УДК: 004.738.056

ФРЕКВЕНТНОТО ПОТСКОКНУВАЊЕ КАКО МЕТОД ПРОТИВ НАПАДИТЕ СО ПОПРЕЧУВАЊЕ

Цветаноска Верче, М-р Митко Богдановски, Доц. Д-р Сашо Гелев
Европски Универзитет – Охрид, Р. Македонија
verce_19_cvet@hotmail.com, {mitko.bogdanoski, saso.gelev}@eurm.edu.mk

Апстракт - *Иако нападите со попречување кај безжичните мрежи спаѓаат во група на напади кои се најтешки за спречување, нивното забележување, а уште повеќе нивното санирање, претставуваат вистински предизвик. Постојат повеќе техники за откривање и борба против нападите со попречување. Еден од методите за избегнување на овие напади е употребата на фреквентно потскокнување. Фреквентното потскокнување е прочуен пристап по неговото ублажувачко дејство врз ефектите од нападот со попречување. Цел на овој труд е да се прикажат можностите на фреквентното потскокнување, како едно од решенијата за намалување на ефектот на нападите со попречување, како и да се разгледаат и анализираат различните видови фреквентни потскокнувања кои се во употреба.*

Клучни зборови – *проактивен, реактивен, фреквентно, потскокнување, попречување.*

1. ВОВЕД

Попречувањето на безжичните мрежи претставува голем проблем, кој што е поттикнат од самата природа на безжичните мрежи, како отворен и споделен медиум за пренос. Попречувачот во безжичните мрежи вметнува голема количина на шум,или интерференција. Целта при ваквата акција на попречувачот е да попречи легален сообраќај, примање и испраќање на легални пораки, или одбивање на некоја услуга.

Достапноста на комерцијалните уреди има големо влијание врз зголемениот ефект и зачестеност на нападите со попречување.[1] [2]

Денешните уреди се направени да заштедуваат енергија, со што попречувачите имаат повеќе време да дејствуваат врз мрежата, а со тоа и да ги дознаат тајните кои ги крие истата. [3]

Постојат два вида на попречувачки напади:

1. Напади во кои попречувачот го знае редоследот на потскокнување по фреквенциите - ваквиот вид на напади се најтешки за идентификување и спречување, и
2. Напади во кои попречувачот не го знае редоследот на потскокнување по фреквенции, а исто така нема ниту други споделени информации меѓу јазлите кои комуницираат.

Вториот вид на напади може да се решат со помош на фреквентното потскокнување, од таа причина што попречувачот не користи толку софистицирана опрема со помош на која ќе го открие нашиот редослед на потскокнување.[4]

Фреквентното потскокнување од секогаш се сметало како ублажувачка техника против нападите со попречување и според неговата природа тоа може да се справи само со напади од теснопојасни попречувачи, кои може да преплават само неколку фреквенции, а не против широкопојасните, кои буквално можат да ги преплават сите фреквенции.

Како што е познато, 802.11 работи на неколку фреквентни канали, па ако во непосредна околина се наоѓаат повеќе попречувачи кои попречуваат на различни канали од оној на кој моментално работи 802.11 уредот, фреквентното потскокнување може дополнително да го зголеми ефектот на попречувачите.[3]

На фреквентното потскокнување како техника и на нејзината ефективност влијаат два фактори, а тоа се:

1. Бројот на ортогонални канали кои може да се користат.
2. Фреквентното разделување помеѓу овие ортогонални канали.

Се тврди, според досега направените истражувања, дека кога легитимните парови работат на канал кој е ортогонален на тој што е користен од попречувачот, автоматски на тој начин се заштитува линкот, но сепак не до толкава мера за да не бидат намалени перформансите на мрежата или да не биде намален капацитетот кој го постигнале легитимните парови.[5]

2. ПОПРЕЧУВАЧ НА CSMA/CA МРЕЖА

Како што веќе споменавме, попречувачот постојано испраќа сигнали кон медиумот со цел да спречи легитимна комуникација и размена на податоци на каналот.

Попречувачот ги остварува своите замислени цели во CSMA/CA мрежата (пр.802.11), преку искористување на две нејзини функционалности на каналот, кои во случајов всушност претставуваат нејзини слабости:

1. MAC протоколот побарува од тој што испраќа да го слуша медиумот дали е зафатен, пред испраќањето на своите пакети. Ова му помага на попречувачот на тој начин што, во негово присуство на медиумот за пренос, јазелот кој испраќа секогаш ќе ја одложува својата акција.
2. Пакетите на попречувачот се судруваат со легитимните пакети кај примачот.

