უსადენო ლოკალური ქსელების უსაფრთხოების მონიტორინგის ლოგიკური და სტრუქტურირებული პროცესის ავტომატიზებული დაპროექტება

ოთარ შონია[1], იოსებ ქართველიშვილი[1], ზებურ ბერიძე[2],
იბრაიმ დიდმანიძე[2], ლევან ყოლბაია[1]

1-საქართველოს ტექნიკური უნივერსიტეტი
2-ბათუმის სახელმწიფო უნივერსიტეტი

რეზიუმე

წარმოდგენილია უსადენო ლოკალური ქსელების კომპონენტები და სისტემები. მოყვანილია უსადენო ლოკალური ქსელების 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 აუტენთიფიკაციის სერვერი და ქსელურ მოწყობილობებს შორის კონკრეტული შეერთებები.

საკვანძო სიტყვები: უსადენო ლოკალური ქსელები. ქსელების უსაფრთხოების მონიტორინგი. წვდომის წერტილები. მარშრუტიზატორები.

1. შესავალი

უსადენო ლოკალური ქსელები სრულიად აკმაყოფილებს მოთხოვნებს, რომლებიც წაყენებულია უსადენო შეერთებისთვის შენობის ფარგლებში კავშირის დასამყარებლად. უსადენო ლოკალური ქსელები შედგება ისეთივე კომპონენტე-ბისაგან, როგორისგანაც ტრადიციული ლოკალური სადენიანი Ethernet-ის ქსელები. ასევე ჰგვანან მათი პროტოკოლები Ethernet--ის პროტოკოლებს. განსხვავება მხოლოდ იმაშია, რომ უსადენო ლოკალური ქსელების გამართვის დროს სადენების გამოყენება აუცილებელი არ არის. უსადენო ლოკალური ქსელების მომხმარებლები მუშაობენ ბევრ მოწყობილობასთან - პერსონალურ კომპიუტერებთან, ნოუთბუქებთან და ა.შ. მოწყობილობების ერთმანეთთან დასაკავ-შირებლად უსადენო ლოკალური ქსელების გამოყენება პერსონალური კომპიუტერებისათვის ეფექტურია იმიტომ, რომ გამორიცხავს სადენების გაყვანის აუცილებლობას.

უსადენო ლოკალური ქსელის ძირითადი კომპონენტებია: ქსელის ინტერფეისის რადიოპლატა, წვდომის წერტილები, მარშუტიზატორები და განმმეორებლები. ქსელის ინტერფეისის რადიოპლატა რეალიზებულია 802.11 სტანდარტზე. ეს რადიოპლატები ჩვეულებრივ მუშაობს ერთ ფიზიკურ დონეზე - 802.11ა ან 802.11ბ/გ. რადიოპლატამ, რომელიც შეთავსებულია უსადენო ლოკალურ ქსელთან, რეალიზება უნდა გაუკეთოს სტანდარტის ვერსიას. უსადენო ლოკალური ქსელის რადიოპლატები, რომლებიც უზრუნველყოფს და რეალიზაციას უკეთებს აღნიშნული სტანდარტის სხვადასხვა ვერსიას და გააჩნია ურთიერთქმედების მაღალი დონის შესაძლებლობა, ხდება უფრო და უფრო გავრცელებადი [1].

2. ძირითადი ნაწილი

წვდომის წერტილი შედგება რადიოპლატისაგან და უზრუნველყოფს კავშირს უსადენო ლოკალური ქსელის ცალკეულ სამომხმარებლო მოწყობილობასა და ქსელის ინტერფეისის მავთულიან პლატას შორის, რაც უზრუნველყოფს განაწილებულ სისტემასთან ურთიერთქმედებას, როგორიც არის Ethernet. წვდომის წერტილების სისტემური პროგრამული უზრუნველყოფა განაპირობებს უსადენო ლოკალური ქსელის ნაწილებსა და წვდომის წერტილების განაწილებულ სისტემას შორის ურთიერთქმედებას. იგი წვდომის წერტილებს დიფერენცირებას უკეთებს მმართველობის ხარისხით და უსაფრთხოების ფუნქციებით.

