

უსადენო ქსელებში გამოყენებული მოდულაციის ტექნიკის და აუტენტიფიკაციის მეთოდების განხილვა

გიორგი გამდლიშვილი, ვლადიმერ ადამია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

წარმოდგენილია უსადენო ქსელების კომუნიკაციის მოქნილი მექანიზმები, რომელთა საფუძველზე შესაძლებელია ფიზიკური მედიასაშუალებების დონეზე რადიო-სიხშირული ტალღების გამოყენება. ასევე მოცემულია თუ როგორ ხდება რადიოსიხშირის დატვირთვა გადასაცემი ინფორმაციით და რა ტექნოლოგიები გამოიყენება. ამ მიზნით სტატიაში აღწერილია სიხშირული დიაპაზონები და მათი დანიშნულება. განხილულია მოდულაციის ტექნიკა და წარმოდგენილია ამ ტექნოლოგიის რამდენიმე ვარიანტი. წარმოდგენილია უსადენო ქსელის რამდენიმე სტანდარტი და მათი მათემატიკური შესაბამისი სიხშირეები. ასევე განიხილება აუტენტიფიკაციის მექანიზმები. შედეგად შესაძლებელია წარმოდგენილი მექანიზმების მეშვეობით ეფექტური უსადენო ქსელის აგება, რაც ინფორმაციის მოქნილი, სწრაფი და საიმედო გაცვლის ბაზისია.

საკვანძო სიტყვები: მოდულაციის ტექნიკა. ცენტრალიზებული აუტენტიფიკაცია. სიხშირული დიაპაზონები.

1. შესავალი

მიუხედავად იმისა, რომ უსადენო ქსელები ბაზარზე გამოჩნდა 1990 წლიდან, ტექნოლოგია ფაქტიურად არსებობდა 1800 წლიდან. მუსიკოსმა და ასტრონომმა უილიამ ჰერშელმა (1732-1822) აღმოაჩინა ინფრაწითელი სხივები, რომელიც ადამიანის თვალისთვის უხილავი იყო. აღმოჩენა წარმოადგენდა გზას ელექტრომაგნიტური ტალღების თეორიისაკენ რომელიც სილვანუსტრუდმა შემდგომში გამოკვლეული იქნა ჯეიმს მაქსველის მიერ. მისი აღმოჩენების უდიდესი ნაწილი ელექტრომაგნიტიზმის კუთხით დაფუძნებული იყო მიხეილ ფარადეის და ანდრე მარია ამპერის კვლევებზე. მაქსველის აღმოჩენები გამოიყენა ჰენრი ჰერცმა და დაასკვნა, რომ ელექტრომაგნიტური ტალღები მოძრაობს სინათლის სიჩქარით და ელექტრობა შესაძლებელია გადატანილი იქნას ამ ტალღების მიერ [2].

ჩნდება კითხვა - რა კავშირშია ყოველივე ზემოთქმული უსადენო ქსელებთან. ქსელში მონაცემები გადაიცემა ეზერნეტის სადენის საშუალებით ელექტრონული სიგნალის სახით, ხოლო ჰერცის აღმოჩენა საშუალებას იძლევა საჭირო გზების მეშვეობით განხორციელდეს იგივე მონაცემების გადაცემა როგორც ელექტროსიგნალის. საბოლოოდ ყოველივე ამის გადაწყვეტა ხორციელდება რადიოტალღების მეშვეობით.

უსადენო ქსელების ერთ-ერთი მთავარი ამოცანაა მომხმარებლისთვის ქსელთან წვდომის მოქნილი სისტემის შექმნა და ასევე ისეთ გარემოში მუშაობა სადაც სადენის დამონტაჟება გართულებულია ან არ არსებობს შესაბამისი დონის მოთხოვნა. ამ შემთხვევაში ძალზედ მნიშვნელოვანია თუ რა მექანიზმით მოხდება ფიზიკური სიგნალის დატვირთვა გადასაცემი ინფორმაციით. ამის უზრუნველყოფა ხდება სხვადასხვა მოდულაციის ტექნიკის მეშვეობით. მნიშვნელოვანია აგრეთვე არხთან დაშვების ტექნოლოგიები. ქსელურ რესურსებთან დაშვების მექანიზმს კი წარმოადგენს აუტენტიფიკაციის საშუალებები, რომლებიც იზღუდება არალეგიტიმური მომხმარებლის დაშვება ქსელთან. ეს მექანიზმები ერთობლივად უზრუნველყოფს უსადენო ქსელის სტაბილურ და უსაფრთხო ფუნქციონირებას.

