Міністерство освіти та науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВИЯВЛЕННЯ DENIAL - OF - SERVICE АТАК НА БАЗІ НЕЙРОННОЇ МЕРЕЖІ

Виконав: Блідченко Ю. В.
Науковий керівник к.т.н., доц. каф. КН Арсенюк І. Р.

- Об’єктом дослідження є процес виявлення Denial – of – service атак;
- Предметом дослідження є програмне забезпечення виявлення Denial – of – service атак;
- Метою дипломного проекту є підвищення ефективності виявлення Denial – of – service атак

Для досягнення мети слід розв’язати такі задачі:

- виконати аналіз сучасних аналогів виявлення Denial – of – service атак;
- виконати варіантний аналіз шляхів розв’язання поставленої задачі;
- розробити алгоритм функціонування інтелектуальної системи виявлення атак;
- розробити UML діаграми класів системи;
- розробити програмне забезпечення для системи виявлення Denial – of – service атак та провести його тестування.

АКТУАЛЬНІСТЬ РОЗРОБКИ

- Мережеві та інформаційні технології змінюються дуже швидко тому статичні захисні механізми не можуть надати ефективного захисту .
- З розвитком мережевих технологій розвиваються і мережеві загрози.
- За останні роки саме Denial – of – service вид атаки набув високої популярності.
- Інтернет ресурси надають значну кількість інформації, що повідомляє про інтернет злочини такого типу.

Тому потрібні методи, що дозволять оперативно виявляти порушення безпеки. Адже своєчасне виявлення DoS-атаки дозволить зберегти працездатність мережі.

АКТУАЛЬНІСТЬ РОЗРОБКИ

Створення ефективних систем захисту інформаційних систем стикається також з браком обчислювальної потужності.

З самого початку розвитку комп'ютерів і комп'ютерних мереж спостерігаються дві тенденції, звані законом Мура і законом Гілдера.

Закон Мура каже про щорічне подвоєння продуктивності обчислювачів, доступних за одну і ту ж вартість.

А закон Гілдера - про потроєння пропускної спроможності каналів зв'язку за той же період.

Таким чином, зростання обчислювальної потужності вузлів мережі відстає від зростання обсягів переданої по мережі інформації, що з кожним роком посилює вимоги до обчислювальної складності алгоритмів систем захисту інформації.

ПОНЯТТЯ ТА ВИДИ DoS АТАК

- DoS атака (відмова в обслуговуванні) – це атака на мережу з метою довести її до відмови, тобто створити такі умови, за яких легальні користувачі мережі не зможуть отримати доступ до надаваних ресурсів.
- У дипломному проекті розглянуто декілька типів DoS атак:

- «NUKE»
- «SMURF»
- «LAND»
- «Ping of Death»
- «TEARDROP»

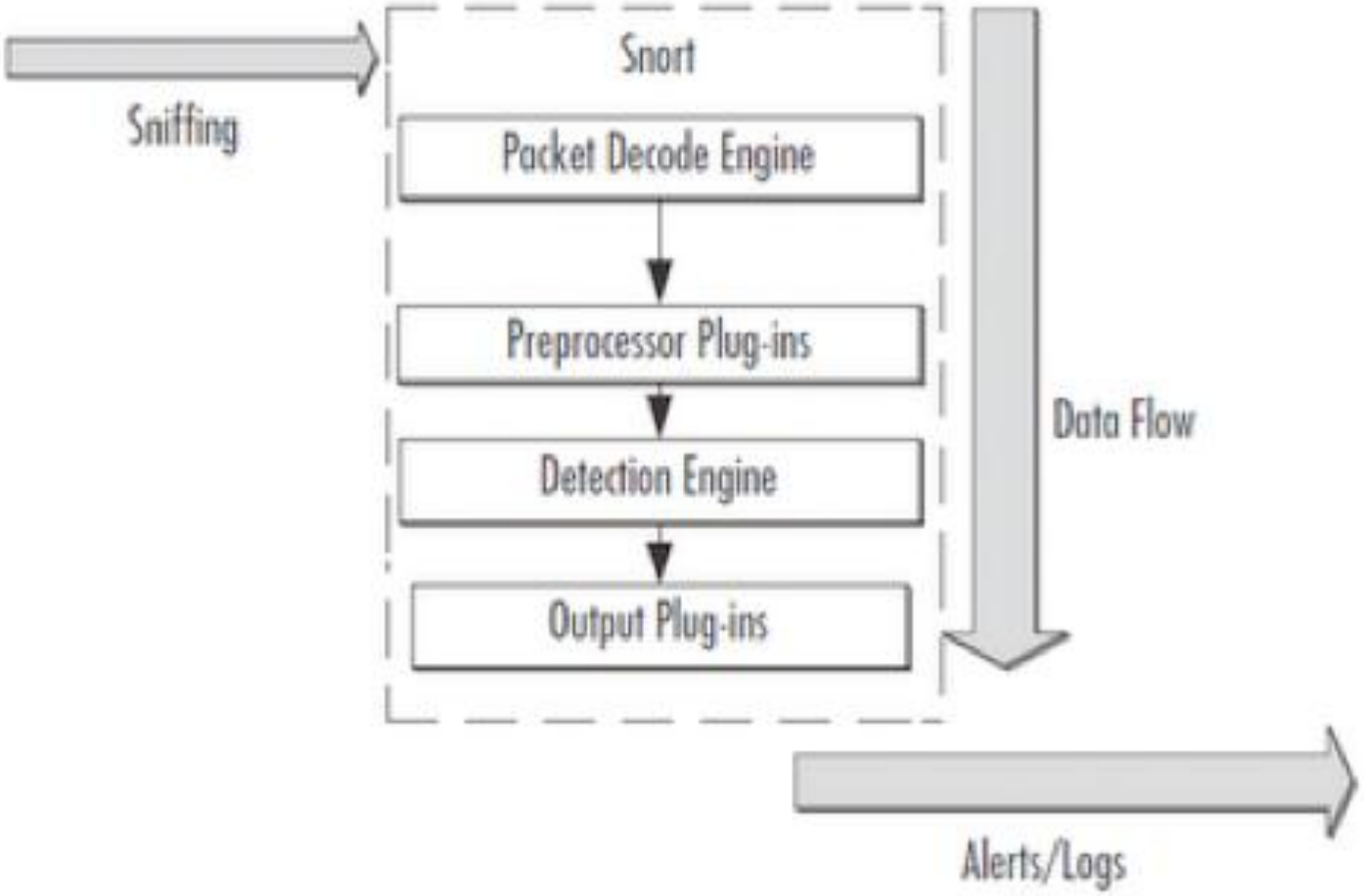
- DoS «NUKE» атака - у разі виникнення помилки з'єднання повертається досить докладна діагностика ситуації. Наприклад: "Мережа недоступна", "Адреса недоступна", "Помилка маршрутизації" та інші. По приході пакету з повідомленням про помилку виробляють певні дії, в першу чергу перебудову таблиці маршрутизації. При цьому, як побічний ефект, розриваються всі встановлені з'єднання з машиною, що має адресу, про який стало відомо, що він недосяжний. На використанні цього ефекту і будуються диверсії.
- DoS «LAND» атака - надсилається SYN-пакет з адресою відправника, що збігається з адресою одержувача, жертви. Пакет надсилається на будь-який відкритий порт. Для WINDOWS систем це майже завжди може бути 139-й порт. Для інших систем це може бути будь-який відомий порт (21-й, 80-й та ін.). Реакцією WINDOWS - комп'ютера на LAND є абсолютне "зависання" .
- DoS «TEARDROP» атака - полягає в надсиланні великої кількості udp-пакетів зі спотвореною адресою відправника на 19-й порт, що призводило до підвищення трафіку.

- DoS «SMURF» атака - одна з найнебезпечніших видів DoS-атак, так як у комп'ютера-жертви після такої атаки відбудеться відмова в обслуговуванні практично з 100% гарантією. Зловмисник використовує широкомовлення для перевірки працюючих вузлів в системі, відправляючи ping-запит. Очевидно, атакуючий поодинці не зможе вивести з ладу комп'ютер-жертву, тому потрібен ще один учасник - це підсилює мережу. У ній по широкомовній адресі зловмисник відправляє підроблений пакет. Потім адреса атакуючого змінюється на адресу жертви. Всі вузли надішлють їй відповідь на ping-запит. Тому пакет, відправлений зловмисником через посилюючу мережу, яка містить 200 вузлів, буде посилений в 200 разів. Тому для такої атаки зазвичай вибирається велика мережа, щоб у комп'ютера-жертви не було жодних шансів.
- DoS «Ping of Death» атака - змушують системи реагувати непередбачуваним чином при отриманні занадто великих IP-пакетів. TCP/IP підтримує максимальний розмір пакета в 65Кб (як мінімум 20 байт інформації в IP-заголовку, деяка кількість додаткової інформації та інша частина пакету, що містить основні дані). Атаки «Ping of Death» можуть викликати аварію, зависання та перезавантаження системи.

Вибір та огрунтування аналогу

- В якості аналогу для розробки було обрано систему виявлення атак під назвою «Snort».
- Система розповсюджується, як вільна програма з відкритим вихідним кодом під ліцензією GPL.
- Вона використовує мову опису правил, який поєднує переваги методів обстеження, заснованих на підписах, протоколах і аномаліях
- Система Snort працює таким чином, що при надходженні пакету, пакет послідовно проходить через декодери, препроцесори і тільки потім вже потрапляє в детектор, який починає застосовувати правила. Це показано на слайді 9.

Послідовність проходження пакетів

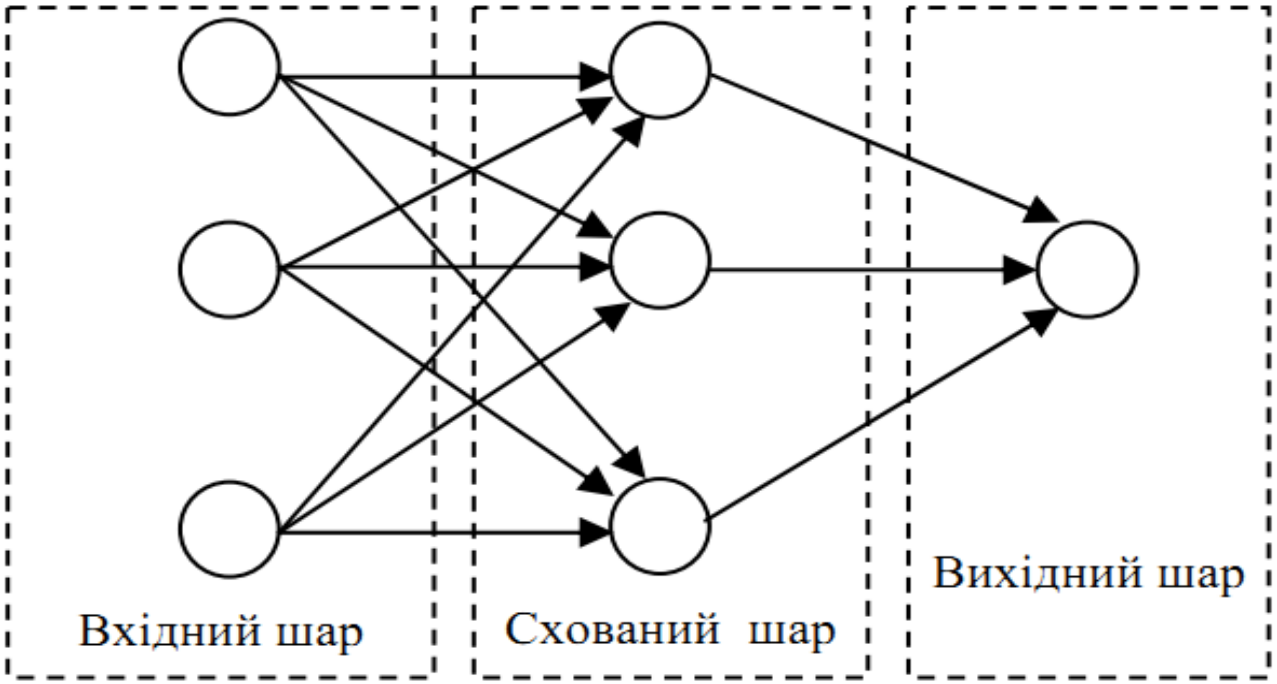


Недоліки аналогу Snort та їх метод вирішення у новій системі

- Основними недоліками даного аналогу є нездатність проводити гнучкий аналіз даних, що виливається в нездатність працювати з великими обсягами даних.
- Також до недоліків можна віднести не змогу захистити мережу від видів поширених DoS атак, таких, як «TEARDROP» та «SMURF»
- У розробці дані проблеми вирішується насамперед застосуванням нового більш детального планування структури майбутньої розробки. Якіснішого контролю трасування, моніторингу та більш сучасних інструментальних засобів, що надходять та контролюються у реальному часі.

Загальна структура нейронної мережі

- Способом вирішення проблем у обраному аналозі є застосування у новій системі нейронної мережі на базі двошарового персептрону.



Математична модель системи

- Двошаровий персептрон може виконувати операцію логічного "І" над півпростору, освіченими гіперплощинами першого шару ваг. Це дозволяє формувати будь-які, можливо необмежені, опуклі області у просторі вхідних сигналів.

$$\frac{N_0 P}{1 + \log_2 P} \leq L_w \leq N_1 \left(\frac{P}{N_1} + 1\right)(N_1 + N_0 + 1) + N_1,$$

$$\frac{P}{10} - N_1 - N_0 \leq L_w \leq \frac{P}{2} - N_1 - N_0,$$

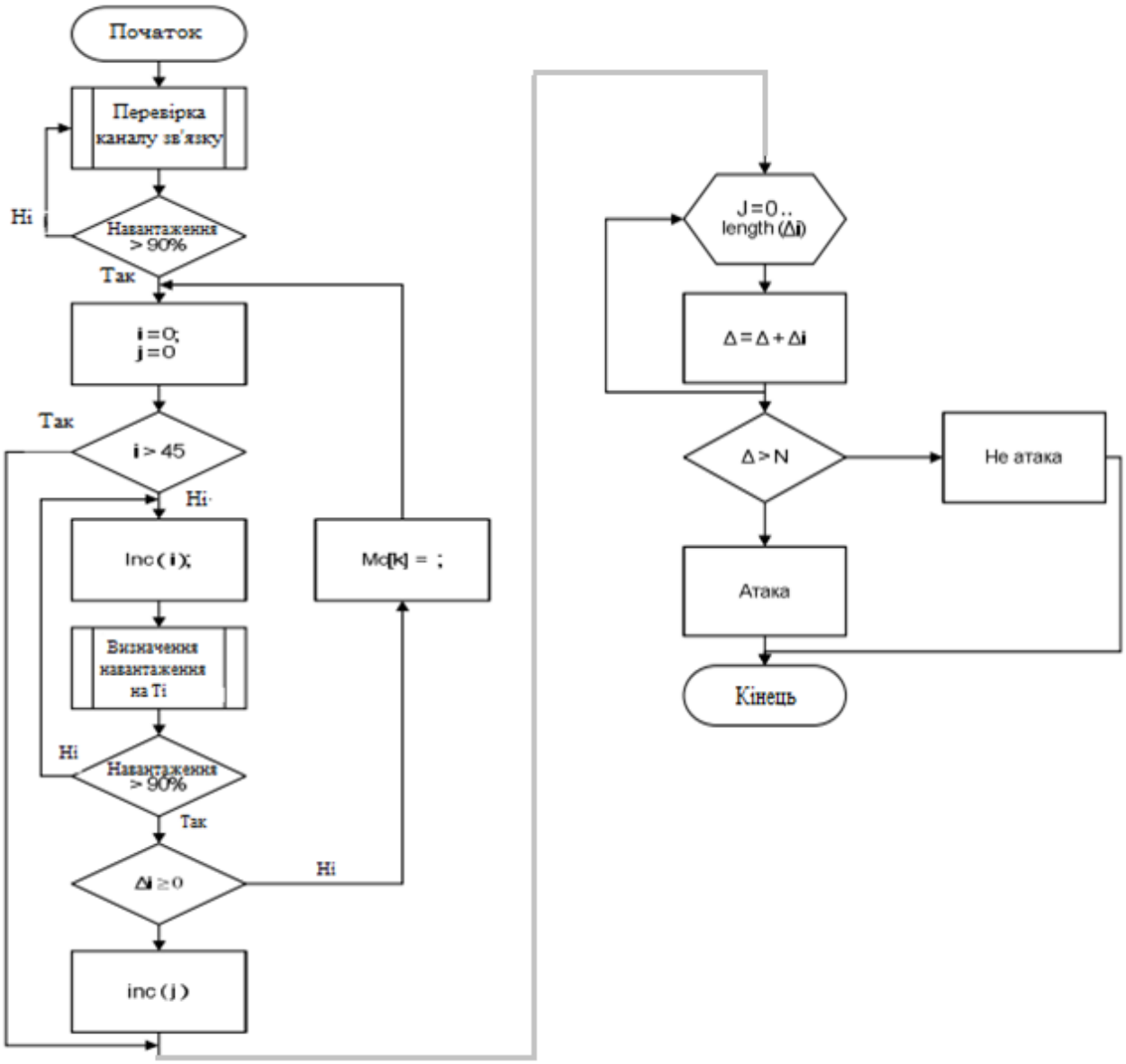
$$L_w < P \times \varepsilon_{max},$$

- Приведені вирази для оцінки оптимальної кількості синаптичних зв'язків та кількості схованих нейронів в двошаровому персептроні

$$D_i = |X - w_i| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + \cdots + (X_c - \omega_{ci})^2},$$

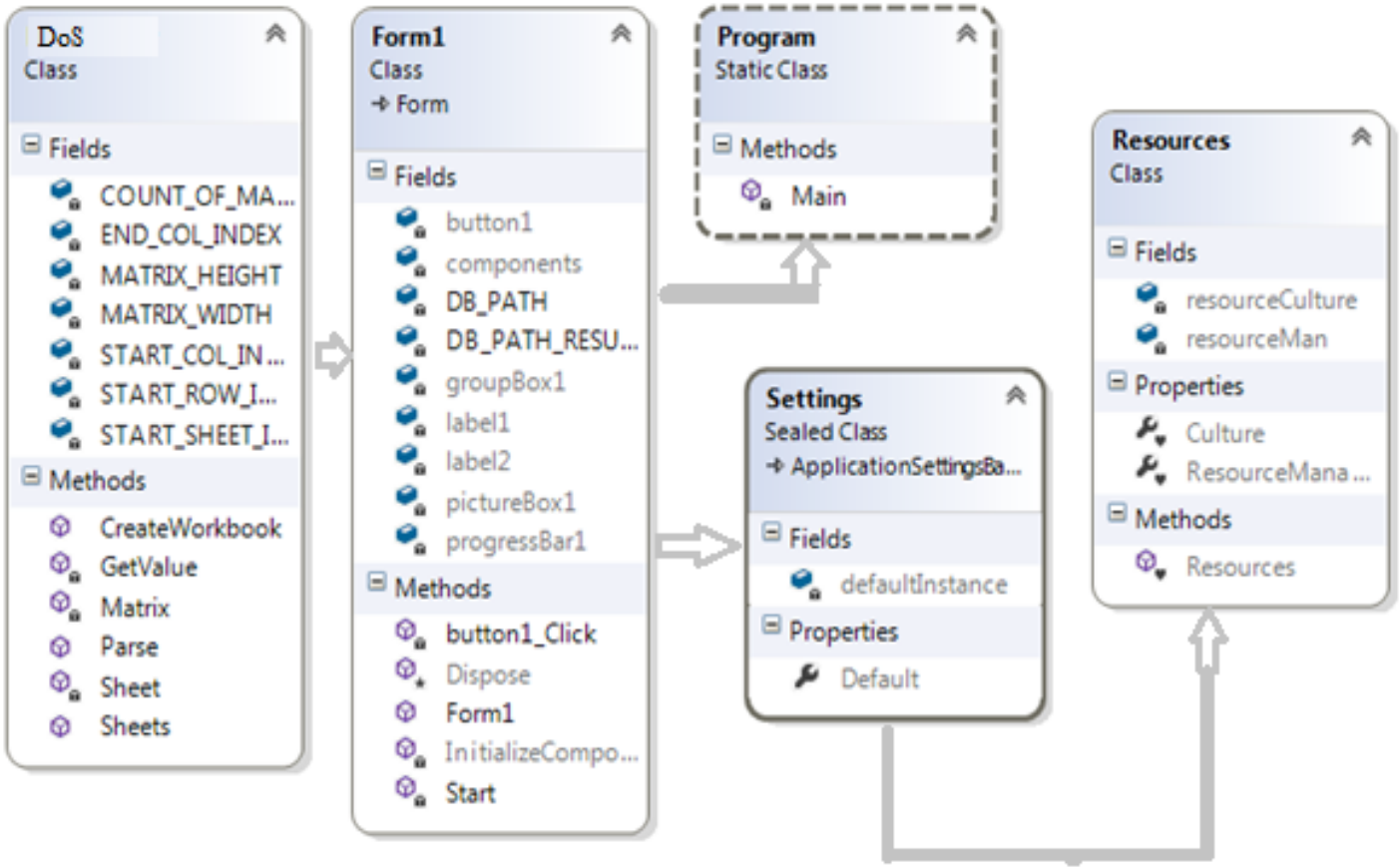
- Визначення відстані між вхідним і ваговим вектором і-го нейронного елемента.

Алгоритм виявлення DoS атак

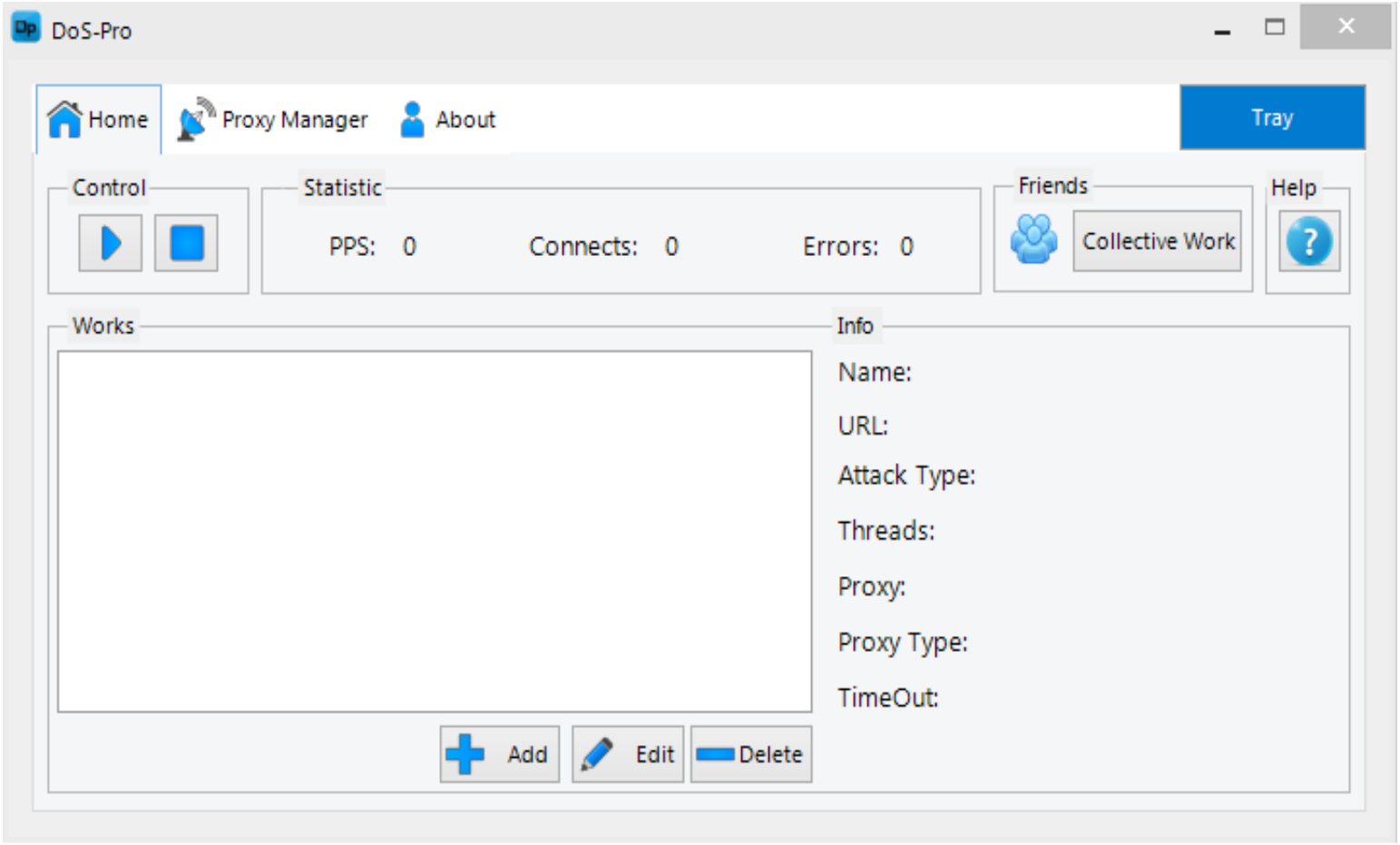


Алгоритм функціонування системи виявлення атак

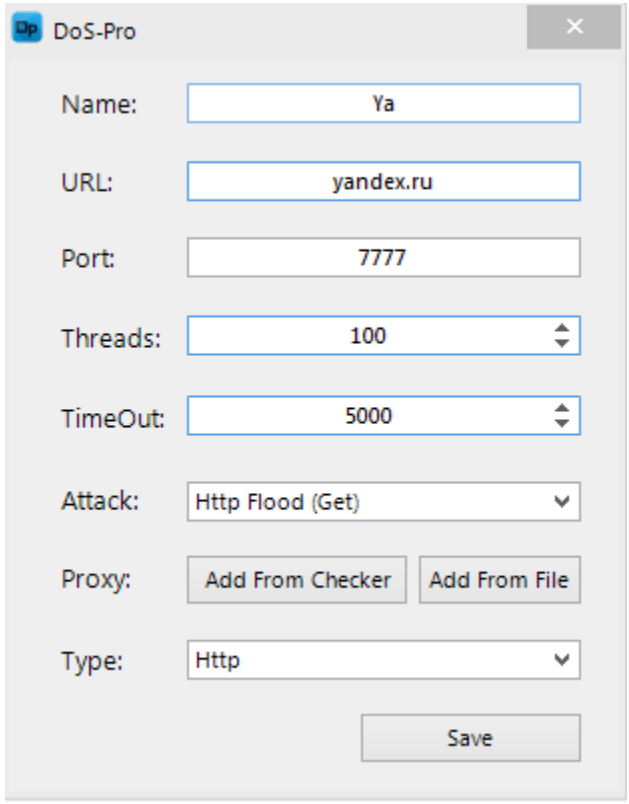
UML діаграма класів системи



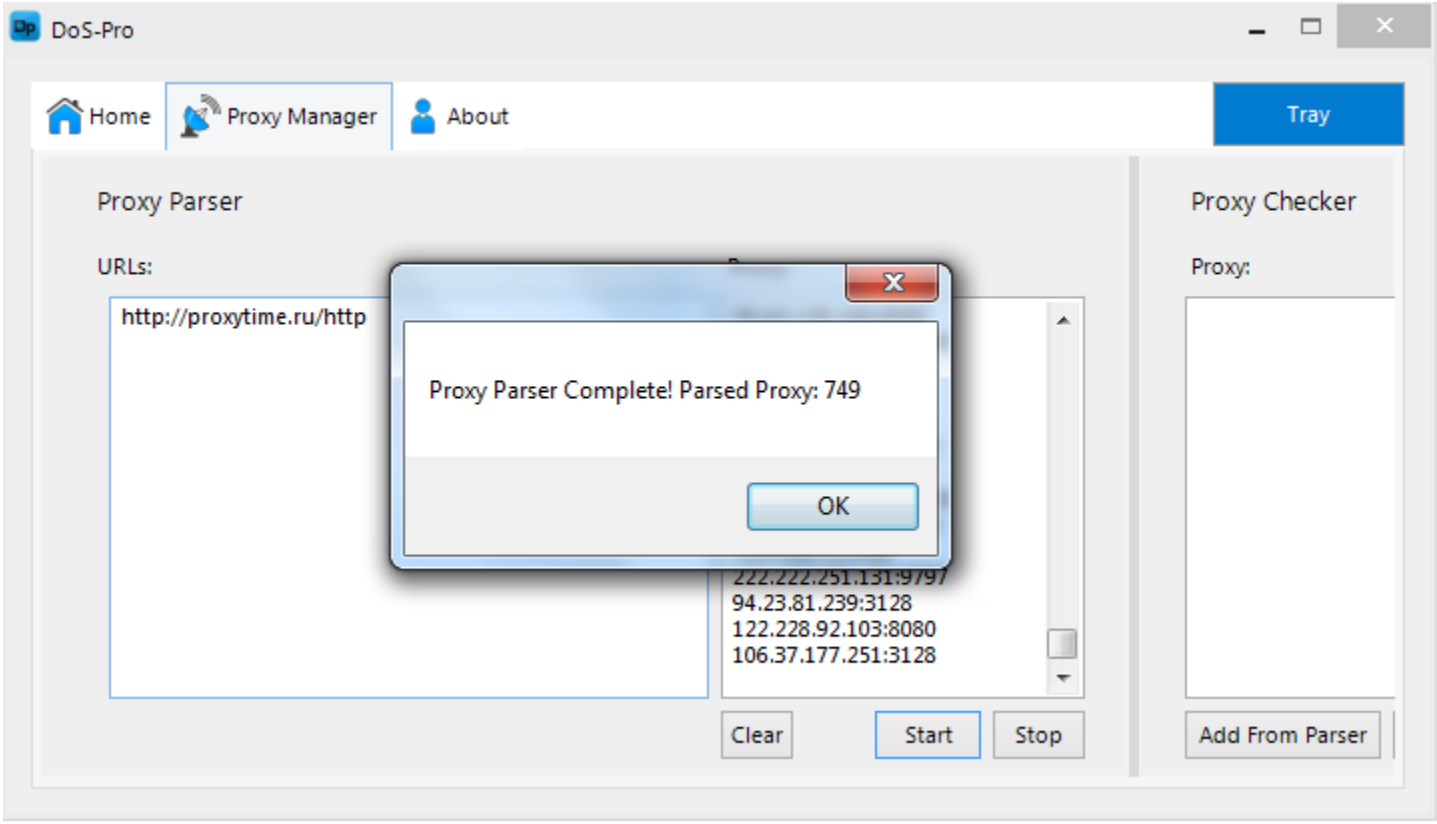
Інтерфейс програми



Головне вікно системи



Додавання нового сервера



Завершення аналізу адрес і виведення кількості атак

Порівняння результатів виявлення атак аналога і власної розробки

Показники	Аналог	Нова розробка
DoS «NUKE» атака	86%	87%
DoS «LAND» атака	74%	76%
DoS «TEARDROP» атака.	91%	90%
DoS «SMURF» атака	75%	75%
DoS «Packet sniffers» атака	97%	97%

Економічне обгрунтування

- Проведені у проекті економічні розрахунки підтверджують економічну доцільність розробки інтелектуальної системи виявлення Denial – of - service атак на базі нейронної мережі, оскільки вона є дешевше ніж аналог на 207,79 грн., термін його окупності складає менше року, а саме 4 місяці.
- Вирахувано, що загальні витрати на розробку нового програмного продукту складають 201131 грн., прогнозований прибуток складає 46564,33 грн.

Висновки

- У дипломному проекті розроблено інтелектуальну систему виявлення Denial – of – service атак на базі нейронної мережі.
- Проведено техніко – економічне обґрунтування доцільності розробки системи, в ході якого проаналізовано суть технічної проблеми, вибрано та обґрунтовано аналоги, визначено технічні вимоги до об’єкту проектування, поставлено задачу дослідження. Виконано прогноз величини попиту, розраховано цінову та конкурентну політику. Розраховано економічну доцільність нового програмного продукту.
- Досліджено предметну область, охарактеризовано та проведено аналіз переваг та недоліків існуючих систем подібного призначення.
- Проведено варіантний аналіз шляхів розв’язання поставленої задачі. Проаналізовано процес виявлення атак.
- Обґрунтовано вибір середовища та об’єктно-орієнтованої мови програмування.

Висновки (продовження)

- Запропоновано математичну модель та алгоритм роботи інтелектуальної системи виявлення DoS атак.
- Розроблено структуру програмного забезпечення виявлення атак та приведено тестовий приклад роботи програми, який показав правильність її роботи.
- Розраховано витрати на розробку, собівартість, ціну реалізації програмного продукту та чистий прибуток для виробника. Також проведено обрахування терміну окупності і експлуатаційних витрат, пов’язаних з обслуговуванням програми.
- Проведене економічне обґрунтування доцільності розробки показало, що новий програмний продукт раціонально впроваджувати в галузі інформаційних технологій, оскільки його реалізація принесе достатні прибутки та витрати будуть покриті впродовж 4 місяців з моменту виходу продукту на ринок.
- Здійснено розрахунок річного економічного ефекту від впровадження нової розробки.
- Отже, можна вважати, що мета дипломного проекту досягнена, це підтверджується проведеними дослідженнями і встановленими результатами.

ДЯКУЮ ЗА УВАГУ