Безбедно користење на безжични ad-hoc мрежи

Илија Апостолов[1], Митко Богданоски[2]

[1] Европски Универзитет – Скопје, Р. Македонија, apostolov.ilija11@live.eurm.edu.mk

[2] Воена академија – Скопје, Р. Македонија, mitko.bogdanoski@eurm.edu.mk

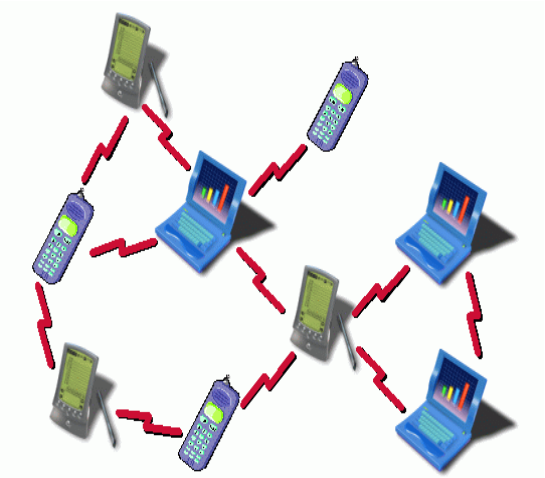
***Абстракт*—Безжичните мрежи се решенија кои овозможуваат поврзување на компјутерските мрежи за пренос на податоци на отворени и затворени локации, пренос преку интернет конекција и користење на сите бенефити од мрежното поврзување. Безжична ad hoc мрежа е колекција од јазли/крајни станици кои комуницираат еден со друг, формирајќи повеќескоковна радио мрежа и одржувајќи конективност на децентрализиран начин, односно без централен сервер. Тие создаваат привремена конекција, при што некои од уредите се членови на мрежата само додека трае комуникациската сесија. Секој јазол во ad hoc мрежата функционира и како хост и како рутер, што значи контролата на мрежата е дистрибуирана помеѓу јазлите. Додека јазлите комуницираат преку безжичните линкови тие мораат да се соочуваат со ефектите на радио комуникацијата, како што е бучност, слабеење на сигналот со оддалеченоста и пречки. Целта на овој труд е да се разгледа принципот на функционирање на безжичните ad-hoc мрежи и да се разгледаат безбедносните механизми кај овие мрежи, кои, поради нивната природа се значително поспецифични од останатите безжични мрежи. На крај е прикажан практичен пример за правилно и безбедно креирање на безжична ad-hoc мрежа кај Windows 7 OS.**

***Клучни зборови*— Wi-fi, Ad hoc, Безжични ad hoc мрежи, Безбедност.**

I. Вовед

AD HOC мрежите може да се формираат, спојуваат или делат на одделни мрежи по потреба, без задолжително да се засноваат на фиксна инфраструктура за управување со мрежата. Јазлите на ad hoc мрежите честопати се мобилни, што исто така значи дека тие применуваат безжична комуникација за одржување на поврзаноста. Ваквите мрежи се нарекуваат мобилни ad hoc мрежи (MANET).

Во ad hoc мрежите може да постојат статични и физички поврзани јазли кои може да ги користат услугите понудени од фиксната инфраструктура. Ad hoc мрежите можат да бидат различни една од друга, во зависност од областа на примена. Перформансите на јазлите во ad hoc мрежите се од клучно значење, бидејќи количеството на достапна моќност за прекумерни пресметки и радио преноси се ограничени. Освен тоа, достапните бранови должини и радио фреквенции можат значително да се ограничени и брзо да се менуваат. Сепак, бидејќи количеството на достапна меморија и моќноста на компјутерот се прилично мали, поставувањето на силна заштита за ad hoc мрежите е тешко остварливо. [1]