მარშრუტიზატორი, სახელწოდების მიხედვით თუ ვიმსჯელებთ, გადასცემს ინფორმაციულ პაკეტებს ერთი ქსელიდან მეორეში, არჩევს რა შემდგომ საუკეთესო არხს უახლოეს წერტილში პაკეტის გადასაცემად. მარშრუტიზატორები გამოიყენებენ ინტერნეტ პროტოკოლის (Internet Protocol, IP) პაკეტის სათაურებს და მარშრუტიზაციის ცხრილებს. აგრეთვე იყენებენ შიდა პროტოკოლებს თითოეული პაკეტის გადასაცემად საუკეთესო გზის განსაზღვრისათვის. უსადენო ლოკალური ქსელის მარშრუტიზატორი ანიჭებს შესაძლებლობას Ethernet-ის მრავალპორტიან მარშრუტიზატორს შეასრულოს ჩაშენებული წვდომის წერტილის ფუნქციები. ამის წყალობით შესაძლებელია Ethernet-ისა და უსადენო ქსელების კომბინირება. უსადენო ლოკალური ქსელის ტიპიურ მარშრუტიზატორს გააჩნია 4 პორტი, ამიტომ მას აგრეთვე შეუძლია შეასრულოს სერვერის ბეჭდვის ფუნქცია. ყოველივე ეს უსადენო ქსელის მომხმარებლებს აძლევს საშუალებას ისევე მიიღოს და გააგზავნოს პაკეტები ბევრ მავთულიან ქსელში, თითქოს ისინი შეერთებულნი არიან ერთ-ერთ მათგანში.

მარშრუტიზატორები იყენებს ქსელების მისამართების ტრანსლაციის პროტოკოლებს (Network address translation, NAT), რომელიც ბევრ ქსელურ მოწყობილობას აძლევს საშუალებას ერთობლივად გამოიყენოს ერთი IP მისამართი, წარმოდგენილი ინტერნეტ მომსახურების პროვაიდერის მიერ (Internet service provider, ISP). მარშრუტიზატორები აგრეთვე იყენებენ დინამიკური კვანძის კონფი-გურირების პროტოკოლს (dynamic host configuration protocol, DHCP) ყველა მოწყობილობის მომსახურებისათვის, რომელიც იძლევა საშუალებას ყველა მოწყობილობას წარმოუდგინოს ცალკეული IP მისამართები. ერთობლივი ძალებით NAT და DHCP შესაძლებელს ხდის რამოდენიმე ქსელური მოწყობილობის (როგორიცაა, პერსონალური კომპიუტერები, ნოუთბუქები და პრინტერები) მუშაობას ინტერნეტში მხოლოდ ერთი IP მისამართის გამოყენებით.

განმმეორებელი, არსებულ ქსელურ ინფრასტრუქტურაში, მოქმედების რადიუსის გასაფართოვებლად, უბრალოდ რეგენერირებას უკეთებს სიგნალებს, რომლებიც ვრცელდება ქსელში. უსადენო ლოკალური ქსელის განმმეორებელს არ გააჩნია ფიზიკური კონტაქტი რომელიმე ქსელის ნაწილთან. ის იღებს წვდომის წერტილისაგან რადიოსიგნალებს და განმეორებით გადასცემს მიღებულ მონაცემთა ფრეიმებს. ყოველივე ეს განმმეორებელს, რომელიც განთავსებულია წვდომის წერტილსა და მოცილებულ მომხმარებელს შორის, აძლევს იმის საშუალებას, რომ იფუნქციონიროს, როგორც ფრეიმების რეტრანსლატორმა, რომელიც გადასცემს მომხმარებლიდან წვდომის წერტილისაკენ და პირიქით. აქედან გამომდინარე, უსადენო განმმეორებლები

წარმოადგენს ეფექტურ გადაწყვეტილებას რადიოხარვეზებით გამოწვეული სიგნალების დასუსტების პრობლემის გადასაჭრელად.

უსადენო ლოკალური ქსელებისათვის უსაფრთხოება უაღრესად მნიშვნელოვანი საკითხია, ვინაიდან გარემოში გავრცელებული საკომუნიკაციო სიგნალები ხელმისაწვდომია დასაჭერად. აქედან გამომდინარე, კომპანიებმა და ინდივიდუალურმა მომხმარებლებმა უნდა შეიცნონ პოტენციურად არსებული პრობლემები და მიიღონ შესაბამისი ზომები. ნებისმიერ სისტემას, რომელსაც დაცვა სჭირდება, გააჩნია სისუსტეები ან ხარვეზები, რომელთა ნაწილს ან ყველას ერთად ამოირჩევს თავდამსმხმელი ობიექტად. შესაბამისად, სისტემის უსაფრთხოების მექანიზმების შექმნის ერთ-ერთ მიდგომას წარმოადგენს განხილვა იმ საფრთხეებისა და სავარაუდო თავდასხმებისა, რომელთა წინაშე დგას სისტემა, იმის გათვალისწინებით, რომ სისტემას ხარვეზები გააჩნია. უსაფრთხოების მექანიზმებმა უნდა უზრუნველყონ სისტემის უსაფრთხოება მოცემული საფრთხეების, თავდასხმებისა და ხარვეზების გათვალისწინებით[2].