Како што може да се заклучи и двата ефекти предизвикуваат голема деградација на мрежата, од причина што не може да се изврши легитимна комуникација, примање и испраќање на пораки и барања, односно попречувачот на ваков начин прави одбивање на услуги. [5]

3. СТРАТЕГИИ НА ФРЕКВЕНТНО ПОТСКОКНУВАЊЕ

Постојат четири стратегии на фреквентно потскокнување кои се користат и тоа реактивно, проактивно, координирано и некоординирано фреквентно потскокнување [6][7][8]. Поради лесната имплементација, проактивното фреквентно потскокнување најчесто се применува како контра напад против попречувачите, но вреди да се спомнат и другите стратегии, за да се увидат предностите и недостатоците меѓу истите.

3.1. Проактивно фреквентно потскокнување

Во шемата на проактивното фреквентно потскокнување парот на примопредаватели кои формираат врска се префрлаат на друг канал на секои k секунди, без разлика на тоа дали има или нема попречувач на тековниот канал.

Во [6] е предложено проактивно фреквентно потскокнување со псевдо-случајно потскокнување на каналот, а во [9] брзо фреквентно потскокнување, но и двете не го сметаат spill преливањето на енергијата помеѓу соседните ортогонални канали.

Проактивното фреквентно потскокнување претставува добра метода за соочување со нападите со попречување на тој начин што е намален бројот на скокови за единица време и нема потреба за постојано проверување за постоење на попречувач, но сепак, во зависност од тоа како системот е изграден, проактивното фреквентното потскокнување може да претставува закана за перформансите на мрежата и губење на капацитетот при префрлувањето меѓу каналите. За добро изградените системи, ваквите загуби се многу мали.

3.2. Реактивно фреквентно потскокнување

Реактивното фреквентно потскокнување работи на таков начин што јазолот го менува својот канал само во случај кога е забележано постоење на попречувач. Менувањето на каналот мора да биде синхронизирано од двете страни, на тој начин што кога едниот јазол го менува својот канал тогаш и другиот на некој начин треба да го утврди тој настан и тој да се префрли на истион канал.

Во [7] е предложено реактивно фреквентно потскокнување, но каналот на кој двата јазли треба да се префрлат е предвреме одреден.

Оваа стратегија е се уште во истражување, познати се погодностите од нејзиното користење, но сепак во пракса не е применета.

Можните предизвици и последиците од користењето на ваков вид на стратегија се синхронизација, скалабилност, губење на пакети и сл.

3.3. Некоординирано случајно фреквентно потскокнување

Некоординираното фреквентно потскокнување е стратегија со која два јазли комуницираат преку множество од познати фреквентни канали на некоординиран и случаен начин. Целта при користењето на оваа стратегија е што повеќе да се избегне знаењето на попречувачот за редоследот на потскокнување по фреквенциите, а во исто време успешно да се пренесе дадена порака. За остварување на оваа стратегија потребно е испраќачот и примачот да примаат и испраќаат податоци на ист фреквенциски канал.

Пораката која се праќа, пред да се испрати, потребно е да се раздели на повеќе фрагменти и на тој начин поделената порака се испраќа преку голем број на испраќања, еден фрагмент после друг.

При ваквиот метод на работа, за успешно праќање на пораката и комплетирање на сите фрагменти, мора примачот да слуша на правилниот канал.

Протокот со ваквата комуникација е намален од таа причина што испраќачот мора повеќе пати да испраќа еден ист фрагмент додека тој успешно не биде примен од страна на приемникот. Исто така е констатирано дека веројатноста да се попречи пораката со оваа стратегија е иста со координираната стратегија на фреквентно потскокнување, со таа разлика што попречувачот за секој фрагмент кај некоординираниот случаен начин на фреквентно потскокнување ќе мора да ја одреди фреквенцијата на пренос.[8]

3.4. Координирано фреквентно потскокнување

Координираното фреквентно потскокнување се смета како спротивна страна на некоординираното случајно фреквентно потскокнување. Кај оваа стратегија на фреквентно потскокнување постои редослед по кој ќе се менуваат и прескокнуваат фреквенциите, но исто

така потребно е испраќачот и примачот да слушаат на ист фреквенциски канал.