Слика 1.MANET мрежа

Wireless Fidelity или **Wi-Fi**, е заштитен знак на Wi-Fi алијансата. Овој знак производителите можат да го користат за обележување на своите сертифицирани производи од класата на WLAN (wireless local area network), односно уреди базирани на IEEE 802.11 стандардите. Поради поврзаноста со овие стандарди, поимот Wi-Fi често се користи како синоним за технологијата базирана на IEEE 802.11стандардите. Wi-Fi алијансата претставува светска непрофитабилна асоцијација на компании кои ја подржуваат и унапредуваат WLAN технологијата и кои издаваат сертификати за производи кои се во согласност со одредени стандарди за електронска комуникација. Не секој уред која одговара на IEEE 802.11 стандардот е предаден за тестирање за издавање на сертификат од страна на Wi-Fi алијансата. Најчесто, причина за ова, се високите трошоци за издавање на сертификатот. Ако

некоја направа, односно уред не го носи Wi-Fi логото на себе, тоа не мора да значи дека истиот не е во склад со другите Wi-Fi уреди. Од 2010 година, IEEE 802.11 технологијата се вградува скоро во сите персонални компјутери, конзоли за видеоигри, паметни телефони, печатачи и други надворешни единици и буквално во сите лаптоп и рачни компјутери. [2]

II. Интернет пристап

Wi-Fi уредите можат да се поврзат на Интернет ако се во дометот на безжична мрежа која овозможува пристап до Интернет. Покривањето на една или повеќе точки на пристап (кои се меѓусебно поврзани), уште попознати под англискиот термин hotspot, може да зафати површина со големина од неколку соби до неколку квадратни километри. Покривањето на поголема површина може да се изведе со група од повеќе точки на пристап, чии сигнали ќе се препокриваат. Wi-Fi технологијата се користи за градење на таканаречени безжични меш мрежи [3]. Покрај употребата за градење на приватни мрежи по домовите и канцелариите, Wi-Fi технологијата се користи и кај хотспотовите за доделување на јавен пристап до Интернет, бесплатно или со претплатување кај разни комерцијални услуги. Организациите и фирмите, како тие што управуваат со аеродроми, хотели и ресторани, често имаат бесплатни пристапни точки за да ги привлечат или да им помогнат на своите муштерии. Властите или поединци кои сакаат да обезбедат услуги или да го промовираат својот бизнис, често нудат бесплатен Wi-Fi пристап. Од 2008 година започнати се повеќе од 300 проекти (познати како Muni-Fi) низ целиот свет, за изградба на Wi-Fi мрежи на ниво на цели градови. Во мај 2008 год. Чешката Република имала 879 Wi-Fi провајдери на безжичен интернет. Рутерите со Wi-fi поддршка кои имаат и вграден модем за дигитална претплатничка линија (анг. digital subscriber line modem) или кабловски модем, често се поставени по домовите или други простории и нудат интернет пристап и работење во мрежа на уредите кои се поврзани со нив, преку Wi-Fi или со кабел. Исто така, Wi-Fi уредите можат да се поврзат во директна клиент-клиент врска во ad hoc режим на работа без посредство на рутер. Преку Wi-Fi денес се овозможува интернет пристап и до тоалети, кујни и на ред други места кои порано биле изоставени од ваквата технологија.[4]

A. Комуникација помеѓу два компјутери

Wi-Fi технологијата исто така овозможува директна комуникација меѓу два или повеќе компјутери без посредство на точка на пристап. Ваквото поврзување се вика ad hoc режим на пренос на податоци преку Wi-Fi . Ваквиот ad hoc режим на поврзување се покажа доста популарен кај конзолите за видеоигри кои подржуваат вклучување на повеќе учесници. Слично на ова, Wi-Fi алијансата ја подржува таканаречената Wi-Fi Direct технологија, која е се уште во развој, и која користи нови методи на пронаоѓање и безбедност при пренесување на податоци. [5]

III. Безжични AD – hoc мрежи

Бежичната ad-hoc мрежа е децентразлизирана бежична мрежа. Мрежата е ad-hoc поради тоа што не се потпира на претходно постоечка инфраструктура, како што се рутерите во жичната мрежа или пристапните точки во управуваните бежични мрежи. Наместо тоа, секој компјутер учествува во рутирање со препраќање на податоците, така што одредувањето на тоа до кој компјутер треба информацијата да се препрати е направено динамички, базирајќи се на мрежното поврзување. Најраните ad-hoc бежични мрежи се “packet radio” мрежи (PRNETs).