მაგალითად, ნებისმიერ ბოროტგანმზრახველს სხვადასხვა პროგრამული საშუალებების გამოყენებით შეუძლია ადვილად მოიძიოს უსადენო ქსელის დაუცველი პაკეტები და მთლიანად გახსნას მასში არსებული მონაცემები. მაგალითად, გარეშე პირებს, რომლებიც იმყოფებიან რამდენიმე ასეული მეტრით დაშორებით შენობიდან, სადაც ფუნქციონირებს უსადენო ლოკალური ქსელი, შესწევთ ძალა მოიძიონ ყველა ტრანზაქცია, რომელიც სრულდება უსადენო ქსელის ნაწილში. ძირითადი საფრთხე მდგომარეობს იმაში, რომ შეტევების შედეგად ვიღაცას შეიძლება ხელში ჩაუვარდეს ისეთი მნიშვნელოვანი ინფორმაცია, როგორიცაა მომხმარებლების სახელები და პაროლები, კრედიტ-ბარათების ნომრები და სხვა.

ანალოგიურად ნებისმიერს, რომელიც იმყოფება შენობის შორიახლოს, ყოველგვარი ძალისხმევის გარეშე, შეუძლია მონიტორინგის ჩატარება უსადენო ლოკალურ ქსელში არსებული სისტემების მიმართ, თუ არ არის მიღებული სიფრთხილის წინასწარი ზომები. მაგალითად, ვინმეს, რომელიც იმყოფება შენობის მახლობლად მდგარ ავტომობილში, შეუძლია მიებას შენობაში განლაგებული საბაზისო სადგურებიდან ერთ-ერთს. თუ არ არის მიღებული საჭირო დაცვის საჭირო ზომები, ასეთ პირს შეუძლია შეაღწიოს სერვერზე და სისტემებში, რომლებიც სრულდება კორპორატიულ ქსელში. სამწუხაროდ, კომპანიების უმრავლესობა უსადენო ქსელების გამართვის დროს იყენებს საბაზისო სადგურების კონფიგურაციას, რომელიც თავიდანვეა დაყენებული (default) და ვერ უზრუნველყოფს უსაფრთხოების საჭირო ზომებს, რაც წინასწარ განსაზღვრავს სისტემების სერვერთან დაუბრკოლებელ ურთიერთქმედებას.

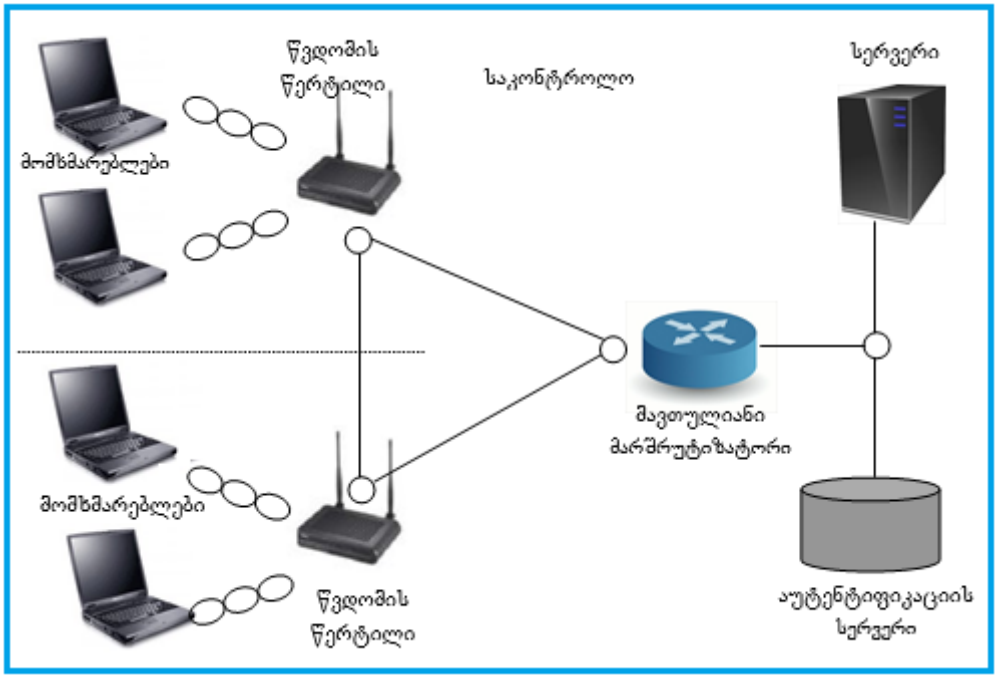
ხშირად, როდესაც წვდომის წერტილში ამოქმედებულია დაცვის მექანიზმები, არსებულ საფრთხეს წარმოადგენს მიდგმული წვდომის წერტილის (roguee Access point) ჩართვის შესაძლებლობა. ასეთი წერტილი ითვლება არაავტორიზებულ წვდომის წერტილად, რომელიც მიერთებულია ქსელში. მაგალითად, რომელიმე მომსახურე პერსონალს შეუძლია შეიძინოს წვდომის წერტილი, არ გაითვალისწინოს ქსელის უსაფრთხოების ნორმები და დააყენოს იგი თავის ოფისში. ასევე ჰაკერს შეუძლია შენობაში განათავსოს წვდომის წერტილი, განზრახ შეაერთოს დაუცველი წვდომის წერტილი კორპორატიულ ქსელში. მიდგმულ წვდომის წერტილში, როგორც წესი, არ არის