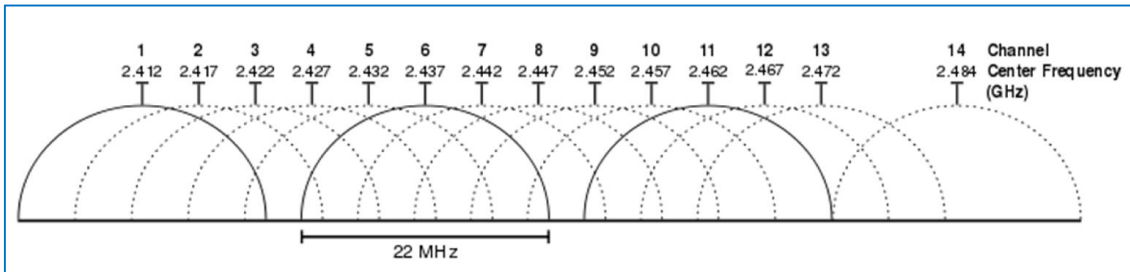
მთავარ მიზანს წარმოადგენს რადიოტალღების მეშვეობით მაქსიმალურად სწრაფად და მაქსიმალურად შორს განხორციელდეს ინფორმაციის გადაცემა, მაგრამ ასეთი ტექნოლოგიის

გამოყენებას თან სდევს ისეთი ფაქტორები როგორცაა სხვადასხვა რადიოტალღების ურთიერთშემოქმედება და ჩახშობა.

2. ძირითადი ნაწილი

IEEE 802.11-უსადენო ქსელების სტანდარტია, რომლის ოპერირებაც ხორციელდება ფედერალური საკომუნიკაციო კომისიის მიერ განსაზღვრული წესების ფარგლებში[3]. უნდა აღინიშნოს, რომ ეს სტანდარტი იყენებს არალიცენზირებულ სიხშირეს (ISM). ინფორმაციის გადაცემის პროცესში ხორციელდება გადამტანი სიგნალის დატვირთვა მონაცემებით. ამ პროცედურას მოდულაციის ტექნიკა ეწოდება. უსადენო ქსელების ერთ-ერთი მთავარი ამოცანაა მომხმარებლისთვის ქსელთან წვდომის მოქნილი სისტემის შექმნა და ასევე ისეთ გარემოში მუშაობა, სადაც სადენის დამონტაჟება გართულებულია ან არ არსებობს შესაბამისი დონის მოთხოვნა. ასევე მის მთავარი ამოცანაა მობილურ მომხმარებელზე ორიენტირებული გარემოს შექმნა და, საჭიროების შემთხვევაში, როუმინგის უზრუნველყოფა. უსადენო წვდომის მარშრუტიზატორს აქვს შესაძლებლობა განახორციელოს მაუწყებლობა მის განკარგულებაში არსებული არხებიდან ერთ-ერთზე, რომელიც მოცემულ სიტუაციაში არ ფარავს სხვა არხს და ამით დაცულია ინფორმაციის დაზიანებისგან.

ნახ. 1-ზე მოცემულია არხების დიაპაზონები და ამასთან მათი განაწილების სქემა, რათა თავიდან არიდებულ იქნას სიგნალის დამახინჯება და ერთ წერტილში რამდენიმე დაფარვის ზონის არსებობის შემთხვევაში მათი ურთიერთშეუფერხებელი მუშაობა. აქედან გამომდინარე შესაბამისი სიხშირული დიაპაზონები უნდა განისაზღვროს წინასწარ ან დადგინდეს თვითონ მოწყობილობის მიერ წინასწარ სივრცის სკანირების შედეგად[2].



ნახ.1. არხების დიაპაზონები და მათი განაწილების სქემა

დღესდღეობით ყველაზე გავრცელებული არალიცენზირებული სიხშირეა 2,4Ghz. ამ სიხშირეზე მაუწყებლობენ 802.11b, 802.11g, 802.11n, ასევე გვაქვს 802.11a სტანდარტი, რომელიც მაუწყებლობისთვის იყენებს 5Ghz სიხშირეს. აქვე უნდა აღინიშნოს, რომ უსადენო ქსელებში გამოყენებული მოდულაციის ტექნიკის ვარიანტებია: DSSS, OFDM, MIMO[3].