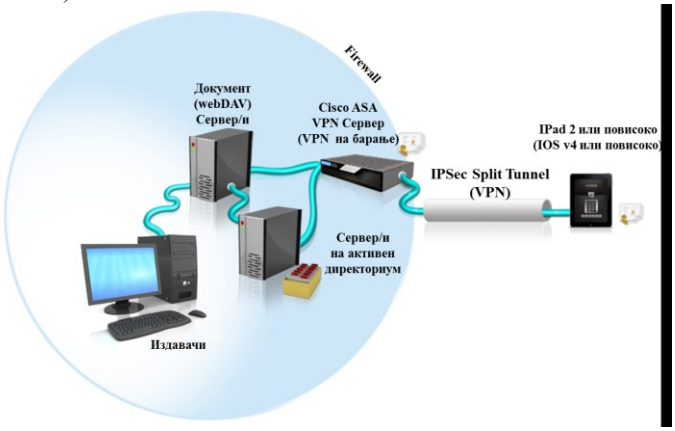
Слика 2.Безжична Ad-hoc мрежа

Децентрализираната природа на бежичните ad-hoc мрежи ги прави погодни за различни апликации каде централните компјутери неможат да се искористат, односно таму каде безжичните ad-hoc мрежи нудат подобра услуга. Иако во рамките на теоријата и практиката инфраструктурните безжични мрежи се поискористени сепак, минималната конфигурација и брзото распоредување, ги направи ad-hoc мрежите погодни за итни ситуации како природни катастрофи и воени конфликти, но и доста искористливи за терени каде што не е можно да се постави инфраструктурна мрежа. Присуството на динамичен и приспособлив рутинг протокол им овозможува на ad-hoc мрежите да се брзо формирање. Ad-hoc мрежата е составена од повеќе компјутери поврзани со врски. Врските се под влијание на ресурсите на компјутерот (на пр. достапно снабдување на енергија, моќност на предавателот, компјутерска моќ и меморија), како и од својствата на врските (пр. Оптичка видливост, интерференција,, должина на линкот, губење

на сигналот, пречки и бучава). Бидејќи на мрежата можат да бидат поврзани и исклучени во секое време нови и стари врски, функционалната мрежа мора да биде способна да се справи со овие динамични реструктуирања и тоа по можност на начин кој е навремен, ефикасен, сигурен и стабилен. Мрежата мора да им овозможи на било кои компјутери да комуницираат често преку други компјутери кои ја пренесуваат информацијата. Патека е серија на врски што поврзуваат два компјутери. Често има повеќе патеки помеѓу било кои компјутери. Компјутерите се често ограничени од моќта на предавателот и расположливите енергетски ресурси. Моќта на предавателот често троши највеќе енергија во компјутерот. Според инверзното квадратно право повеќе е енергетски ефикасно да се препраќаат информации низ мрежата преку повеќе јазли.[6] [7].

IV. Безбедност кај безжичните ad-hoc мрежи

Безбедноста на ad-hoc мрежите може да се заснова на заштитата во линкот или мрежниот слој. Во некои ad-hoc решенија, силни безбедносни услуги за заштита на доверливоста и автентичноста нуди и линковскиот слој, и во тој случај сите барања за безбедност не треба да се однесуваат на мрежниот или горните слоеви. На пример во некои безжични LAN мрежи се применува шифрирање на слојот на линкот. Сепак, во повеќето случаи безбедносните услуги се применуваат во погорните слоеви, на пример во мрежниот слој, бидејќи многу ad-hoc мрежи применуваат рутирање базирано на IP адресата и ја препорачуваат употребата на **Internet Protocol Security** (IPSec).