აქტივირებული დაშიფვრის სისტემა. აქედან გამომდინარე, იგი წარმოადგენს ყველასათვის ღია კარს, ვინც კი მოინდომებს შენობის გარედან შეაღწიოს კორპორატიულ ქსელში. ამიტომ კომპანიებმა ყოველთვის უნდა შეამოწმონ მიდგმული წვდომის წერტილების არსებობა. ეს პრობლემა აქტუალურია დამოუკიდებლად იმისა, დაყენებულია უსადენო ქსელი თუ არა, ვინაიდან ვინმეს შეუძლია მიდგმული წვდომის წერტილი მიუერთოს სადენიან ქსელს.

აუტენტიფიკაციისა და დაშიფვრის მექანიზმების გამოყენების წყალობით იზრდება უსადენო ქსელების უსაფრთხოება, მაგრამ გამოცდილი ჰაკერები ძებნიან სუსტ მხარეებს, იციან რა, თუ როგორ მუშაობს ქსელის ოქმები. განსაკუთრებულ საშიშროებას წარმოადგენს ,,ადამიანი შუაში" (man-in-the-middle attacks) სახეობის შეტევები. ჰაკერი განათავსებს ფიქტიურ მოწყობილობას ლეგალურ მომხმარებლებსა და უსადენო ქსელს შორის. მაგალითად, სტანდარტული ,,ადამიანი შუაში" სახეობის შეტევის განხორციელების დროს გამოიყენება მისამართების გარდამქმნელი პროტოკოლი (Adress resolution protocol, ARP), რომელიც გამოიყენება ყველა TCP/IP (Transmission Control Protocol/Internet Protocol - გადაცემის მართვის პროტოკოლი/ინტერნეტ პროტოკოლი) ქსელში. ჰაკერს, შეიარაღებულის პროგრამული საშუალებებით, ARP-ს გამოყენებით შეუძლია დაამყაროს კონტროლი უსადენო ქსელზე.

,,მომსახურებაზე უარი" სახეობის შეტევა (Denial of service, DoS) - ეს არის თავდასხმა, რის შედეგადაც უსადენო ქსელი ხდება გამოუსადეგარი ან მისი მუშაობა იბლოკება. ასეთი შეტევის შესაძლებლობა უნდა გაითვალისწინოს ყველამ, ვინც კი გამართავს უსადენო ქსელს. აუცილებელია დაფიქრება იმაზე, თუ რა მოხდება, როდესაც ქსელი გახდება მიუწვდომელი განუსაზღვრელი დროით. DoS შეტევის სერიოზულობა დამოკიდებულია იმაზე, თუ რა შედეგს გამოიწვევს უსადენო ქსელის მწყობრიდან გამოსვლა. უსადენო ლოკალურ ქსელებში, ჩვეულებრივი ქსელებისგან განსხვავებით, თავდასხმებთან დაკავშირებით ადგილი აქვს მომატებული რისკის ფაქტორს, რაც გამოწვეულია შემდეგი ძირითადი მიზეზებით: უსადენო ქსელებში არ არსებობს ფილტრი, რომელიც შეიძლება იყოს გამოყენებული თავდასხმებისაგან დასაცავად; არ არსებობს სერვერი, რომელიც მომატებული ნდობის ფაქტორით ხასიათდება; უსადენო ქსელები ხასიათდება ობიექტების მუდმივი მოძრაობით და ამასთან ერთად არ არსებობს ფიზიკური არხები; ამ არხების არ არსებობის გამო ინფორმაცია გადაიცემა ეთერის საშუალებით, რაც თავისთავად აგრეთვე საშიშროებას წარმოადგენს, ვინაიდან თავდასხმები იწყება ზუსტად არხის მოსმენიდან. ზემოაღნიშნული პრობლემებიდან გამომდინარე უსადენო ლოკალურ ქსელში მარშრუტიზაციის უსაფრთხოების ამაღლების მიზნით შემუშავებულია ახალი მეთოდი. უსადენო ლოკალურ ქსელში აუცილებელია გამოყენებული იქნას აუტენტიფიკაციის სერვერი, რისი საშუალებითაც მოხდება ქსელურ მოწყობილობებს შორის კავშირის დამყარების პროცესების თვალყურის დევნება და მონაცემთა ბაზაში ჩაწერა. აგრეთვე აუცილებელია ქსელურ მოწყობილობებს შორის გამოყენებული იყოს ორმხრივი აუტენტიფიკაცია, რომლის წყალობით შესაძლებელია უამ¬რავი პრობლემების გადაწყვეტა, რომლებიც დაკავშირებულია უსაფრთხოებასთან. ორმხრივი აუტენტიფიკაციის დროს უსადენო მომხმარებელი და უსადენო ქსელი ერთმანეთს უმტკიცებს თავიანთ იდენტურობას.

