NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA UNIVERZITETA U BEOGRADU

Na svojoj sednici Komisija za studije II stepena nas je odredila za članove Komisije za pregled i ocenu master rada kandidata **Vladimira Jelić**, dipl. inž., pod naslovom **„Selekcija obeležja u jednoj klasi sistema za detekciju upada u računarske mreže"**. Komisija je pregledala priloženi rad i dostavlja Nastavno-naučnom veću sledeći

IZVEŠTAJ

1. Biografski podaci

Vladimir J. Jelić je rođen 07.04.1983. godine u Sisku, Hrvatska. Završio je gimnaziju u Pančevu sa odličnim uspehom. Elektrotehnički fakultet u Beogradu upisao je 2001. godine, na odseku za Računarsku tehniku i informatiku. Diplomirao je u junu 2010. godine. Master studije upisao je na Elektrotehničkom fakultetu u Beogradu u oktobru 2010. godine na odseku za Računarsku tehniku i informatiku. Položio je sve ispite na master studijama sa prosečnom ocenom 7,80.

2. Organizacija rada

Cilj ovog rada je upoznavanje sa savremenim metodama selekcije obeležja u sistemima za detekciju upada u računarske mreže. Predmet predloženog master rada odnosi se na postupak sinteze efikasnih sistema za detekciju upada u računarske mreže (IDS – Intrusion Detection Systems) selekcijom najinformativnijih diskriminatornih obeležja u uslovima nebalansiranih obučavajućih skupova. Ova situacija je tipična za ovu klasu sistema, budući da su intruzivne aktivnosti po pravilu retki dogadjaji u odnosu na normalno ponašanje korisnika.

Ovaj rad predlaže postupak za rangiranje najinformativnijih obeležja pomoću neuronskih mreža. Predložena suboptimalna procedura meri značaj svakog pojedinačnog obeležja u zavisnosti od promene tačnosti klasifikacije prilikom uključivanja i isključivanja ovog obeležja iz radnog skupa obeležja nad kojim se vrši obučavanje.

Master rad kandidata Vladimira Jelić sadrži 48 strana teksta sa 15 slika, 7 tabela i podeljen je u tri celine.

U prvom delu rada su prezentovane teorijske osnove sistema za detekciju upada u računarske mreže. Posebna pažnja je posvećena statističkim metodama za procenu efikasnosti sistema za detekciju upada u koje spadaju: osetljivost, određenost i tačnost. Takođe, pažnja je posvećena klasifikaciji sistema za detekciju upada. Za nas je posebno bitna podela na sisteme za detekciju upada koji su zasnovani na detekciji anomalija i sistema koji su zasnovani na potpisima. U ovom radu se izučavaju sistemi zasnovani na detekciji anomalija. Prednost detekcije anomalija u odnosu na sisteme zasnovane na potpisima je ta što se detektuje ponašanje koje je novo i neuobičajeno, dok sistemi zasnovani na potpisima mogu da detektuju samo stare napade za koje već postoji potpis.

U drugom delu rada prezentovane su tehnike za detekciju anomalija. Od svih tehnika za nas su najbitnije veštačke neuronske mreže, čije su generalizacione

performanse teorijski garantovane unapred. Mogućnost rada veštačkih neuronskih mreža u prostorima obeležja visoke dimenzionalnosti (praktično neograničene dimenzionalnosti) čine ih danas najkorišćenijim sistemima u okviru različitih klasifikacionih i dijagnostičkih sistema veštačke inteligencije. U ovom radu prezentovani su osnovni principi rada za ovu klasu sistema veštačke inteligencije.

U trećem delu rada se daje teorijska postavka za nalaženja optimalnog broja obeležja u slučaju nebalansiranih obučavajućih skupova. Na ovaj način je istovremeno uspostavljeno efikasno eksperimentalno okruženje u kome se mogu izučavati metodi za selekciju obeležja merenjem performansi posmatranog sistema za detekciju upada.

3. Analiza rada sa ključnim rezultatima

Predložena metoda je evaluirana na *Darpinom KDD Cup '99* skupu podataka, koji se smatra referentnim benčmark skupom za ovu klasu problema. Eksperimenti su bili ograničeni na klasu napada *Probe*. Usled nepovoljnog uticaja nebalansiranih obučavajućih skupova pri sintezi IDS sistema, kao kriterijum performansi obučenih neuronskih mreža je uzet integralni pokazatelj AUC (Area Under Curve) koji se izvodi iz standardne ROC (Receiver Operating Curve). Analizom eksperimenralnih rezultata dobijen je skup koji sadrži 21 važno obeležje (20 obeležja je odbačeno kao nebitno). Ovom selekcijom obeležja smanjen je broj ulaznih podataka koje koristi neuralna mreža i samim tim je postignuto kraće vreme koje je potrebno za trening sistema i za proračun koji sistem izvršava prilikom detekcije upada. Smanjenjem broja obeležja smanjena je i potreba za računarskim resursima koje koristi sistem za detekciju upada.

4. Zaključak i predlog

Na osnovu izloženog Komisija sa zadovoljstvom predlaže Nastavno-naučnom veću da prihvati master rad pod naslovom „Selekcija obeležja u jednoj klasi sistema za detekciju upada u računarske mreže", i kandidatu Vladimiru Jelić, dipl. inž. odobri usmenu odbranu.

Beograd, 31.05.2013. godine

Članovi Komisije:

Dr Milan Milosavljević, redovni profesor

Prof. dr Željko Đurović