Слика 3. Cisco IPSec-базирана DMZ безбедносна архитектура [8]

Повеќето протоколи за рутирање на мобилни и компјутерски ad-hoc мрежи изгледа дека добро се справуваат со брзите промени на средината на мрежно поврзување. Бидејќи протоколот за рутирање е одговорен за одредување и одржување на потребната структура за рутирање за јазлите, протоколот мора да биде заштитен од било каков напад на доверливоста, веродостојноста, интегритетот, неотфрлањето и достапноста. Ако доверливоста на информациите при рутирање е загрозена, непријателот може да ги идентификува или лоцира јазлите со прислушување при рутирањето на сообраќајот кој тие го праќаат или препраќаат. [5]

A. Автентичност

Доколку се користат јавни системи за шифрирање на клучот, паралелно се постапува со автентичноста и интегритетот на информациите при рутирањето, бидејќи дигиталните потписи се применуваат и за потврдување на потеклото на податоците и за нивниот интегритет. Без било каква заштита на интегритетот, напаѓачот ќе може да уништува пораки, да манипулира со заглавијата на пакетите, па дури и да генерира лажен сообраќај, така што постапките нема да може да се разликуваат од грешки на хардверот или мрежата. Автентичноста на податоците при рутирањето е од суштинско значење, така што јазлите може да го потврдат изворот на нови или променети информации при рутирањето. Ако автентичноста не е загарантирана непријателот би можел да извршува напади со имитирање, да го пренасочува сообраќајот на произволни дестинации, па дури и да ја испомеша структурата на рутирањето, така да поврзувањето во ad-hoc мрежата биде сериозно прекинато. Во најлош случај, напаѓачот може да ги изврши своите постапки и да ја напушти мрежата без да се смета за натрапник. Мрежната безбедност е во одреден дел поврзана со автентичноста, а сообраќајот при рутирањето мора да остави траги, така што која било страна која испраќа информации при рутирањето не може подоцна да го негира ширењето на податоци до други делови на мрежата. Податоците за управување со мрежата имаат слични барања за безбедност како и сообраќајот при рутирањето. Информациите за управувањето мора да бидат заштитени од објавување, доколку во нив се содржат ранливи информации, како што се податоците за статусот каде што јазлите се собираат. Уште поважна е заштитата од напади на фалсификување и имитирање при управувањето со сообраќајот. На пример, ако информациите за статусот кои јазлите ги испраќаат до системот за управување не се потврдени или заштитени од напади на интегритетот, штетен јазол може да ги фати валидните информации и наместо тоа да испрати неправилни податоци за статусот. Ова може да доведе до погрешни претпоставки за состојбата на јазлите во рамки на системот за управување и да доведе до употреба на невалидни податоци за конфигурацијата, како реакција на забележаните промени на статусот на јазлите. Очигледно е дека нападите со имитирање можат да имаат сериозни и непредвидливи последици врз разменетите информации за конфигурација, особено ако непријателот може во исто време да го контролира испраќањето на информации за статусот од јазлите. Освен тоа, бидејќи во ad-hoc мрежите мануелната конфигурација на јазлите може да биде невозможна, податоците за конфигурација може динамички и по барање да се разменуваат, со што операциите за управување уште повеќе се ранливи на гореспоменатите напади. Во најлош случај, непријателот може произволно

да конфигурира било кој јазол и на тој начин да го контролира системот за управување, што може да ги протолкува разгледаните недоследности како „природни“ неуспеси, а не како штетни активности настанати од активен напаѓач. [8]