კერძო კომპანიებში თუ საწარმოებში უსადენო ლოკალური ქსელი სასურველია შედგებოდეს რამოდენიმე წვდომის წერილებისაგან და მავთულიანი მარშრუტიზატორისაგან. წვდომის წერტილისა და მავთულიანი მარშრუტიზატორის კომბინაციას შეუძლია შეცვალოს უსადენო ლოკალური ქსელის მარშრუტიზატორი და ეს ნაკლებად ძვირადღირებული გადაწყვეტილებაა, ვიდრე უსადენო ლოკალური ქსელის მარშრუტიზატორის შეძენა. აგრეთვე აუცილებელია რომ რამდენიმე უსადენო მომხმარებელი (კომპიუტერები ან ნოუთბუქები) მიერთებულნი იყვნენ რომელიმე კონკრეტულ წვდომის წერილებთან და არავითარ შემთხვევაში არ მოხდეს ინფორმაციის გადაცემის დროს წვდომის წერტილების შემთხვევითი სახით მოძიება. აგრეთვე ყველა ქსელურ მოწყობილობებზე ინდივიდუალური სახით უნდა მოხდეს IP მისამართების გაწერა ქსელის ადმინისტრატორის მიერ და არავითარ შემთხვევაში არ მოხდეს DHCP პროტოკოლის დახმარებით ლოკალური ქსელის მომხმარებლებზე შემთხვევითი სახით IP მისამართების წარდგენა (ნახ.1).



ნახ.1. უსადენო ლოკალური ქსელი აუტენთიფიკაციის სერვერით და კონკრეტული შეერთებებით

ყველაზე ხშირად უსადენო ლოკალურ ქსელებს ქმნიან 802.11 სტანდარტის შესაბამისობით. სტანდარტი IEEE 802.11 აღწერს წვდომის მართვის საერთო ოქმს გადაცემის არეში (Media Access Control, MAC) და უსადენო ლოკალური ქსელების რამოდენიმე ფიზიკურ დონეს. IEEE 802.11 სტანდარტის შემმუშავებელი სამუშაო ჯგუფი აქტიურად მუშაობს უსადენო ლოკალური ქსელების თვისებებისა და უსაფრთხოების გაუმჯობესების მიზნით. ყველა ქსელურ მოწყობილობას გააჩნია თავისი უნიკალური MAC მისამართი და მისი და IP მისამართების გადამოწმებით ინფორმაციის გადაცემამდე მოწყობილობების ინდენტურობის დასადგენად უნდა მოხდეს ორმხრივი აუტენტიფიკაცია.

შემოვიტანოთ აღნიშვნები. $P_{\{i\}}$ აღვნიშნოთ მომხმარებლების სიმრავლე, ხოლო $W_{\{j\}}$ - ით წვდომის წერტილების სიმრავლე.

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

სადაც, n - საკონტროლო ზონაში მომხმარებლების რაოდენობაა, ხოლო m - წვდომის წერტილების რაოდენობა.

თითოეული სიმრავლისათვის შემოვიღოთ სტატუსები $P_{\{i\}Statuse}$ და $W_{\{j\}Statuse}$.

თუ $P_{\{i\}Statuse}$ =1, მომხმარებელი ამოწმებს წვდომის წერილის იდენტურობას, თუ $P_{\{i\}Statuse}$ =2, აუტენთიფიკაცია წარმატებით განხორციელდა, თუ $P_{\{i\}Statuse}$ =0, აუტენთიფიკაცია უშედეგოდ განხორციელდა და ადგილი აქვს კავშირის გაწყვეტას.

