, without any effort to monitor the systems within the wireless local network, if the preliminary safety measures have not been taken. E.g. anyone, in the vehicle nearby the building, is able to connect to one of the base stations located in the building. If the necessary safety measures have not been taken, such person is able to access the server and systems which terminate in the corporate network. Unfortunately, most of the companies, when arranging the wireless local network, use the default configuration of the base stations and cannot provide the necessary safety

measures which can predefine the smooth interaction of the systems with server.

Frequently, when the security mechanisms are in action, the existed risk is the ability of switching the roguery access point. Such access point is deemed as unauthorized access point, connected to the network. For instance, any person from staff may purchase the access point and without consideration of safety measures install it in his/her office. Also, the hacker can install the access point in the building and connect the unsecured access point to the corporate network, intentionally. In the roguery access point, as a rule, there is no encoding system activated. Therefore, it is an open door for everyone who intends to have the access to the corporate network from outside of the building. So, the companies must always check the presence of roguery access points. This is a topical problem, even if the wireless network is installed because somebody can connect the roguery access point to the wired network.

By using the authentication and encryption mechanisms, the security of the wireless network is increasing, but the experienced hackers find the weaknesses because they know how the network protocols work. Especially dangerous is the "man-in-the-middle attacks". The hacker places the fictive devices between the legal user and wireless network. For example, at standard "man-in-the-middle" attack, the address resolution protocol ARP is used, which is used in all TCP/IP (transmission Control Protocol/ Internet Protocol) networks. Hacker, having the software means, is able to control the wireless network.

"Denial of Service", DoS – is the attack, which makes the wireless network useless or its operation is blocked. All those who arrange the wireless network will consider possibility of such attack. It is necessary to think over the situation when the network becomes inaccessible for unlimited time. The severity of the DoS attack depends on the results of the wireless network disabling. In difference with ordinary networks, there are more risks of attacks in the wireless local networks, caused by the following reasons: there is no filter in the wireless networks, which may be used for protection against the attacks; there is no server, which has the increased reliability; the wireless networks are characterized with permanent motion of objects and in addition, there are no physical channels, because of the absence of such channels, information is transmitted ethereal, which is also threat because the attacks start from the eavesdropping of the channels. Due to the abovementioned, in order to increase the security of the routing in the wireless local area network, a new method is elaborated. It is necessary to use the authentication server, by which the processes of connection among the network devices will be monitored and entered into the database. It is also necessary to use the double-sided authentication between the network devices, which provides the solution of many problems, related to the safety. During the double-sided authentication, the wireless user and wireless network confirm their identity to each other.

In private companies and enterprises, the wireless local area network will consist of several access points and wire routers. Combination of the access point and wire router can change the wireless local area network router and it is a less expensive solution than purchase of the wireless local network router. It is also necessary that several wireless users (PCs or notebooks) to be connected to any certain access points and in no case, random finding of the access points at information transmission. In addition, the IP address for all network devices should be designated individually by the administrator and in no case to submit, the IP address randomly to the users of the local network via DHCP protocol (Fig 1).

Most frequently, the wireless local area networks are created in accordance with 802.11 standards. IEEE 802.11 standard describes general management protocol in the transmission area (Media Access Control, MAC) and several physical levels of the wireless local networks. The working group developing the IEEE 802.11 standard actively works for improvement of features and safety of the wireless local net-