V. Безбедност при управување со клучеви

Во ad-hoc мрежите безбедноста се базира на употребата на соодветен клуч за управување со системот. Бидејќи ad-hoc мрежите значително се разликуваат едни од други во многу аспекти, потребен е систем за управување со клучеви што е ефикасен и зависен од средината. За да може да се заштитат јазлите со користење на шифрирање, на пример од прислушување, јазлите мора да имаат склучено меѓусебен договор за заедничка тајна или да имаат разменеувано јавни клучеви. За ad-hoc мрежите кои многу брзо се менуваат, размената на клучеви за шифрирање може да биде адресирана на барање, а со тоа да не се претпоставува за претходно преговараните тајни. Во помалку динамични средини, клучевите може да бидат взаемно проактивно договорени, па дури и мануелно конфигурирани. Ако се применува шифрирање на јавниот клуч, целиот заштитен механизам се потпира на безбедноста на приватниот клуч. Како резултат на тоа, бидејќи физичката безбедност на јазлите може да биде слаба, приватни клучеви треба доверливо да се чуваат во јазлите, на пример, да бидат шифрирани со системски клуч. За динамичните ad-hoc мрежи ова не е посакувана функција и на тој начин безбедноста на приватниот клуч мора да биде загарантирана со соодветна хардверска заштита (смарт картички) или со дистрибуција на клучот во делови на неколку јазли. Хардверската заштита, како таква, сепак не е соодветно решение за спречување на нападите. Во ad-hoc мрежите централниот пристап во управувањето со клучеви може да не биде достапна опција, бидејќи може да не постојат никакви централизирани ресурси. Освен тоа централизираните пристапи се ранливи поради единствената точка на неуспех. Механичкото умножување на приватни клучеви или други информации не е адекватен заштитен пристап, бидејќи, на пример, во тој случај постои поголема можност приватните клучеви на јазлите да бидат компромитирани. Со оглед на тоа, потребен е пристапот на распространетост при управувањето со клучеви за секој систем за шифрирање кој се користи. [6]

VI. Закани на ad-hoc мрежите и видови закани

Нападите врз ad hoc мрежите можат да бидат поделени во две групи:

- Пасивни напади кои типично вклучуваат само прислушување на податоци.
- Активни напади кои вклучуваат дејства извршени од страна на непријатели, на пример умножување, промена и бришење на разменетите податоци.

Слика 4. Видови на напади

Еден напад се смета за активен кога прави големи трошоци на енергија се со цел да изврши закана, додека за разлика од активните, пасивните напади се во главно со недостаток и имаат за цел да заштедат енергија. Јазлите кои што вршат активни напади со цел да им наштетат на други јазли со прекин на мрежата се сметаат за злонамерни, додека јазлите кои што вршат пасивни напади, со цел да заштедат батерија за своите комуникации се сметаат за себични напади.

Покрај предходно споменатата поделба постои и друга поделба на нападите и тоа на надворешни и внатрешни.

Надворешните напади обично се напади кои се насочени, на пример, кон случаеви како што се: предизвикување метеж, ширење на неточни информации при рутирање, спречување на услуги да работат правилно или нивно целосно затворање. Надворешните напади обично може да се спречат со користење на стандардните безбедносни механизми, како што се мрежни бариери, шифрирање итн.

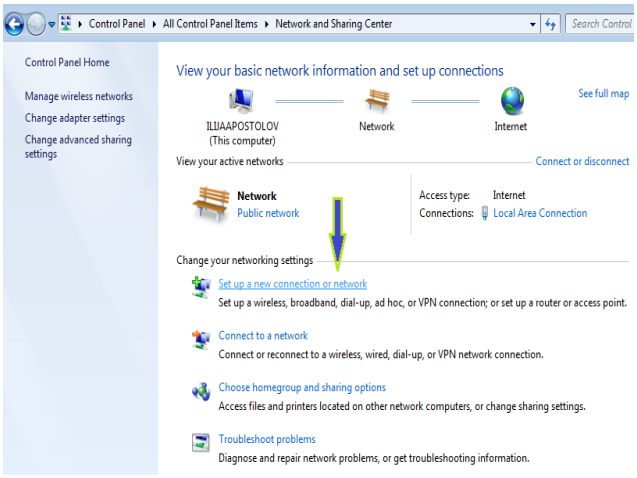
Внатрешните напади обично се посериозни напади, бидејќи штетните внатрешни јазли веќе припаѓаат на мрежата како овластен член и на тој начин се заштитени со безбедносните механизми на мрежата и услугите кои тие ги нудат. На тој начин, таквите штетни внатрешни членови, кои можат дури и да работат во група, можат да користат стандардни безбедносни средства за да ги заштитат своите напади. Овие штетни членови се нарекуваат компромитирани јазли, бидејќи нивните акции ја загрозуваат безбедноста на целата ad-hoc мрежа. [9]