ანალოგიურად თუ $W_{\{j\}Statuse}$=1, წვდომის წერილი ამოწმებს მომხმარებლის იდენტურობას, თუ $W_{\{j\}Statuse}$=2, აუტენთიფიკაცია წარმატებით განხორციელდა, თუ $W_{\{j\}Statuse}$=0, აუტენთიფიკაცია უშედეგოდ განხორციელდა და ადგილი აქვს კავშირის გაწყვეტას.

თითოეული მომხმარებლისთვის განსაზღვრულია მისაერთებელი წვდომის წერტილის MAC მისამართი.

დასაწყისისთვის $P_{\{i\}Statuse}$ =1

თუ $P_{\{i\}MAC} = W_{\{j\}\,MAC}$, მაშინ $P_{\{i\}Statuse}$ =2;

თუ $P_{\{i\}MAC} \neq W_{\{j\}\,MAC}$, მაშინ $P_{\{i\}Statuse}$ =0

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

სადაც $P_{\{i\}MAC}$ მომხმარებლისთვის განსაზღვრული მისაერთებელი წვდომის წერილის MAC მისამართია, ხოლო $W_{\{j\}\,MAC}$ - წვდომის წერტილის MAC მისამართი. შემდეგ წვდომის წერტილი ამოწმებს მომხმარებელს:

დასაწყისისთვის $W_{\{i\}Statuse}$ =1

თუ $W_{\{i\}IP} = P_{\{j\}IP}$, მაშინ $W_{\{i\}\,Statuse}$ =2;

თუ $W_{\{i\}IP} \neq P_{\{j\}IP}$, მაშინ $W_{\{i\}Statuse}$ =0

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

აღნიშნულ პროცესებში, თუ რომელიმე ქსელური მოწყობილობა შეეცდება თავისი MAC და IP მისამართის შეცვლას ან გაჩნდება ახალი მისამართები, აუტენთიფიკაციის სერვერი მაშინვე მიიღებს შესაბამის ზომებს და ეჭვის ქვეშ მყოფ ქსელურ მოწყობილობას გათიშავს ქსელიდან და მომხდარის ფაქტზე შეატყობინებს ქსელის ადმინისტრატორს.

ორმხრივი აუტენთიფიკაციის წარმატებით განხორციელების შემდეგ უნდა მოხდეს ინფორმაციის გადაცემა. თუმცა, მანამდე გადაცემამდე მომხმარებლის სადგურმა (PC ან ნოუთბუქი) უნდა მიიღოს წვდომა გარემოსადმი, ანუ უნდა შემოვიღოთ კოორდინაციის გამანაწილებელი ფუნქცია. აღნიშნული რეჟიმის ხელშეწყობა აუცილებელია, რომელიც უზრუნველყოფს მრავალგვარ წვდომას საარსებო კონტროლთან და აღმოფხვრის კოლიზიას. კოორდინაციის გამანაწილებელი ფუნქციის მუშაობის დროს სადგურები შედის კონკურენციაში გარემოსადმი წვდომისათვის და ცდილობს გადასცენ ინფორმაცია,

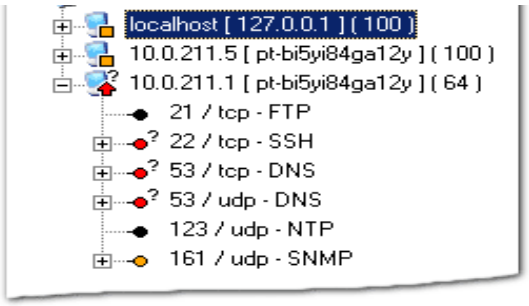
თუ ამ დროს არცერთი სხვა მომხმარებლის სადგური არ ახორციელებს ფრეიმის გადაცემას. თუ რომელიმე გადასცემს ინფორმაციას, დანარჩენები ელოდება არხის გათავისუფლებას.