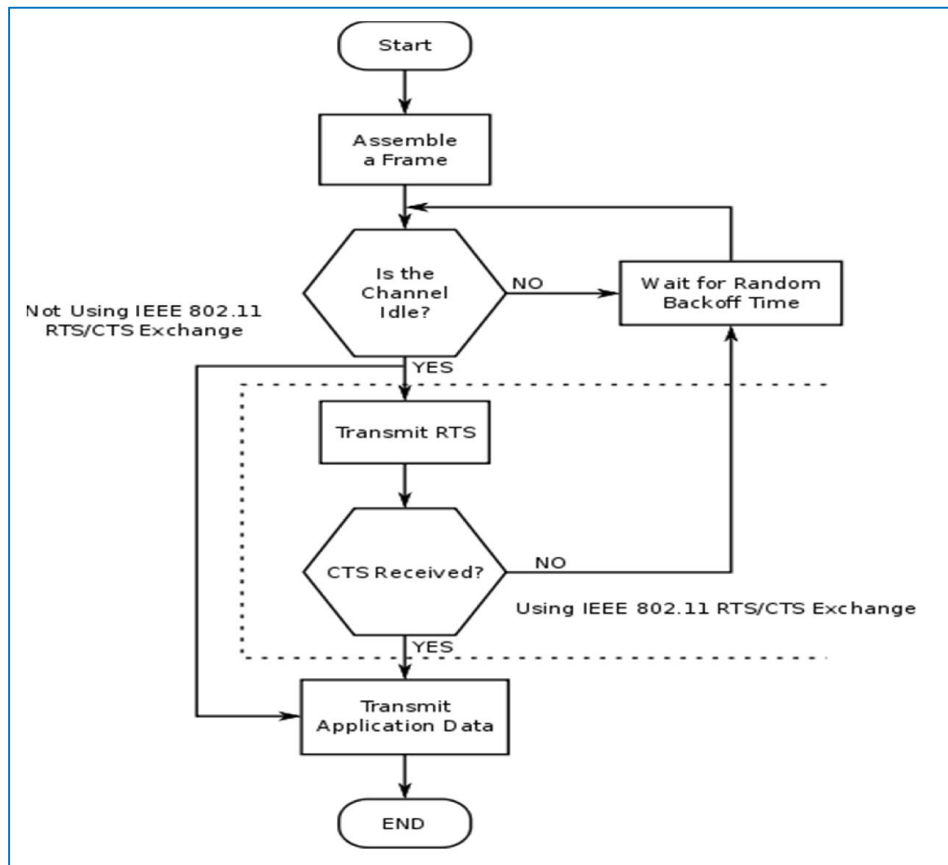
DSSS მოდულაციის ტექნიკის გამოყენების დროს ადგილი აქვს სიგნალის გავრცელებას მის მიერ გამოყენებულ მთლიან სიხშირულ სპექტრზე. მაგალითად, თუ უსადენო წვდომის მარშრუტიზატორი მაუწყებლობისთვის იყენებს 1 არხს, იგი ავრცელებს სიგნალს მთელ არხზე, რომლის სიგანეც არის 22MHz.

იმისათვის რომ განხორციელდეს მონაცემთა კოდირება DSSS-ის მეშვეობით, გამოიყენება მიკროკადრების თანმიმდევრობა. საბოლოოდ კოდირება ეს არის მონაცემთა ერთი ფორმატიდან მეორეში გარდაქმნა. მოდულაციის ეს ტექნიკა მუშაობს ინფორმაციის გადაცემის შედარებით დაბალ სიჩქარეებთან და 11 Mbps სიჩქარით მაუწყებლობის დროს იყენებს CCK მექანიზმს, რომელიც 64 უნიკალური კოდის სიტყვის მეშვეობით წარმოადგენს მონაცემების 6 ბიტს[2].