A. Рутирање на ad-hoc мрежа

Современите протоколи за рутирање кај ad-hoc мрежите добро се справуваат и со динамичното менување на топологијата, но не се дизајнирани за да се приспособат на одбраната од штетните напаѓачи. Ниту еден од стандардните протоколи не ги фаќаат заедничките безбедносни закани и не обезбедуваат насоки за да го обезбедат рутирањето. Рутерите неформално разменуваат мрежни топологии со цел да воспостават правци помеѓу јазлите, што е уште една потенцијална цел за штетните напаѓачи кои имаат намера да ја пробијат мрежата. Надворешните напаѓачи вметнуваат многу погрешни информации при рутирањето, ги повторуваат старите информации или ги изобличуваат информациите при рутирањето, со цел да се прегради некоја мрежа или да ја преоптоварат мрежата со повторени преноси и неефикасно рутирање. Кај внатрешните компромитирани јазли потешко доаѓа до откривање, но и потешко се прави корекција. Информациите при рутирањето потпишани од страна на секој јазол нема да работат, бидејќи компромитираните јазли можат да генерираат валидни потписи со користење на нивните приватни клучеви. Откривањето на компромитирани јазли преку информациите при рутирањето, исто така, е тешко поради динамичната топологија на ad-hoc мрежите. Протоколите за рутирање кај ad-hoc мрежите мора да се справуваат со застарените информации при рутирање, за да се приспособат на динамичната промена на топологијата. Лажните информации при рутирањето кои се генерирани од компромитирани јазли, исто така, можат да се сметаат како застарени информации при рутирање. Сè додека постои доволен број на важечки јазли, протоколот за рутирање треба да биде способен да ги заобиколи компромитираните јазли, но за тоа треба да постојат повеќе неповрзани правци помеѓу јазлите. Доколку на постоечките има грешки, протоколот за рутирање треба да биде способен да користи алтернативен пат.[10]

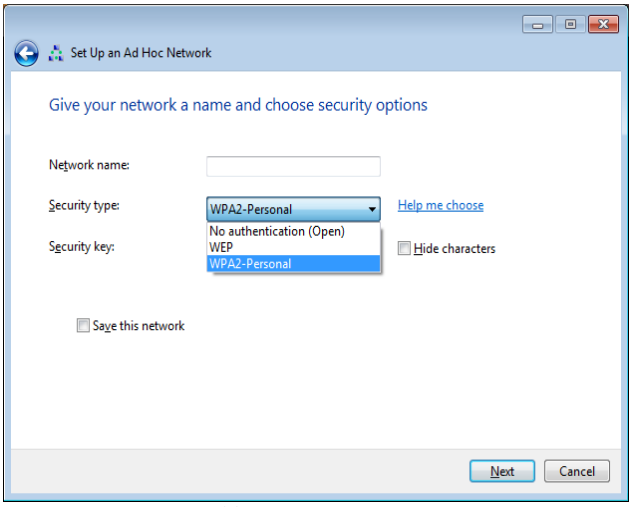
VII. КРЕИРАЊЕ AD-HOC МРЕЖА КАЈ WINDOWS 7 OS

Во овој дел ќе биде опфатено креирањето на ad-hoc мрежа кај Windows 7 оперативни системи. Ad-hoc мрежата е всушност привремена врска помеѓу компјутери и уреди кои се користат за одредена намена, како што е на пример размена на документи за време на состанок или играње на мултиплеер компјутерски игри. Исто така, може привремено да споделиме интернет конекција со други корисници на ad-hoc мрежата, со тоа што другите корисници немаат потреба да поставуваат своја интернет конекција. За да се воспостави ad-hoc мрежа потребно е на нашиот компјутер да имаме инсталирано безжичен адаптер. За воспоставување пристапуваме преку ***Control Panel > Network and Sharing Center*** и ја избираме опцијата ***Set up a new connection or network.***



