РЕЦЕНЗИЯ

на дисертационен труд за придобиване на образователна и научна степен „доктор" по професионално направление 4.6 Информатика и компютърни науки (Информатика - Компютърни мрежи и архитектури)

Тема: "Изграждане на система за защита от DDoS атаки"

Автор: гл. ас. Стела Иванова Русева, катедра „Изчислителни системи", Факултет по математика и информатика, Софийски университет „Св. Климент Охридски"

Рецензент: проф. д-р Пламенка Боровска

Рецензията е изготвена в съответствие със заповед № РД38-342 от 17.07.2012 год. на Ректора на Софийски университет „Св. Климент Охридски"

Представеният за рецензиране дисертационен труд съдържа въведение, изложение от четири глави, заключение, справка за приносите, приложения (представена е част от програмния код на реализираната софтуерна система, която включва над 500 реда; списък на публикациите; списък на цитираните литературни източници). Общият обем на текста е 133 страници, в който се съдържат 20 графични фигури и 5 таблици. Списъкът на цитираната литература (общо 156 източника) съдържа 152 заглавия на английски език, 3 на руски език и 1 на български език.

1. Актуалност на разработвания в дисертационния труд проблем

В дисертацията е направен задълбочен анализ на съвременни и актуални проблеми в сигурността на компютърните мрежи.

Проблемът с DDoS атаките е сериозна заплаха за съвременното Интернет пространство.

Темата на дисертационния труд е актуална, интересна и трудна.

Акуалността на дисертацията не подлежи на съмнение.

В настоящия труд докторантката прави опит да реши проблема, като предлага универсален, комплексен подход, което прави темата на дисертацията много актуална.

Направените от докторантката обосновка на актуалността и изложените съображения са коректни и основателни.

2. Степен на познаване състоянието на проблема

Докторантката прави много задълбочен обзор на съвременното състояние на проблематиката, свързана с DDoS атаките. Извършен е подробен анализ на съвременните най-перспективни разработки. Тя демонстрира много добро познаване на изследваната област. Библиографската справка включва 156 информационни ресурси, което показва, че тя е запозната много добре с последните постижения в избраното научно направление. Направено е подробно разглеждане на резултатите от изследванията, отразени в литературните източници, което показва нейните възможности за творческа интерпретация на литературния материал.

3. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд

Дисертационният труд е прецизно оформен, като е структуриран в 4 глави, следвайки логическата последователност:

В първа глава се прави обзор на различните видове атаки "отказ от обслужване", с описание на начина на функционирането им, както и на метода за тяхното откриване и блокиране. Представено е състоянието на проблема и е предложена класификация на този род атаки. Обзорът на огромно количество информационни ресурси е сериозен принос на дисертантката. Показани са най-перспективните разработки в областта "защита на компютърните мрежи", свързана с противодействие на DDoS атаките.

Във втора глава е представен разширен анализ на подходите за изграждане на система за защита. Избрана е LAMP архитектура на сървъра. Разгледани са особеностите, възможностите и характеристиките на LAMP сървър. (LAMP – Linux, Apache, MySQL, PHP). Описани са методите и средствата за изграждане на противодействаща система срещу DDoS атаките.

В трета глава е представен модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и на защитавания сървър. Представен е модел, отчитащ загубата на пакети в мрежата, причинена от TCP SYN атака. За целта системата за масово обслужване се разделя на две подсистеми: първата описва обслужването на заявките, за които полуотворените съединения ще бъдат успешно установени, а втората - заявките, за които

няма да бъдат установени свързвания и след изтичането на таймаут ще бъдат изтрити. Получена е прагова стойност на параметъра максимално допустим брой полуотворени свързвания на сървъра.

В четвърта глава авторката разработва конкретна система за защита от DDoS атаки Ruslan. Определени са компонентите, алгоритмите, конфигурацията на елементите и настройката на параметрите, позволяващи оптимална защита на уеб сървър от DDoS атаки. Базови елементи на системата за защита Ruslan са параметрите на ядрото на ОС, TCP/IP стека, скрипт за iptables. Системата променя параметри на ядрото на ОС, основни конфигурационни файлове, съдържа допълнителни модули. Проектирани и имплементирани са елементите, чрез които се цели да бъдат избегнати проблемите, предизвикани от DDoS атаките.
Представена е експериментална проверка и анализ на получените резултати. Експериментално са обосновани двата основни параметъра, представени в математическия модел в глава 3: размер на буфера и интервал за очакване на установяване на връзка.

Дисертационният труд е добре структуриран. Като цяло описанието е коректно и задълбочено. Специфичният стил и начин на изложение на дисертационният труд потвърждават неговото авторство.

4. Съответствие на избраната методика на изследване и поставената цел и задачи на дисертационния труд с постигнатите приноси

Основната цел на дисертацията е: "Изследване на методи и начини за защита на компютърна система от DDoS атаки, които позволяват получаване на оптимална сигурност и достъпност на ресурсите."

За решаване на поставената цел се формулират следните по-конкретни задачи:

1. Определяне на оптимална конфигурация на системата за защита от DDoS атаки.