OFDM არ არის გადაწყვეტილი როგორც სიგნალის გავრცელების სპექტრული ტექნოლოგია. OFDM მოდულაციის ტექნიკის გამოყენებით შესაძლებელია მიღწეულ იქნას ინფორმაციის სწრაფი გადაცემა და გარე ზემოქმედების მიმართ მდგრადობა. OFDM განსაზღვრავს არხების გარკვეულ რაოდენობას მოცემულ სიხშირულ დიაპაზონში, ხოლო შემდგომში არხი რომელზეც ხორციელდება მაუწყებლობა, იყოფა ქვეარხებად. არხის სიგანე შეადგენს 20MHz და იგი იყოფა ქვეგადამტან სიხშირეებად 300 KHz დიაპაზონით. ასეთი მიდგომით ჩვენ ვღებულობთ 52 ქვეგადამტან სიხშირეს თითოეულ არხზე. OFDM წარმოადგენს ორთოგონალურად დაყოფილი სიხშირის მულტიპლექსინგს. ასეთი მოდულაციის ტექნიკა გამოიყენება 802.11a და 802.11g სტანდარტის უსადენო ქსელებში.

MIMO არის ტექნოლოგია, რომელიც გამოიყენება ახალი სტანდარტის 802.11n უსადენო ქსელებში. ამ ტექნოლოგიაში რამდენიმე ანტენაა სიგნალების მიღება-გადაცემისთვის. ინფორმაციის გადაცემა წარმოებს რამდენიმე არხის მეშვეობით პარალელურად, რაც მნიშვნელოვნად ზრდის სიჩქარეს. ამ სტანდარტის მიღება-გადაცემის სიჩქარე 300Mbps აღწევს.

უსადენო ქსელებში გამოიყენება CSMA/CA ტექნოლოგია (ნახ.2) [1]. ვინაიდან ინფორმაციის გადაცემა წარმოებს უსადენო ქსელის წვდომის წერტილის მეშვეობით და მისი ფუნქციონირება მსგავსია ჰაბის ფუნქციონირების, უნდა განხორციელდეს კოლიზიების თავიდან აცილება. ამ მიზნით კლიენტის მხრიდან ხდება მოთხოვნის გენერირება ინფორმაციის გადაცემის უფლების მიღებაზე. ამ პროცესში ადგილი აქვს RTS/CTS სიგნალების კომბინაციის გენერირებას. ერთი აღნიშნავს გადაცემაზე უფლების მოთხოვნას, მეორე მინიჭებას[2].



ნახ.2. CSMA/CA - ტექნოლოგია

ზემოთ აღწერილი ტექნოლოგიების მეშვეობით ხორციელდება გარკვეულწილად ქსელთან წვდომის მოქნილობის გაზრდა და გარკვეულწილად დანახარჯების შემცირება.

უსადენო ქსელების აგებისას და მათი გამოყენებისას ძალზედ მნიშვნელოვანია უსაფრთხოების მექანიზმების გამოყენება. უსადენო ქსელებისთვის სამ ძირითად საფრთხეს წარმოადგენენ:

- პირები, რომლებიც სკანირების მეშვეობით ცდილობენ დაუცველი არის აღმოჩენას და შემდგომ მასთან მერთებას;
- კრეკერები, რომლებიც ცდილობენ არაავტორიზებული წვდომის მიღებას;
- თანამშრომლები, რომლებმაც შესაძლოა დაფარვის არის გაზრდის მიზნით განახორციელონ უსადენო ქსელის წერტილის მიერთება კორპორაციის ქსელთან.

ერთ-ერთი გავრცელებული საფრთხეა შუალედური უსადენო წვდომის წერტილის ჩანერგვა. როგორც ცნობილია, სადენის შემთხვევაში ჩვენ ფიზიკურად უნდა მიუერთდეთ მას, რათა განხორციელდეს ტრაფიკის მოსმენა. უსადენო ქსელებში ამის აუცილებლობა არ არის, ამასთან ერთად უნდა აღინიშნოს, რომ ნებისმიერ ნოუთბუქს აქვს შესაძლებლობა შესაბამისი პროგრამული უზრუნველყოფის ინსტალაციის შედეგად იფუნქციონიროს როგორც უსადენო ქსელთან წვდომის წერტილმა. ამ გზით შესაძლებელია განხორციელდეს ლეგიტიმური მომხმარებლების მიერთება და შემდგომ მათგან სენსიტური ინფორმაციის მოპოვება, ისეთისა, როგორცაა პირადი მონაცემები, პაროლები, კონფიდენციალური ბიზნეს მიმოწერა.