И кај оваа стратегија пораката се дели на фрагменти, но за разлика од некоординираното случајно фреквентно потскокнување, веројатноста дека пораката ќе стигне цела е многу поголема. Кај некоординирано случајно фреквентно потскокнување загубата на фрагменти се зголемува со зголемениот број на обиди за пренос.

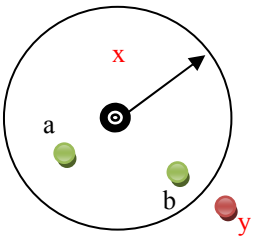
Како стратегија за борба против нападите со попречување, координираното фреквентно потскокнување може многу брзо да биде совладано, од самиот факт што попречувачите располагаат со врвна техника која за многу кратко време може да ја пронајде секвенцата на менување на фреквенции. Оваа стратегија може да се користи за послаби напади, односно против попречувачи кои не користат многу софистицирана опрема.

4. ОСОБИНИ НА ФРЕКВЕНТНО ПОТСКОКНУВАЊЕ

Фреквентното потскокнување работи на тој начин што кога два јазли комуницираат меѓу себе тие комуницираат на иста фреквенција. Кога попречувачот го зафаќа каналот на кој работат јазлите, тогаш тие одбираат друга фреквенција на која ќе работат. Изборот на друга фреквенција може да биде случаен или претходно утврден.

4.1. Како влијае бројот на ортогонални канали

Да земеме во предвид сценарио кое изгледа како на Сликата 1. Во ова сценарио се претставени попречувачите x и y, кои ја попречуваат комуникацијата помеѓу јазлите a и b.



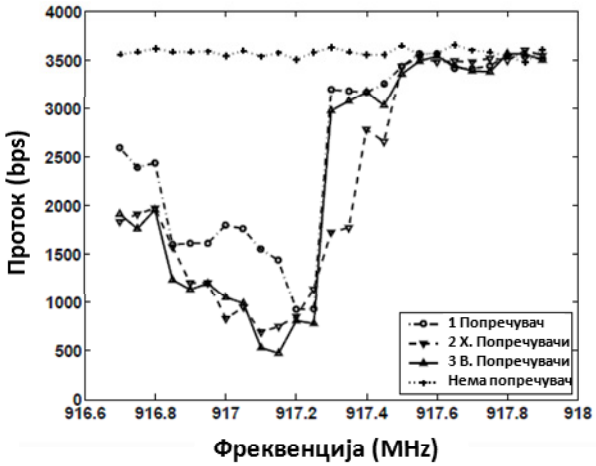
Слика 1. Сценарио на еден систем на јазли и попречувачи.

Со цел да се разбере фреквентното потскокнување, важно е да се разбере природата на интерференцијата, односно мешањето кое се јавува помеѓу различни канали, со цел при менувањето на фреквенцијата јазлите да се префрлат на чист канал. Ако попречувачот користи иста опрема како и јазлите a и b, потребно е да се дознае колку ортогонални канали се достапни, за да префрлувањето се изврши на еден од овие канали. Од друга страна, ако попречувачот не ја користи истата опрема како и јазлите, тогаш мора на некој начин јазлите да дознаат за начинот на кој се генерира попречувачкиот сигнал од страна на попречувачот, или мора да го дознаат неговото однесување, со што би можеле да се префрлуваат само на безбедни канали.

Како што е познато, бројот на ортогонални канали кај 802.11b е 3, додека кај 802.11a е 12 [6] [9].

4.1.1. Експериментално одредување ортогоналност на канали

Според експиментот направен во [7], со користење на Berkeley уреди, експериментално е утврден бројот на ортогонални канали. Во овој експеримент два јазли комуницираат како испраќач и примач, при што меѓу себе разменуваат континуирани пакети со иста големина. Стандардната фреквенција на уредите е 916.7 MHz. Резултатите од овој експеримент се прикажани во Слика 2 .



Слика 2. Експериментално одредување ортогоналност на канали

Во овој резултат се забележува дека кога сите уреди испраќаат со стандардна фреквенција од 917.5 MHz, тогаш капацитетот помеѓу два јазли кои комуницираат значително се намалува за разлика од случајот кога во близина или помеѓу јазлите би немало попречувачи.

