Posudek vedoucího bakalářské práce

Autor práce:	Ondřej Měkota
Název práce:	Anomaly Detection Using Generative Adversarial Networks
Studijní program:	Informatika
Studijní obor:	Obecná informatika
Rok odevzdání:	2019

Student se své práci zabývá detekcí anomálií pomocí techniky zvané Generative Adversarial Networks (GAN). Testovacími daty použitými v práci jsou anonymizované záznamy z transakcí platebními kartami. Cílem práce je vyvinout co nejspolehlivější softwarový nástroj, který pro daný požadavek k provedení transakce rozhodne, zda je oprávněná nebo se jedná o podvod, a tudíž je nutné transakci zablokovat. Správná automatická rozpoznávání podvodů může bankám ušetřit značné finanční prostředky nejen k náhradě škod, ale i mzdové prostředky analytiků zabývajících se podvody. Na druhou stranu oprávněné transakce chybně označené jako pokusy o podvody velmi znepříjemňují život zákazníkům, což může vést k odchodům ke konkurenci. Jelikož se zločinecké organizace obvykle pokouší o velký počet podvodných transakcí, stačí umět rozpoznat malou část podvodů k rozkrytí sítě. Z těchto důvodů banky preferují detekční systémy, které sice rozpoznají menší počet podvodů (tzv. úplnost), ale s velkou jistotou jsou označené transakce doopravdy podvody (tzv. přesnost).

Student při vytváření detekčního systému vychází z publikovaných výsledků, zejména Schlegl at al. (2017) a Zenati at al. (2018), které dále upravuje. Hlavním přínosem práce oproti publikaci Schlegl at al. (2017) spočívá ve výměně GAN za Wasserstein GAN a vytvoření encoderu do latentního prostoru, což vede ke zlepšení spolehlivosti a zároveň k výraznému zrychlení vyhodnocování. Dále trénování popsané v publikaci Zenati at al. (2018) nahrazeno nezávislým trénováním encoderu od trénování generátoru a kritika.

Studentem navržený systém je srovnán s nejlepšími známými nástroji pro detekci anomálií založených na učení bez učitele. K testování byla použita veřejně dostupná anonymizovaná data zvaná Credit Card Fraud Dataset (CCFD). Ke srovnání byly použity dvě metriky: Area under precision-recall curve (AUPRC) a přesnost při různých hodnotách úplnosti.

K experimentům s metodami Class Support Vector Machines (OC-SVM) a Isolation Forest student použil Python a knihovnu Scikit-learn a nastavil vhodné hyperparametry. Z měření vyplynulo, že studentova metoda AnoWGAN+e docílila nejlepší hodnotu v metrice AUPRC (0.4625), OC-SVM docílila hodnoty 0.4113 a Isolation Forest 0.1827. Dále AnoWGAN+e docílila lepší přesnosti než Isolation Forest pro všechny hodnoty úplnosti a ve srovnání s OC-SVM byla lepší v hodnotách úplnosti $0 - 0.2$ a $0.6 - 1$. Navíc při úplnosti 0.1 dosahovala metoda AnoWGAN+e téměř třetinové chybovosti (0.11) oproti OC-SVM (0.3) a při úplnosti 0.8 docílila metoda AnoWGAN+e více než dvojnásobné přesnosti (0.20) než OC-SVM (0.08).

Jelikož nelze prokázat, že v experimentech s OC-SVM a Isolation Forest byly použity nejlepší možné hodnoty hyperparametrů pro daný typ testovacích dat, tak student ještě našel publikaci od Porwal et al. (2018), ve které autoři uvádějí výsledky svých experimentů na stejných testovacích datech CCFD s použitím metody zvané k-Means ensemble. Jejich metodu též student jednoznačně překonává, protože hodnotu AUPRC mají méně než poloviční (0.2231). Autoři dále uvádí, že zvládnou identifikovat 40% podvodů při přesnosti 0.1, kdežto

AnoWGAN+e umí identifikovat 80% podvodů, a to dokonce při přesnosti 0.2. Autoři též pro srovnání použili metodu Isolation Forest a docílili hodnoty AUPRC jen 0.1381.

Zároveň metoda AnoWGAN+e zvládá zpracovávat více než 1000 transakcí za sekundu na běžném počítači i přesto, že je implementována v jazyce Python, což by mělo být dostatečně rychlé i pro významné mezinárodní finanční instituce.

Student bohužel neměl čas ověřit spolehlivost jeho metody AnoWGAN+e na jiných datech ani zjistit citlivost metody na volbě hyperparametrů. Pokud metoda prokáže stejně dobré výsledky i těchto testech, pak by ji neměl být problém publikovat nebo prezentovat (např. IEEE Symposium Series on Computational Intelligence, případně i The International Conference on Learning Representations).

Student ve své práci výborně pracuje se předměty obvykle probíranými až na magisterském stupni, které dále rozšiřuje o znalosti z vědeckých publikacích. Student byl po celou dobu velmi samostatný. Zájem o studium zadaného tématu prokazoval pravidelným hledáním relevantních informací ve vědeckých publikacích.

Myslím si, že student jednoznačně překonal nároky kladené na bakalářské práce, proto doporučuji uznat práci za bakalářskou.

Praha, 3. 5. 2019

Jiří Fink
KTIML MFF UK