2. Създаване на модел на система за защита, описващ взаимодействието на сървъра и клиентите.

3. Разработка на алгоритми и програмна реализация на системата за защита.

4. Имплементация на комплекс от програмни средства, предпазващи от DDoS атаки и експериментална верификация на създадените средства.

Поставените задачи са адекватни на целта и са решени в необходимия обем на високо научно ниво.

Избраната методика на изследване, а именно, методите на логическия
синтез и анализ, теорията на системите за масово обслужване, елементи на математическия анализ, считам за правилна и в пълно съответствие с поставената цел и задачи на дисертационния труд, както и с постигнатите приноси.

5. Приноси на дисертационния труд

Приемам резултатите, получени в дисертационния труд, и ги оценявам както следва:

5.1. Като научни приноси оценявам следните резултати, които принадлежат към групата „нови методи за синтез и анализ и получаване и доказване на нови факти":

- Създаден е модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и на защитавания сървър. С помощта на математическия апарат на теорията на системите за масово обслужване са определени допустимите интервали за броя на полуотворени TCP връзки на сървъра.

5.2. Като научно-приложни приноси оценявам следните резултати, които принадлежат към групата „нови схеми и технологии:

- Дефинирани са базовите променливи за конфигуриране на защитните механизми за LAMP сървър за противодействие на DDoS атаките, като са определени средствата за противодействие и нивата за защита за уеб сървър. Изследвани са методите за изграждане на противодействаща система срещу DDoS атаките.
- Разработена е системата за защита Ruslan, която променя параметри на ядрото на ОС, основни конфигурационни файлове и съдържа допълнителни модули.

5.3. Като приложни приноси оценявам следните резултати, които принадлежат към групата „получаване на потвърдителни факти":

- Предложена е класификация на известните видове DDoS атаки и методи за борба с тях, като е извършен сравнителен анализ.
- Проведена е експериментална проверка на теоретичните положения в дисертацията чрез разработената система Ruslan,

като е подтвърдена способността на тази система да запазва работоспособността на сървъра.

Получените приноси в дисертационния труд оценявам като значими.

Извършена е имплементация на предложената система за защита и нейна оценка.

Получените експериментални резултати са отразени в 4 таблици и 2 диаграми.

6. Преценка на публикациите в дисертационния труд

Авторката е представила своите резултати в публикации както у нас, така и в чужбина в специализирани списания и на научни конференции. Общият брой на публикациите е 6. От тях научните статии са 2, научните доклади са 4.

Сравнявайки отделните раздели в дисертационния труд с публикациите на авторката, имащи отношение към него, установявам, че преобладаващата част от резултатите са публикувани, което говори за тяхната достоверност и обективност. Така например, в глава 1 отделните раздели съответстват на публикации № 1, 3, 4, 5, 6. Глава 2 съдържа резултати, които са публикувани в № 1, 2, 3, 5, 6. Глава 3 съдържа резултати, които са публикувани в № 2, 5, 6. Глава 4 съдържа резултати, които са публикувани в № 2, 5.

Авторката се е постарала съобразно възможностите си да доведе своите резултати до знанието на научната общност.

Не са представени материали за връзка на изследванията в дисертационния труд с научно-изследователски проекти.

7. Оценка на съответствието на автореферата с изискванията на изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд

Авторефератът, както и изложението на дисертационния труд, е оформено изключително акуратно, с множество цветни илюстрации и текстове, подпомагащо по този начин свободното четене и възприемане на представяната същност. Обемът на автореферата е премерен и изложеното в него отразява същността на целта, задачите и техните решения.

Авторефератът съдържа пълния текст на научните и научно-приложните приноси, както и списъка с публикациите, свързани с дисертацията.

8. Мнения, препоръки и бележки

Дисертационният труд е изготвен прецизно, има ясно изградена логическа структура и определено има постигнати значими научни, научно-приложни и приложни приноси.

По дисертацията и автореферата могат да се направят следните забележки и препоръки:

- Анализът на експерименталните резултати е много кратък.
- Препоръчвам към отделните оригинални глави да се добавят виждания за бъдещи изследвания на докторанта.
- Считам, че трудът е стойностен и препоръката ми е авторката да продължи изследванията в областта.

9. Заключение

Оценката ми за дисертационния труд е положителна. Дисертантката постига поставените цели и задачи в дисертационния труд. Приносите, за които дисертантката претендира, действително са получени и са дело на докторантката. Съществените приноси на дисертационния труд са отразени в научни публикации. Дисертационният труд отговаря на изискванията на закона за Развитието на академичния състав на Република България за присъждане на научната степен „доктор". Като се вземат предвид достойнствата на представения ми за рецензия дисертационен труд на тема "Изграждане на система за защита от DDoS атаки", респ. *актуалност, значимост и полезност*, оценявам ***положително*** дисертационния труд на гл. ас. ***Стела Иванова Русева*** и считам, че научното жури може да й присъди образователна и научната степен ***"доктор".***

19.08.2012 г.

Подпис:

(проф. д-р Пламенка Боровска)