УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ 6.**

НАЗИВ ФАКУЛТЕТА ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ИЗВЕШТАЈ О ОЦЕНИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

I ПОДАЦИ О КОМИСИЈИ

1. Датум и орган који је именовао комисију:
   29.03.2018., Решењем бр. 012-72 /35 - 2015, Декан Факултета техничких наука на предлог Наставно-научног већа Факултета Техничких Наука у Новом Саду.
2. Састав комисије са назнаком имена и презимена сваког члана, звања, назива уже научне области за коју је изабран у звање, датума избора у звање и назив факултета, установе у којој је члан комисије запослен:
   - **Др Мирослав Поповић**, редовни професор, изабран у звање 17.07.2002. , Универзитет у Новом Саду, ФТН; УО: Рачунарска техника и рачунарске комуникације, председник;
   - **Др Никола Теслић**, редовни професор, изабран у звање 14.04.2011. , Универзитет у Новом Саду, ФТН; УО: Рачунарска техника и рачунарске комуникације, члан;
   - **Др Мило Томашевић**, редовни професор, изабран у звање 15.07.2015. , Универзитет у Београду, Електротехнички факултет; УО: Рачунарска техника и информатика, члан;
   - **Др Драган Кукољ**, редовни професор, изабран у звање 19.09.2003., Универзитет у Новом Саду, ФТН; УО: Рачунарска техника и рачунарске комуникације, члан;
   - **Др Илија Башичевић**, ванредни професор, изабран у звање 11.06.2014., Универзитет у Новом Саду, ФТН; УО:Рачунарска техника и рачунарске комуникације, члан;

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме:

   Миодраг (Сава) Петковић

2. Датум рођења, општина, држава:

   01.10.1963., Инђија, СФРЈ

3. Назив факултета, назив студијског програма дипломских академских студија – мастер и стечени стручни назив:
   ФТН Нови Сад, смер аутоматика и рачунарска техника, дипломирани инжењер електротехнике.
4. Година уписа на докторске студије и назив студијског програма докторских студија

5. Назив факултета, назив магистарске тезе, научна област и датум одбране:
   ФТН, „Приступ пројектовању заштићеног информационог система у рачунарски независној и рачунарски зависној фази“, Рачунарска техника и рачунарске комуникације ,15.07.1999

6. Научна област из које је стечено академско звање магистра наука: **Рачунарска техника и рачунарске комуникације**

III НАСЛОВ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Прилог развоју методе за детекцију напада ометањем услуге на Интернету
(енгл.: A contribution to the method for detection of denial of service attacks in Internet)

IV ПРЕГЛЕД ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Докторска дисертација кандидата написана је на српском језику на 110 страна формата А4. Садржи 11 поглавља, у којима се налази 55 слика и 7 табела. Дисертација обухвата 84 литературна навода. Поглавља у дисертацији су:

1. Увод
2. Напад ометањем услуге
3. Теоријске основе детекције аномалија саобраћаја
4. Фази логика
5. Такаги-Сугено-Канг модел
6. Опис постојећих решења
7. Одабир инфраструктуре за истраживање
8. Синтеза детектора
9. Резултати
10. Предлог идејног решења за примену ТСК-ФС методе на хардверским компонентама
11. Закључак

Дисертација такође садржи и кључне докуметацијске информације, садржај, списак слика, списак табела, номенклатура коришћених појмова и референце на коришћену литературу.

V ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Истраживање изложено у дисертацији бави се развојем новог метода за детектовање напада ометањем услуге на Интернету и постављен је циљ да се постојећи методи побољшају додавањем неуро-фази степена обраде саобраћаја са мреже.

Прво поглавље уводи појам напада ометањем услуге. Представљен је укратко метод детекције применом ентропије. Истакнут је проблем постојећих метода базираних на статистичким аномалијама а то је велики број лажних детекција. Постављен је јасно и прецизно циљ истраживања да се у другој фази детекције, после примене стандардних метода базираних на ентропији, додатном применом Такаги-Сугено-Канг неуро-фази метода, у дисертацији под називом ТСК-ФС, побољша квалитет детекције напада ометањем услуге и описани су кораци у истраживању.

Друго поглавље детаљно описује технологију напада ометањем услуге и тренутно стање овог проблема у свету. Дат је опис инфраструктуре напада заједно са начином грађења и употребе глобалне мреже - ботнета, затим мотива напада, извођења и последица напада као и последица напада. Набројани су и на занимљив начин описани познати случајеви напада. Све је то употпуњено најновијим кварталним извештајима из релевантних извора о статистици напада ометањем услуге у свету.