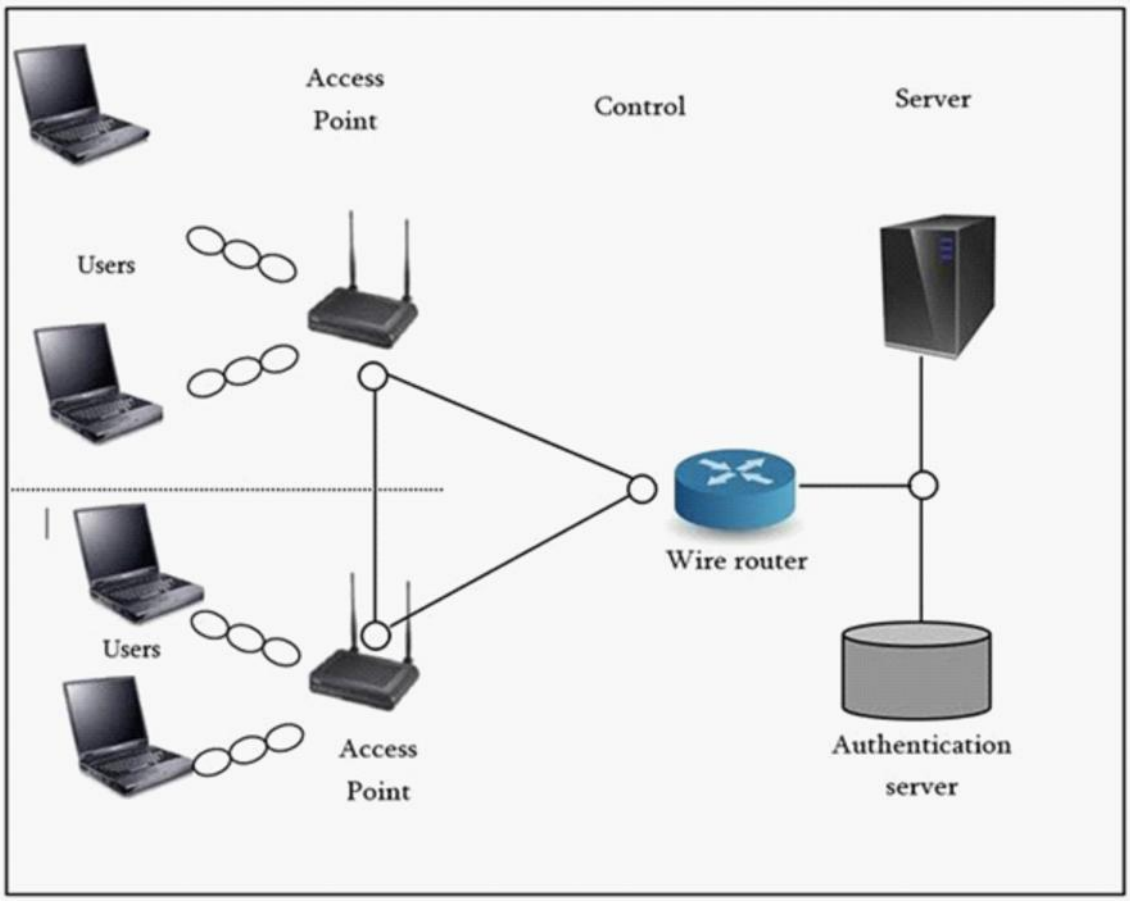

Fig. 1. Wireless local area network, where the authentication server and certain connections are used.

works. Each network device has its unique MAC address and by checking the MAC and IP addresses, before information transmission, for identification of the devices, the double-sided authentication should be made.

Let us introduce the symbols. Let $P_{\{i\}}$ be the set of users and $W_{\{j\}}$ the set of access points.

$$i=\overline{1,n} \text{ and } j=\overline{1,m},$$

where, n – is the number of users in the control zone, and m - is the number of access points.

For each set introduce the status $P_{\{i\}Status}$ and $W_{\{j\}Status.}$

If $P_{\{i\}Status}$ =1, the user checks the identity of the access point, if $P_{\{i\}Status}$ =2, the authentication is made successfully if $P_{\{i\}Status}$ =0, the authentication is un-successful and the connection is interrupted.

Similarly, if $W_{\{j\}Status}$.=1, the access point checks the identity of user, if $W_{\{j\}Status}$.=2, the authentication is made successfully if $W_{\{j\}Status}$.=0, the authentication is unsuccessful and the connection is interrupted.

For each user the MAC address of the access point to be connected is defined.

For beginning $P_{\{i\}Status}$=1

If $P_{\{i\}MAC} = W_{\{j\}MAC,}$ then $P_{\{i\}Status}$=2;

If $P_{\{i\}MAC} * W_{\{j\}MAC}$, then $P_{\{i\}Status}$=0

$i=i+1;\ \ j=j+1$

Where, $P_{\{i\}MAC}$ is the MAC address of the access point defined for the user, and $W_{\{j\}MAC}$ is the MAC Address of the access point.

For beginning $W_{\{i\}Status}$=1

If $W_{\{i\}IP} = P_{\{j\}IP}$, then $W_{\{i\}Status}$=2;

if $W_{\{i\}IP} * P_{\{j\}IP}$, then $W_{\{i\}Status}$=0

$i=i+1;\ \ j=j+1$

In the mentioned processes if any of the network device try to change its MAC and IP address, or new address detected, authentication server will take the relevant measures and disconnect the network device from the network and notifies the network administrator about it.

After successful implementation of double-sided authentication, the information will be transmitted. However, before transmission, user's switch (PC or notebook) will get the access to media or we will introduce the distributive function of coordination. Support of the mentioned mode is necessary because it provides various accesses to the essential control and eliminates the collision. During the work of the distributive function of coordination, the stations come into competition for access to environment and try to transmit the information, the rest of them wait for the channel release.

For access to the environment, the station checks the value of network distribution vector (N), which is the counter placed on all stations, the value of which corresponds to the time for transmission of the previous information frame. Before the frame is transmitted, according to its volume, the station counts the time necessary for transmission and speed of data transmission in the network. The station places the values at the top of the frame. When the station receives the frame, it checks the value and uses it as a basis for its N. Through this process, the backup of the environment used by the transmission station is ensured. The main aspect of this mode is the backward timer, which is used by the station if the transmission environment is busy. When the channel is used by other station, the station that needs transmission will standby during the certain time, and then try again to get access to the environment. Therefore, it will exclude the situation when several stations start the data transmission simultaneously. The backward timer significantly decreases the collisions and number of repeated transmission, especially when the number of active users is large.