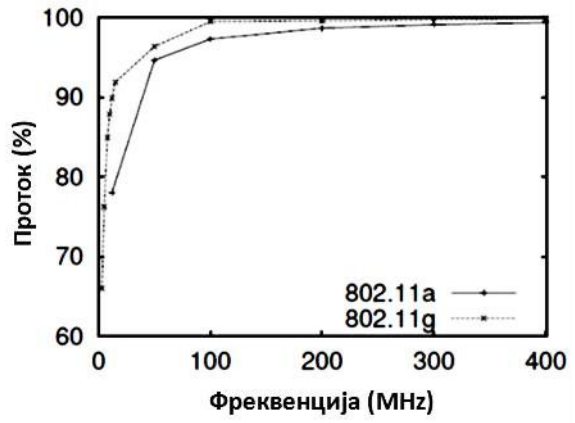
Понатака, поигрувајќи со големината на фреквенцијата која постојано и различно се доделува, се забележува дека се додека фреквенцијата не се искачи над 917.5 MHz, помеѓу јазлите ќе постои интерференција и намален капацитет, а во спротивен случај, значи кога јазлите имаат фреквенција над 917.5 MHz, помеѓу истите нема интерференција. Исто така, се доаѓа до заклучок дека разликата помеѓу два ортогонални канали мора да биде најмалку 800 KHz.

Кај фреквентното потскокнување, ако јазлите кои комуницираат и попречувачите ги следат правилата на MAC протоколот, тогаш во никој

случај капацитетот помеѓу нив не може да биде нула, а во обратен случај тој може да биде нула.

4.1.2. Како влијае бројот на ортогонални канали

Според истражувањата направени користејќи фреквентно потскокнување [5],[6],[7],[10] и [11], се доаѓа до заклучок дека бројот на ортогонални канали и нивната соодветна оддалеченост се пресуден фактор за ефикасноста на фреквентното потскокнување при обидот за соочување со попречувачите.



Слика 3. Ефикасност на фреквентното потскокнување во зависност од бројот на канали

Од истражувањето направено во [5], како што може да се види и на Сликата 3, се заклучува следното: кога бројот на ортогонални канали би бил приближен до 100 или повеќе, тогаш фреквентното потскокнување би била многу ефикасна техника против попречувањето и мрежата многу бргу би можела да го повраќа својот капацитет, иако во системот постојат и попречувачи. Причината лежи во тоа што во овој случај би имале повеќе канали и со тоа јазлите ќе имаат на располагање повеќе фреквенции на кои би потскокнувале и со тоа самиот систем би бил покомплициран за попречувачот. Во овој случај попречувачот ќе треба да пребарува преку многу фреквенции (канали), со што се ограничуваат и неговите можности во однос на достапната енергија која му е на располагање и сретствата кои може да си ги дозволи за опрема која ќе може да управува со таков систем.

5. КОИ СЕ ОГРАНИЧУВАЊАТА НА ФРЕКВЕНТНОТО ПОТСКОКНУВАЊЕ

Фреквентното потскокнување е добро во соочување со попречувач кој попречува тесен појас, односно е во можност на поплавување на одреден број на фреквенции, а не на сите фреквенции во множеството фреквенции со кои располага 802.11. Доколку попречувачот би можел да ги преплави сите фреквенции, тогаш на мрежата и се суди пропаст, т.е., фреквентното потскокнување на никој начин не може да се справи со неговиот противник.

Исто така, големо влијание има и типот на фреквентно потскокнување кој сме го спровеле во системот, односно дали фреквенциите се задаваат на случаен начин или на веќе предодреден начин.[10]

Вториот случај, земајќи во предвид дека денес постојат голем број на комерцијални и се пософистицирани уреди, би бил поризичен. Тука, попречувачот на многу лесен начин може да го одреди редоследот според кој се менуваат фреквенциите. Во овој случај мрежата ќе се соочи со пад од самиот факт што комуникацијата помеѓу јазлите би била попречена и ќе нема можност помеѓу нив да се одвива легитимна размена на податоци.

Не дека случајното менување на фреквенции нема свои недостатоци и не дека е целосно безбедно, но сепак за попречување на ваков вид мрежа потребна е поскапа опрема и повеќе време за откривање на редоследот, но од друга страна случајното менување на канали би имало негативен ефект во однос на намалување на перформансите на мрежата, при генерирањето на случајните редоследи, а исто така и нивно откривање и синхронизација од страна на јазлите кои комуницираат.

Во истражувањата направени врз влијанијата на перформансите на мрежата дојдено е до заклучок дека ефективноста на фреквентното потскокнување ќе зависи од тоа колку попречувачот влијае на одреден ортогонален канал. [12]

Секако дека капацитетот на каналот нема да биде ист во присуство и без присуство на попречувачи во околината. Се покажало дека присуството и дејствувањето на попречувачот на даден ортогонален канал не влијае на другите престанати канали. Исто така, важен е и бројот на попречувачи кои ја напаѓаат мрежата, од што произлегува дека колку повеќе попречувачи ја напаѓаат мрежата, толку полесно истата ќе биде совладана. Еден попречувач ќе попречува еден дел од фреквенциите, друг ќе попречува друг дел од фреквенциите и на тој начин ќе се постигне голема деградација на мрежата, која може фатално да заврши. Секако, тука не се земени во предвид широкопојасните попречувачи, кои би имале поголем негативен ефект врз реализираната комуникација помеѓу два или повеќе легални примопредаватели.

Според многу истражувања се покажало дека присуството на попречувач дури и на соседен ортогонален канал (20 MHz оддалечен од легитимната комуникација) го намалува капацитетот од 6 Mbps на 3-4 Mbps.

6. ЗАКЛУЧОК

Според досегашното истражување може да се заклучи дека со оглед на фактот што

фреквентното потскокнување како техника била создадена за борба против нападите со попречување во мрежи кои работат на неколку канали, истата ја покажува својата неможност за борба против попречувачи кои може да оперираат на голем број на фреквенциски канали.

Кога станува збор за контра мерки кои се превземаат против попречувач кој е способен да работи само на неколку фреквенциски канали, би било препорачливо да се користи проактивно фреквентно потскокнување каде редоследот на фреквенции ќе биде случаен.

Пресудноста за неуспехот на фреквентното потскокнување се големиот број на комерцијални уреди достапни на јавноста, кои стануваат се пософистицирани.

Фреквентното потскокнување би била добра техника против нападите со попречување ако достапниот број на ортогонални фреквенциски канали е многу голем.

7. ЛИТЕРАТУРА

1. SESP jammers. http://www.sesp.com/.
2. WIFI Jammer http://69.6.206.229/e-commerce-solutions-catalog1.0.4.html.
3. ARES: An Anti-jamming REinforcement System for 802.11 Networks – Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V.Krishnamurthy, Christos Gkantsidis.
4. Alibi: A framework for identifying insider - based jamming attacks in multi-channel wireless networks – Hoang Nguyen, Thadpong Pongthawornkamol, Klara Nahrstedt.
5. Gaming the Jammer: Is Frequency Hopping Effective ? - Konstantinos Pelechrinis, Christos Koufogiannakis, Srikanth V. Krishnamurthy.
6. Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks. -V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein.
7. Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service -W. Hu, T. Wood, W. Trappe, and Y. Zhang.
8. Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping - Mario Strasser, Christina P¨opper, Srdjan C˘ apkun, Mario C˘ agalj.
9. Handbook of Research on Wireless Multimedia: Quality of Service and Solutions- By Nicola Cranley, Liam Murphy.
10. Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks Loukas Lazos, Sisi Liu, and Marwan Krunz.
11. Mitigating Jamming Attacks in Multi-Radio Wireless Networks - Sherif Khattab.
12. Understanding Wireless LAN Performance Tradeoffs – J.Yee and H.P –Esfahani.

Frequency hopping as a method against jamming attacks

Cvetanoska Verche, M-r Mitko Bogdanoski, Doc. D-r Sasho Gelev

European University– Ohrid, R. Macedonia, verce_19_cvet@hotmail.com

verce_19_cvet@hotmail.com, {mitko.bogdanoski, saso.gelev}@eurm.edu.mk

Abstract– *Although jamming attacks in wireless networks belong to a group of attacks that are most difficult to prevent, their detection, and even more their repairing, is real challenge. There are several techniques for detecting and combating jamming attacks. One of the methods to avoid these attacks is the use of frequency hopping. Frequency hopping has been the most popularly considered approach for alleviating the effects of jamming attacks. The aim of this paper is to show the capabilities of frequency hopping as one of the solutions for reducing the effect of jamming attacks, and to review and analyze various types of frequency hopping methods which are in use.*

Key words – *proactive, reactive, frequency, hopping, jamming.*