Слика 5. Креирање на ad-hoc мрежа

Потоа ни се појавува прозорец каде што ја одбираме опцијата ***Set up a wireless ad hoc (computer-to-computer) network*** и ги следиме понатамошните чекори за сетирање на мрежата. На Слика 6 е опишан делот каде што одбираме име на мрежата, безбедносен тип на мрежата и третото поле е за внесување на сигурносен клуч.



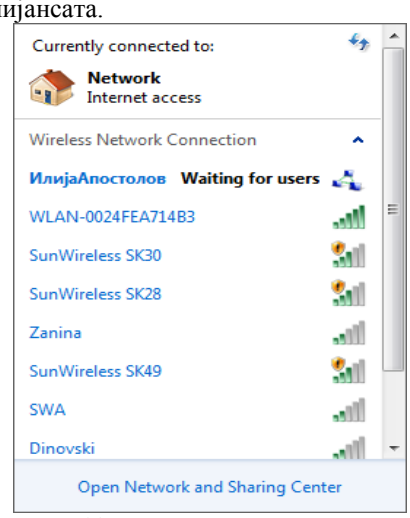
Слика 6. Подесување на ad-hoc мрежа

Како што можеме да забележеме има три сигурносни типови на мрежа и тоа WPA2-Personal, WEP и Open. Секој тип на мрежа има свои карактеристики. Доколку се одлучиме за мрежа од сигурносен тип Open, во тој случај секој безжичен адаптер има пристап до нашата мрежа без да внесува сигурносен клуч. Најчесто користениот стандард за енкрипција на податоци при безжичен трансфер, WEP (Wired Equivalent Privacy), се покажа дека

е лесно пробивлив дури и кога е добро конфигуриран. WPA2 (Wi-Fi Protected Access) стандардите за енкрипција, кои стапија во употреба во 2003 година, беа создадени за да го решат овој проблем и затоа се сметаат како најбезбеден сигурносен тип на мрежа. Оваа технологија ги имплементира задолжителните елементи на IEEE 802.11i спецификацијата. Всушност, WPA2 се базира на RSN (Robust Security Network) механизмот, кој обезбедува поддршка за сите на сите механизми од WPA2, како и:

- Појака криптирачка и автентикациска поддршка за инфраструктурната и ad-hoc мрежата (WPA е повеќе концентриран на инфраструктурната мрежа);
- Намалено оптеретување при изведувањето на клучевите за време на WLAN автентикацискатa размена;
- Поддршка за опотунистичко кеширање на клучевите за намалување на оптеретувањето при роамингот помеѓу пристапните точки;
- Поддршка за пред-автентикација, каде станиците пред роамингот ја комплетираат IEEE 802.1X автентикацискатa размена и
- Поддршка за CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) криптирачки механизам базиран на AES (Advanced Encryption Standard) шифрирањето, кое е искористено како алтернатива за TKIP (Temporal Key Integrity Protocol).

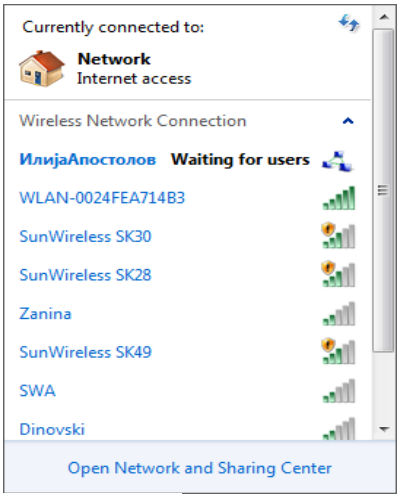
Од март, 2006 година, WPA2 безбедносниот механизам е задолжителен за сета нова опрема која е сертифицирана од Wi-Fi алијансата.