გარემოსადმი წვდომისათვის, სადგური ამოწმებს ქსელის განაწილების ვექტორის (N) მნიშვნელობას, რომელიც წარმოადგენს ყველა სადგურზე განლაგებულ მთვლელს, რომლის მნიშვნელობა შეესაბამება წინა ინფორმაციული ფრეიმის გადასაცემად აუცილებელ დროს. N-ის მნიშვნელობა უნდა იყოს ნულის ტოლი, იმისთვის, რომ სადგური შეეცადოს ფრეიმის გადაგზავნას. ვიდრე ფრეიმი გადაიგზავნება, მისი მოცულობის მიხედვით სადგური გამოთვლის გადაგზავნისთვის საჭირო დროსა და ქსელში მონაცემთა გადაგზავნის სიჩქარეს. სადგური ათავსებს მნიშვნელობებს ფრეიმის თავში. როდესაც სადგური იღებს ფრეიმს, ის ამოწმებს მნიშვნელობას და გამოიყენებს თავისი N-ის დასაყენებელ საფუძვლად. ამ პროცესის წყალობით ხდება იმ გარემოს რეზერვირება, რომელიც გამოიყენება გადამცემი სადგურის მიერ. ამFრეჟიმის მთავარი ასპექტი არის უკუგორების ტაიმერი, რომელსაც სადგური იყენებს იმ შემთხვევაში, როცა გადაცემის გარემო დაკავებულია. როდესაც არხი გამოიყენება სხვა სადგურის მიერ, გადაცემის სურვილის მქონე სადგური რაღაც დროის განმავლობაში უნდა იმყოფებოდეს ლოდინის რეჟიმში, შემდეგ კი კვლავ შეეცადოს მიიღოს წვდომა გარემოსადმი. ამის წყალობით გამოირიცხება იმის შესაძლებლობა, რომ რამოდენიმე სადგურმა პარალელურ რეჟიმში დაიწყოს ფრეიმების გადაცემა. უკუგორების ტაიმერი მნიშვნელოვნად ამცირებს კოლიზიების და განმეორებით გადაცემების რიცხვს, განსაკუთრებით მაშინ, როდესაც აქტიური მომხმარებლების რაოდენობა დიდია.

ლოკალური ქსელების გამოყენებისას, რაც დაფუძნებულია რადიოარხებზე, მონაცემების გაგზავნის დროს გადამცემ სადგურს არ შეუძლია მოუსმინოს გარემოს კოლოზიის წარმოშობას, ვინაიდან მას არ გააჩნია უნარი გამოიყენოს თავისი მიმღები მონაცემთა გადაცემის დროს. ამიტომ მიმღებმა სადგურმა უნდა გააგზავნოს იმის დასტური, რომ მან ვერ აღმოაჩინა მიღებულ ფრეიმში შეცდომა. თუ გადამცემი სადგური რაღაც განსაზღვრული დროის განმავლობაში არ მიიღებს დასტურს, ის დაასკვნის, რომ წარმოიშვა კოლოზია ან რადიოხარვეზების გამო ფრეიმი იყო დაზიანებული და გადააგზავნის განმეორებით. უსადენო ლოკალურ ქსელებში ქსელის ადმინისტრატორის ინიციატივით ან ავტომატიზებულ რეჟიმში უსაფრთხოების ავტომატიზებული სისტემის დახმარებით აუცილებელია პერიოდულად განხორციელდეს ქსელის სკანირება, რომლის საშუალებითაც გამოიკვეთება ქსელის ნაკლოვანი მხარეები და რისი მეშვეობითაც ხორციელდება უსაფრთხოების მონიტორინგის ლოგიკური და სტრუქტურირებული პროცესი. ქსელის სკანირება საშუალებას იძლევა ორგანიზება გაუწიოს ნებისმიერი მასშტაბის კომპიუტერული ქსელის შემოწმებისა და ინფორმაციის შეგროვების პროცესს. ქსელის სკანირებისას შესაძლებელია როგორც ცალკეული IP მისამართის სკანირება, ისე ქსელის ყველა IP მისამართის სკანირება, ასევე შესაძლებელია გარკვეული შუალედის მითითებით მოხდეს სკანირება [3].

სკანირების პროცესის დროს შესაძლებელია როგორც მთლიანი პროცესის მართვა, აგრეთვე ცალკეული ჰოსტების (IP მისამართები) მართვა. პროცესის დროს შესაძლებელია ყველა ან მონიშნული ჰოსტების სკანირების პროცესის შეჩერება ან შეწყვეტა. სკანირების

პროცესის დასრულების შემდეგ შესაძლებელია სკანირების პროცესის შედეგების შენახვა სპეციალურ მონაცემთა ბაზაში, თარიღისა და დროის მითითებით, რომელიც შეიძლება ნებისმიერ დროს გამო¬ძახებულ იქნეს. აგრეთვე ნებისმიერ მომენტში მისგან შესაძლებელია ანგარიშების მომზადება. სკანირებისას მიღებული ყველა შედეგები მაშინვე აისახება სპეციალურ ფანჯარაში. ჰოსტების სკანირებისას მიღებული ყველა შედეგები გამოსახულია სხვადასხვა ფერის აღნიშვნებით, რისგან გამომდინარე ნაკლოვანებების ხარისხი ერთი შეხედვითაც შეიძლება შეფასდეს (ნახ. 2).



