Подход к обнаружению DDOS-атак с

использованием машинного обучения

**1) Какую задачу решали авторы статьи?**

Чтобы распознать и защитить веб-сервер от атаки, важно знать

характер и поведение легитимных и нелегитимных пользователей.

Распределенная атака типа "отказ в обслуживании" (DDoS) может

вызвать массовый отказ систем, т.к по воздействию она похожа на работу в штатном режиме с легитимными клиентами.

Предлагаемый метод пытается обнаружить DDoS-атаку седьмого уровня и DDoS-атаку прикладного уровня на веб-сервер.

**2) Какой алгоритм машинного обучения они использовали для этого?**

В работе использовано несколько алгоритмов и приведено их сравнение:

1. Наивный Байесовский классификатор
2. NaiveBayes Multinomial
3. MultiLayer Perceptron
4. Random Forest
5. RBF Network
6. Logistic

**3) Какие метрики качества были использованы для оценки алгоритма?**

1. Accuracy
2. False positive rate
3. True positive rate

**4) Какие данные были использованы и как они были обработаны?**

В данной работе используются параметры захваченного сетевого пакета, такие как http GET, POST request и delta time.

Предлагаемый авторами метод, на ранней стадии захватывает все пакеты из источника атаки, что позволяет выбирать такие параметры, как

количество http GET или POST запросов с одного IP-адреса.

Также выбирается параметр типа delta time, который может быть определен как интервал времени между любыми двумя последовательными http-запросами, отправленными по одному IP-адресу.

Поскольку DDoS-атака седьмого уровня или прикладного уровня использует протокол http для использования ресурсов веб-сервера, рассматриваются IP-адреса, имеющие максимальное количество http-счетчиков по отношению к одному IP-адресу назначения.

Поскольку обычный пользователь не сможет отправлять http-запросы один за другим с высокой скоростью, авторы рассматривают delta time - время между любыми двумя последовательными запросами. Чем меньше delta time, тем выше вероятность того, что это атака.

Приведенные выше параметры считаются достаточными для определения, имеет ли IP-адрес потенциал для проведения DDoS-атаки. Набор данных, с этими четырьмя параметрами, подается в классификаторы.

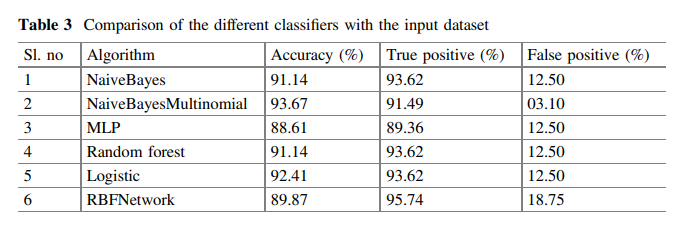
Как пишут авторы, сами данные генерируются вручную.

**5) Как проводилась кросс-валидация и подбор гиперпараметров?**

По псевдокоду в статье можно понять, что кросс-валидацию действительно использовали, но какую именно (реализацию или писали сами - не понятно). Гиперпараметры подбирались grid search методом.

**6) Какие результаты были получены?**

Confusion Matrix



**7) Напишите ваши выводы, замечания и найденные в работе недочеты или слабые места.**

Статья, на мой взгляд, очень интересная. К сожалению, я не являюсь экспертов в области безопасности и для меня этот материал новый. С точки же зрения машинного обучения, замечаний не найдено. Возможно, стоило бы попробовать увеличить кол-во параметров и посмотреть, как это скажется на результатах.