When using the local area networks, which is based on the radio channels, during the data transmission, the transmission station is not able to detect the occurrence of collision in the environment because it has no ability to use the receiver during the data transmission. Therefore, the receiver station should send the confirmation that it has not detected the error in the received frame. If the transmission station does not receive the confirmation, it decides that the collision occurred or the frame was damaged due to the radio interference and transmits repeatedly. By the initiative of the administrator or in automated mode with automated system it is necessary to scan the network periodically, which reveals the drawback of the network and logic and structured process of the security monitoring is performed. Network scanning gives the opportunity to organize the inspection of the computer network of any size and the process of information collection. During the scanning process it is possible to scan both individual IP address and all IP addresses, as well as, to scan with indication of certain interval [3].

During the scanning process it is possible to control the entire process and individual hosts (IP addresses). During the process it is possible to suspend or terminate the scanning process of all or selected hosts. After the scanning process is completed, it is possible to save the results of the process in the special database, with indication of the date and time, which may be recalled at any time. Also, it is possible to make reports at any time. All results will be re-

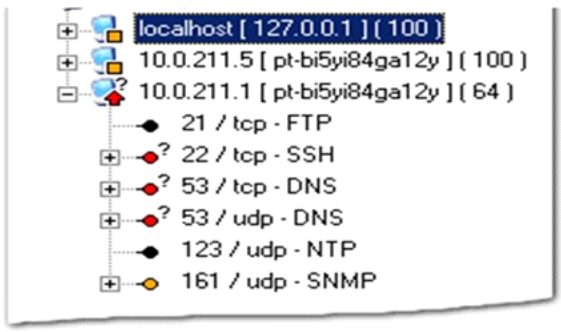

Fig. 2. Result of the Network Scanning

flected in the special panel. All results of scanning are imaged with different colors, according to which the level of drawback can be evaluated at first glance (Fig. 2).

If there is much "red color" in the markings of different colors – it is bad, much "yellow" – not so bad and much 'green" – practically normal. The best result is when there are no colored markings.

The markings are presented quite clearly; the "scanning tree" has three levels (host-port-drawback). If the service has a serious drawback, then its icon is red and accordingly, the icon of its corresponding host will be red, also.

At final phase the network administrator will make the relevant response based on the results of scanning.

Security is the most important issue for wireless local area network, because widespread communicational signals in environment are available for everyone. Therefore, companies and individual users must recognize potentially existing problems and take proper measures to ensure the system safety. Any system that needs protection has weaknesses and failures, and all these must inevitably be considered for proper operation of the system and avoid the expected dangers in future.

ინფორმატიკა

უსადენო ლოკალური ქსელების უსაფრთხოების მონიტორინგის ლოგიკური და სტრუქტურირებული პროცესის ავტომატიზებული დაპროექტება

ო. შონია,* ი. ქართველიშილი*, ზ. ბერიძე*, ი. დიდმანიძე, ლ. კოლბაია***

** საქართველოს ტექნიკური უნივერსიტეტი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტი, თბილისი, საქართველო*
*** შოთა რუსთაველის სახ. ბათუმის სახელმწიფო უნივერსიტეტი, ფიზიკისა და მათემატიკის ფაკულტეტი, ბათუმი, საქართველო*

(წარმოდგენილია აკადემიის წევრის ა. ფრანგიშვილის მიერ)

ნაშრომში წარმოდგენილია უსადენო ლოკალური ქსელების კომპონენტები და სისტემები. მოყვანილია მათი გამოყენებასთან დაკავშირებული საფრთხეების ყველაზე გავრცელებული ფორმები და თითოეული მათგანი დახასიათებულია თავისი თვისებებით. უსადენო ლოკალურ ქსელში მარშრუტიზაციის უსაფრთხოების ამაღლების მიზნით შემუშავებულია ახალი მეთოდი. სქემატურად წარმოდგენილია უსადენო ლოკალური ქსელი, სადაც გამოყენებულია აუტენტიფიკაციის სერვერი და ქსელურ მოწყობილობებს შორის კონკრეტული შეერთებები.

REFERENCES

1. Shonia O., Nareshelashvili G., Kartvelishvili I. (2009) Security of Wireless Networks. Georgian Technical University, Tbilisi (in Georgian).
2. Merrit M., Pollino D. (2004) Bezopasnost', bezprovodnykh setei. M. (in Russian).
3. Mishra A. (2008) Security and Quality of Service in Add Hoc Wireless Networks. Cambridge University Press.

Received February, 2017