ამ პრობლემების თავიდან აცილების ერთ-ერთი მექანიზმია შეღწევის პრევენციის სისტემის არსებობა და, მაგალითად, საწარმოო ქსელის არსებობის შემთხვევაში დაფარვის ზონის სიხშირული სკანირება არალეგიტიმური უსადენო წვდომის წერტილების აღმოჩენის მიზნით. ასევე მნიშვნელოვანია მონიტორინგის სისტემის მიერ ხორციელდებოდეს უსადენო წვდომის წერტილის აპარატურული დატვირთვის შეფასება. თუ უსადენო წვდომის წერტილი ჩვეულებრივზე მეტადაა დატვირთული, მაშინ შესაძლებელია არაავტორიზებული წვდომის მიღების მცდელობის ვარაუდი.

ცენტრალიზებული აუტენტიფიკაციის მიზნით შესაძლებელია გამოყენებული იქნას TACACS და RADIUS სერვერები, რომლებიც საშუალებას იძლევა ერთ კონკრეტულ ადგილას მოხდეს მომხმარებელთა აუტენტიფიკაცია და მხოლოდ ამის შემდეგ ქსელის რესურსებთან მათი დაშვება[2]. ამისთვის გამოიყენება EAP პროტოკოლი. სანამ ეს უსაფრთხოების მექანიზმები დაიმკვიდრებდა ადგილს, გამოიყენებოდა ფიზიკური მისამართების დონეზე ფილტრაცია და არხის იდენტიფიკატორის დაფარვა რაც ვერ უზრუნველყოფდა შესაბამის უსაფრთხოებას, თუმცა ეს მექანიზმი დღესაც გამოიყენება როგორც ერთ-ერთი დამატებითი უსაფრთხოების საშუალება.

3. დასკვნა

მოდულაციის ტექნიკა საშუალებას გვაძლევს ეფექტურად გამოვიყენოთ რადიო სიხშირე, ინფორმაციის გადაცემის დროს თავიდან ავიცილოთ მონაცემთა დაკარგვა და გაეზარდოს ინფორმაციის გადაცემის სიჩქარე კოდირების სხვადასხვა მეთოდის გამოყენებით. ამასთანავე აუტენტიფიკაციის მექანიზმი მნიშვნელოვანი საშუალებაა ქსელურ რესურსებთან დაშვების კონტროლისთვის.

ლიტერატურა:

1. Molish F.(2011). Wireless Communication. Published John Wiley & Sons Ltd. First edition published 2005 Registered office John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom.
2. CCNA Wireless Official Exam Certification Guide Person Education (2008). Brandon James Carroll. Published by: Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA.
3. Steve Rackley. (2007). Wireless networking technology from principles to successful implementation. First published Linacre House, Jordan Hill, Oxford OX2 8DP 30 Corporate Drive, Suite 400, Burlington MA 01803.

REVIEW OF USED MODULATION TECHNIC IN WIRELESS NETWORKS AND AUTHENTICATION MECHANISMS

Gamdlishvili Giorgi, Adamia Vladimer
Georgian Technical University

Summary

In this article is presented flexible mechanisms of wireless network communication. Based this is possible using radio frequencies as transmission media at the physical layer. Also there is given how radio frequency may carry data and which technologies are used. To this aim in this article is described frequencies ranges and their purpose. There is reviewed modulation technic and presented some of different variance of this technology. There are presented number of wireless standards and their sufficient radio frequencies. Also there is described authentication mechanisms. Based this it is possible to build the efficient wireless network, which is platform of efficient, fast and reliable information exchange.

ОБЗОР ТЕХНИКИ МОДУЛЯЦИЙ В БЕЗПРОВОДНЫХ СЕТЯХ И МЕХАНИЗМОВ АУТЕНТИФИКАЦИЙ

Гамдлишвили Г., Адамия В.
Грузинский Технический Университет

Резюме

Представлены гибкие механизмы коммуникаций в беспроводных сетях, с помощью которых можно использовать радиочастотные волны как несущую частоту. Также описан процесс размещения данных на радиочастоте и какие технологии можно использовать. С этой целью в статье описаны частотные диапазоны и их назначение. Рассматривается техника модуляций и представлены различные варианты этих технологий. Также представлены несколько стандартов беспроводной сети и соответствующие частоты. Рассматриваются методы аутентификаций. Представленные механизмы дают возможность построить эффективную беспроводную сеть, которая является основой для быстрой и надёжной передачи информации.