Слика 7. Креирана ad-hoc мрежа

Изборот на безбедносниот механизам кој ќе се искористи зависи од осетливоста на информациите кои се пренесуваат во ad-hoc мрежата, иако се препорачува да се искористи најдоверливиот (WPA2) механизам.

По одбирањето на сигурносниот тип на мрежа, доколку сакаме да споделиме интернет конекција до останатите корисници во нашата мрежа одбираме ***Turn on Internet connection sharing***. Нашата ad hoc мрежа е спремна за користење.[11] [12]



Слика 7. Креирана ad-hoc мрежа

VIII. Заклучок

Ad-hoc мрежното поврзување, како што може да се види од проблемите кои постојат во овие мрежи и решенијата кои произлегуваат од нив, сепак е една неистражена област. Протоколите за управување со клучеви сè уште се многу скапи и не ја гарантираат безбедноста. Постои потреба протоколите за рутирање во ad-hoc мрежите да се направат побезбедни и посилни за да се прилагодат на потребите на барањата на овие мрежи. Флексибилноста, леснотијата и брзината со која овие мрежи може да се постават навестуваат дека тие ќе добијат поширока примена. Ова ги остава ad-hoc мрежите широко отворени за истражување за да се исполнат барањата за примена.

Библиографија

[1] J. Jonsson, *On the Security of CTR + CBC-MAC*, Selected Areas in Cryptography 2002, pp. 76-93
[2] M. Meyers, *Managing and Troubleshooting Networks*, Networks, McGraw Hill, 2004, ISBN 978-0-07-225665-9.
[3] T. Krag and S. Buettrich, *Wireless Mesh Networking*, O'Reilly Wireless Dev Center, January 2001.
[4] S. Viehbock, Brute forcing Wi-Fi Protected Setup, 26 December 201, Available:http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
[5] J. V. Rantwijk, *WPA key calculation - from passphrase to hexadecimal key*, December, December 2006, Available: http://jorisvr.nl/wpapsk.html
[6] A. Bittau, M. Handley and J. Lackey, *The Final Nail in WEP's Coffin*, IEEE Symposium on Security and Privacy, May 2006, pp:400.
[7] *The handbook of ad hoc wireless networks*, CRC Press, Inc. Boca Raton, FL, USA, December 2002.
[8] Security, Available: http://www.dossiere.com/security.
[9] Adam Burg, "Ad hoc network specific attacks ", Seminar on Ad hoc networking: concepts, applications, and Security, Technische Universität München, 2003.
[10] R.T. Carroll, *Ad hoc hypothesis*, The Skeptic's Dictionary, February 2009, Last update 94 January 2012, Available: http://www.skepdic.com/adhoc.html.
[11] *Set up a computer-to-computer (ad hoc) network*, Available: http://windows.microsoft.com/en-US/windows-vista/Set-up-a-computer-to-computer-ad-hoc-network
[12] *No response to 802.1X authentication requests after authentication fails on a computer that is running Windows 7 or Windows Server 2008 R2,* 2010-03-08, Available: http://support.microsoft.com/kb/980295

- -

Summary

Security using Wireless Ad hoc Networks

Abstract – Wireless networks are solutions that allow connecting computer networks to transmit data on open and closed locations, transfer through Internet connectivity and use all the benefits of networking. Wireless ad hoc network is a collection of nodes/end stations that communicate with each another, forming multihot radio network and maintaining connectivity in a decentralized manner, without a central server. They create a temporary connection, where some of the devices are members of the network only for the duration of the communication session. Each node in the ad hoc network acts as a host and as a router, which means that the network control is distributed among the nodes. While the nodes communicate over wireless links they have to face the effects of radio communication, such as noise, signal attenuation with distance and interference. The purpose of this paper is to consider the principle of operation of wireless ad-hoc networks and examine the security mechanisms in these networks, which, by their nature are significantly more specific than other wireless networks. At the end a practical example of properly and safely creation of wireless ad-hoc network in Windows 7 OS is shown.