Треће поглавље описује теоријске основе детекције аномалија мрежног саобраћаја. Проблем квантитативног одређивања одступања од уобичајеног саобраћаја приказано је кроз три најчешће коришћене метрике у истраживањима: ентропије, сложености и самосличности. Детаљно су описане три врсте ентропије које се користе у истраживању као први корак детекције напада ометањем услуге.

Четврто поглавље приказује место фази логике у примењеном методу детекције.

Пореде се два најчешће примењивана фази модела – тип Мамдани и тип Сугено и појашњава зашто је варијанта другог модела, Такаги-Сугено-Канг, применљивија на тему истраживања.

Пето поглавље детаљно описује Такаги-Сугено-Канг модел који се примењује када је структура система који се моделује у старту непозната. Једнонивоска неуронална мрежа се користи за одређивање структуре система који се састоји из повезаних подсистема. Кластери тачака и Н-димензионалном систему представљају подсистеме. На тако формиране подсистеме примењује се фази логика.

Шесто поглавље описује постојећа достигнућа и сазнања из области истраживања, као и постојеће методе детекције напада ометањем услуге.

У седмом поглављу је описан одабир поставки експеримената. Појашњено је зашто се у већем делу истраживања користио симулиран саобраћај. Образложен је одабир софтверског симулатора, као и одабир скупова података насталих од саобраћаја скинутог са реалних мрежа. Такође је образложено које променљиве мрежног саобраћаја и променљиве из заглавља пакета ће се користити за рачунање ентропије.

У осмом поглављу описана је синтеза детектора који је реализован у дисертацији. Описан је начин израчунавања ентропије коришћењем помичног прозора којим се пригушују нагле промене. Описан је процес генерисања неуро-фази модела , процес обуке и процес детекције. За одређивање тачке промене стања, односно почетка или краја напада користи се CUSUM метод који динамички детектује промене у односу на процењену средњу вредност сигнала у ближој околини.

У деветом поглављу детаљно су описани експерименти са различитим врстама ентропије, мрежним топологијама и симулираним и реалним мрежном саобраћајем. Изведени су следећи скупови експеримената:

- Ивична топологија са симулираним саобраћајем.
- Топологија велике размере са симулираним саобраћајем.
- Експерименти са ентропијама више променљивих,
- Експерименти са унакрсном применом модела на две различите топологије
- Експерименти са реалним саобраћајем
- Експерименти са реалним саобраћајем и ентропијама више променљивих.

За сваки скуп експеримената табеларим и графичким приказом јасно су упоређени резултати примене стандардних метода, када се користи само ентропија, и када се примени ТСК-ФС метода. Показано је да се применом ТСК-ФС методе повећава осетљивост и робусност детекције, као и да се смањује број лажних детекција што је кључно за практичну примену.

У десетом поглављу дат је предлог идејног решења за извођење предложеног метода на хардверским компонентама. Показано је да се ентропија може израчунати проточним поступком тако да брзина рачунања вредности ентропије прати брзину пристизања пакета са мреже. На тај начин се знатно ублажава губитак перформанси због увођења неуро-фази метода као додатног степена обраде. Показана је и могућност паралелизовања обраде за случај истовременог праћења ентропије више променљивих.

У једанаестом поглављу дата је рекапитулација резултата истраживања и изнети

су закључци истраживања. Предложени могући правци даљег рада у области детекције напада ометањем услуге као и детекције аномалија у мрежном саобраћају.

Дванаесто поглавље садржи листу коришћене литературе, која је актуелна и адекватна теми истраживања.

VI СПИСАК НАУЧНИХ И СТРУЧНИХ РАДОВА КОЈИ СУ ОБЈАВЉЕНИ ИЛИ ПРИХВАЋЕНИ ЗА ОБЈАВЉИВАЊЕ НА ОСНОВУ РЕЗУЛТАТА ИСТРАЖИВАЊА У ОКВИРУ РАДА НА ДОКТОРСКОЈ ДИСЕРТАЦИЈИ

M23 – Радови објављени у научним часописима међународног значаја

1. Petkovic, M., Basicevic, I., Kukolj, D., Popovic, M.: Evaluation of Takagi-Sugeno-Kang fuzzy method in entropy-based detection of DDoS attacks. Computer Science and Information Systems, Vol. 15, No. 1. (2018)

M33 – Саопштење са међународног скупа штампано у целини

2. Miodrag Petković, Miroslav Popović, Ilija Bašičević, Djordje Sarić: A Hoste Based Method for Data Leak Protection by Tracking Sensitive Data Flow. ECBS, page 267-274. IEEE Computer Society, (2012).

M64 – Саопштење са скупа националног значаја штампано у изводу

3. M. Petković, I.Bašićević, M. Popović, D. Kukolj "Denial-of-service attacks detection using Internet traffic entropy and fuzzy system" "Primena entropije mrežnog saobraćaja i fazi sistema u detekciji Internet napada ometanjem usluge". OSMI NAUČNO-STRUČNI SKUP "InterRegioSci 2015.", Novi Sad, decembar 2015.