ნახ.2. ქსელის სკანირებისას მიღებული შედეგი

სხვადასხვა ფერის აღნიშვნებში თუ ბევრი ,,წითელი ფერია" - ეს ცუდია, ბევრი ,,ყვითელი" - არც ისე ცუდი, ხოლო ბევრი ,,მწვანე" - პრაქტიკულად ნორმალურია. ყველაზე კარგი არის მაშინ, როდესაც ფერადი ნიშნები საერთოდ არ არის. მოვიყვანოთ ყველა ნიშნების ერთობლიობა და მათი აღწერა (ნახ. 3).

ნახ.3. სკანირებისას მიღებული სხვადასხვა ნიშნების აღწერა

ნიშნები სრულიად გასაგებად არის წარმოდგენილი. ,,სკანირების ხეს" გააჩნია სამი დონე (ჰოსტი-პორტი-ნაკლოვანება). თუ სერვისს სერიოზული ნაკლოვანება გააჩნია, მაშინ მისი იკონკა გამოსახულია წითელი ფერით და შესაბამისად მისი შესაბამისი ჰოსტის იკონკაც წითელი ფერით აისახება.

საბოლოო ეტაპზე ქსელის ადმინისტრატორმა სკანირებისას მიღებული შედეგების საფუძველზე უნდა მოახდინოს შესაბამისი რეაგირება.

3. დასკვნა

უსადენო ლოკალური ქსელებისათვის უსაფრთხოება უაღრესად მნიშვნელოვანი საკითხია, ვინაიდან გარემოში გავრცელებული საკომუნიკაციო სიგნალები ხელმისაწვდომია დასაჭერად. აქედან გამომდინარე, კომპანიებმა და ინდივიდუალურმა მომხმარებლებმა უნდა შეიცნონ პოტენციურად არსებული პრობლემები და მიიღონ შესაბამისი ზომები რომლებმაც უნდა უზრუნველყონ სისტემის უსაფრთხოება. ნებისმიერ სისტემას, რომელსაც დაცვა სჭირდება, გააჩნია სისუსტეები ან ხარვეზები, რომელთა გათვალისწინება აუცილებელია სისტემის გამართული მუშაობისათვის და მოსალოდნელი საფრთხეების ასაცილებლად.

ლიტერატურა - References – Литература:

1. შონია ო., ნარეშელაშვილი გ., ქართველიშვილი ი. (2009). უმავთულო ქსელების უსაფრთხოება. სტუ. საგამომც.სახლი „ტექნიკური უნივერსიტეტი“. თბილისი.

2. Мерритт М., Поллино Д. (2004). Безопасность беспроводных сетей. Москва.

3. Mishra A. (2008). Security and Quality of Service in Add Hoc Wireless Networks, Cambridge University Press.

REVEALING OF POTENTIALLY DANGEROUS SITUATIONS IN NORMATIVE-LEGAL DOCUMENTS AND UNDERLINE THE CRITERIA IN THEM

Shonia Otar[1], Kartvelishvili Ioseb[1], Beridze Zebur[2], Didmanidze Ibraim[2], Kolbaia Levan[1]

1-Georgian Technical University, 2-Batumi Shota Rustaveli State University

Summary

The most important issue for wireless local sell is safety, because widespread communicational signals in environment are available for everyone. Therefore, companies and individual users must recognize potentially existing problems and make proper measures to ensure system safety. Any system that needs defense has defects and failings, and all these must be inevitably considered for system's proper work and to avoid expected dangers in future.

АВТОМАТИЗИРОВАННОЕ ПРОЕКТИРОВАНИЕ ЛОГИЧЕСКОГО И СТРУКТУРИРОВАННОГО ПРОЦЕССА МОНИТОРИНГА БЕЗОПАСНОСТИ БЕЗПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Шония[1] О., Картвелишвили[1] И., Беридзе[2] З., Дидманидзе[2] И.,Колбая[1] Л.

1-Грузинский Технический Университет,

2- Батумский государственный университет

Резюме

Безопасность беспроводных локальных сетей очень важный вопрос, потому что в окружающей среде распространёные коммуникационные сигналы доступны для использования. исходя из этого, частные компании и индивидуальные пользователи должны осознать потенциально существующие проблемы и принять соответствующие меры, которые должны обеспечивать безопасность системы. Каждая система, котороя нуждается в защите, имеет слабые стороны или недостатки, рассмотрение которых необходимо для улучшения работы системы и избежания возможных опасностей.