VII ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА

Основни допринос истраживања представљених у овом дисертацији је да је развијен нови метод у детектовању напада ометањем услуге на Интернету који се састоји из два корака: одређивања ентропије за задате променљиве из мрежног пакета и побољшавања детекције применом неуро-фази метода.

Показано је да предложени неуро-фази метод значајно побољшава квалитет детекције напада ометањем услуге као и да и смањује број лажних детекција у односу на стандардане методе засноване на ентропији.

Детекција напада ометањем услуге предложеним неуро-фази методом робуснија тј. поуздана за шири опсег вредности конфигурационих параметара. Такође, показано је да је детекција напада ометањем услуге предложеним неуро-фази методом осетљива за нижи ниво напада у односу на методе засноване само на примени ентропије.

Даље, показано је да се комбиновањем ентропија више величина постиже најбољи квалитет детекције у експериментима са реалним саобраћајем.

Побољшане су перформансе поступка рачунања ентропије користећи проточно израчунавање. Тиме увођење додатног неуро-фази слоја у процес детекције не резултује смањењем перформанси.

На крају је предложено је решење детектора које може да се изведе помоћу хардверских компоненти. На тај начин је показано је да је изложени метод практично применљив за имплементацију у мрежним уређајима и да је ефикасан са аспекта перформанси и да не уноси значајну додатну обраду.

VIII ОЦЕНА НАЧИНА ПРИКАЗА И ТУМАЧЕЊА РЕЗУЛТАТА ИСТРАЖИВАЊА

Истраживање у оквиру дисертације је извршено на симулираном и реалном саобраћају. Периоди трајања напада одбијањем услуге су били унапред познати. Поређени су резултати детекције напада коришћењем неколико типова ентропије са резултатима у којима се додатно примењује предложени неуро-фази метод. Поређења су јасно приказана у облику табела и у облику 3Д дијаграма тако да дају јасну представу о побољшању детекције при примени новог метода.

Приказ дисертације је јасно структуриран, прегледан, и у складу са темом дисертације. Тумачење резултата је аргументовано, а изведени закључци проистичу из добијених резултата истраживања.

Дисертација је проверена у софтверу за детекцију плагијаризма (iThenticate).
Извештај о подударности је показао да је индекс сличности 2%.

У складу са наведеним, комисија **позитивно** оцењује начин приказа и тумачења резултата истраживања.

IX КОНАЧНА ОЦЕНА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Експлицитно навести да ли дисертација јесте или није написана у складу са наведеним образложењем, као и да ли она садржи или не садржи све битне елементе. Дати јасне, прецизне и концизне одговоре на 3. и 4. питање:

1. Да ли је дисертација написана у складу са образложењем наведеним у пријави теме

*Комисија закључује да је докторска дисертација је у **потпуности написана у складу** са образложењем наведеним у пријави теме.*

2. Да ли дисертација садржи све битне елементе

Комисија заључује да дисертација садржи све битне елементе.

3. По чему је дисертација оригиналан допринос науци

У дисертацији је описана оригинална идеја комбиновања метода примене ентропије на мрежном

саобраћају и Такаги-Сугено-Канг неуро-фази метода за детекцију напада ометањем услуге. Показано је да предложени комбиновани метод значајно побољшава квалитет детекције напада ометањем услуге као и да и смањује број лажних детекција у односу на стандардан метод заснован на ентропији. Показано је и да је детекција напада ометањем услуге предложеним методом робуснија тј. поуздана за шири опсег вредности конфигурационих параметара од познатих стандардних метода заснованих на ентропији.
4. Недостаци дисертације и њихов утицај на резултат истраживања *Комисија закључује да дисертација* ***не поседује*** *недостатке који би могли негативно да утичу на вредност постигнутих резултата истраживања.*
X ПРЕДЛОГ:
На основу укупне оцене дисертације, комисија предлаже: *Да се докторска дисертација под називом „****Прилог развоју методе за детекцију напада ометањем услуге на Интернету****“ прихвати, а кандидату одобри одбрана.*

У Новом Саду, 7. маја 2018.

_____

Др Мирослав Поповић, редовни професор

Факултет техничких наука, Нови Сад, председник комисије

_____

Др Никола Теслић, редовни професор

Факултет техничких наука, Нови Сад, члан комисије

_____

Др Мило Томашевић, редовни професор

Електротехнички факултет, Београд, члан комисије

_____

Др Драган Кукољ, редовни професор

Факултет техничких наука, Нови Сад, члан комисије

_____

Др Илија Башичевић, ванредни професор

Факултет техничких наука, Нови Сад, ментор, члан комисије

НАПОМЕНА: Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај.