Выводы по результатам моделирования:

1. задержки на передачу сообщения при равном количестве ЭВМ у сети с управляемой структурой всегда меньше чем, у одно-ранговой;
2. при одно-ранговой организации сети время задержек прямо пропорционально количеству кооперируемых ЭВМ;
3. при использовании сети с управляемой структурой для каждого количества кооперируемых ЭВМ можно найти оптимальное число групп по критерию минимума задержек времени на передачу сообщений о рекордных оценках и нахождения в очереди.

Так, для 60 кооперируемых ЭВМ оптимальное число групп колеблется в интервале от 8 до 12, для 90 ЭВМ – 11-12, 180 ЭВМ– 22-25, 240 ЭВМ –28-35.

Литература:

1. Ревотюк М.П. Кооперативные схемы алгоритмов решения задач выбора на распределенных вычислительных системах. - Мн.: МРТИ, 1990. – 16 с.
2. Романовский И.В. Алгоритмы решения экстремальных задач. - М.: Наука, 1977. - 352 с.

ПРИМЕНЕНИЕ АЛГОРИТМОВ РАСПОЗНАВАНИЯ ОБРАЗОВ В СРЕДСТВАХ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Бахтизин В. В, Крапивин В. А.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, 220600, ул. Платонова, 39, кафедра ПОИТ

Аннотация. Предложенный алгоритм позволяет просто и надежно определять пользователя по его биометрическим характеристикам. Достоинствами предложенного алгоритма являются простота использования, надежность и невысокая стоимость по сравнению с традиционными средствами. Данный метод базируется на аппарате распознавания и классификации образов.

Ключевые слова. Защита от НСД, аутентификация, клавиатурный почерк.

В связи с распространением корпоративных сетей все острее встает проблема однозначной идентификации пользователя при входе в сеть. В связи с необходимостью работ одновременно с несколькими серверами, пользователь вынужден либо запоминать множество имен и паролей для получения доступа к каждому из нужных ему серверов, или применять дорогостоящие карточки.

Для решения этой проблемы используется метод автоматического выполнения запроса к серверу на получение доступа. При этом пользователь при первом доступе к серверу вводит пароль, а система на его рабочем месте запоминает его и при последующих сеансах работы подставляет этот пароль автоматически. Данный подход имеет ряд недостатков:

- пользователям необходимо наличие знаний об именах и паролях;
- для получения доступа к серверу достаточно провести атаку рабочего места пользователя, например при помощи программ «троянский конь».

В связи с вышеизложенным предлагается следующий подход к защите от несанкционированного доступа. Пользователю или группе пользователей присваивается один пароль. Отпадает необходимость в запоминании какой-либо парольной информации конфиденциального характера, так как распознавание пользователя осуществляется не паролем, а с помощью математических методов.

Предлагаемый алгоритм защиты от несанкционированного доступа базируется на методах распознавания и классификации образов. При этом сам процесс определения пользователя использует его биометрические характеристики, а именно его клавиатурный почерк.

Собственно съем данных пользователя представляет собой следующую процедуру. Пользователь вводит требуемую фразу (то есть пароль), а программа фиксирует интервалы между нажатиями на соответствующие клавиши.

Рассмотрим некоторые методы распознавания образов, положенные в основу предложенного метода аутентификации. Более подробную информацию можно получить в [1, 2].

Пусть A - множество значений эталонов. При этом $A=\{x_i\}, i=\overline{1,N}$, N - объем выборки множества A. Множество определено на метрическом линейном пространстве размерности k=s-1, где s - длина пароля в символах.

При этом выполняется условие $A=\bigcup_{j=1}^{M} A_j,\ j=\overline{1,M}$, где M - число пользователей в системе, и условие $A_i \bigcap A_j = 0, \forall j,i=\overline{1,M}, j \neq i$. Данные пользователя, которые были с него сняты, это $x_i \in R_1^k$. В метрическом линейном пространстве задана метрика $d: R^k \times R^k \to R^1$. При этом возможно применение как lp-метрики, так и менее известных метрик [1, 2]. Задача состоит в том, чтобы определить такой класс A_j, что $x \in A_j$.

В разработанном пакете программ используется несколько простых алгоритмов распознавания, в том числе метод k ближайших соседей и метод единственного эталона [1,2].

Пусть $F=\{f_s\}, s=\overline{1,S}$ - множество применяемых методов распознавания, где S - общее число методов. После того, как каждый метод выберет своего кандидата, проводится оценка полученных результатов. В данной системе используется метод коррекции распознавания по большинству [1,2].

Сформируем вектор $a=(a_1, a_2, \ldots, a_M)$ так, что

$$a_i=\sum_{s=1}^{S}\mu_s\{f_s(x)\in A_i\}, \forall i=\overline{1,M}, \quad (1),$$

где μ_s - вес соответствующего метода (обычно μ_s=1). Далее находим $a_i=\max_{i=\overline{1,M}} a_i$. Следовательно, $x\in A_i$. При этом, если

$$a_i<T\times\sum_{i=\overline{1,i\neq l}}^{M} a_i \quad (2),$$

где T - порог прохождения кандидата в пользователи, то определение пользователя по введенным биоданным неоднозначно. Параметр $T\in[0;1]$ задается вручную и показывает степень «строгости» проверки.

В процессе съема биоданных пользователь постепенно обучается, поэтому его параметры постепенно улучшаются. В таком случае возможна ситуация, когда пользователь не получит доступ в сеть, потому что он набрал пароль слишком хорошо. Чтобы этого не случилось, проводится следующая процедура. При каждом успешном входе в сеть осуществляется попытка автоматического занесения снятых биометрических данных в эталонную выборку, а самый первый элемент множества эталонов, характеризующих этого пользователя, удаляется из выборки.

Полученные от пользователей биометрические данные до применения процедуры распознавания предварительно фильтруются. Применение фильтров позволяет нивелировать разницу набора текста одним человеком и тем самым улучшить распознавание пользователей на коротких паролях (5-8 символов). В разработанном пакете программ используются как преобразование Фурье, так и эвристические алгоритмы.

Были проведены следующие эксперименты. Несколько человек с приблизительно равной скоростью набора русского текста ввели по 10-15 раз одну и ту же фразу из нескольких слов (до 30 символов) на русском языке без знаков пре-

пинания и пробелов. Общее число эталонов составило 83 элемента. Были получены следующие результаты, которые приведены в таблице 1, где используются следующие обозначения:

EE-4 – метод единственного эталона, работавший на lp-метрике lp=4.

EE-2 – метод единственного эталона, работавший на lp-метрике lp=2.

ДПФ – дискретное преобразование Фурье.

ЭАФ - эвристический алгоритм фильтрации.

Таблица 1

Длина пароля	Вероятность распознавания		
	Лучший метод	Лучший фильтр	Итого
31	EE-4, 91%	ДПФ, 91%	92%
30	EE-4, 95%	ДПФ,91%	92%
25	EE-4, 91%	ДПФ,91%	91%
20	EE-2, 93%	ДПФ,91%	95%
15	EE-4, EE-2, 90%	ЭАФ,86%	91%
10	EE-4, 90%	ЭАФ, 89%	92%
9	EE-4,94%	ЭАФ, 95%	95%
8	EE-2,92%	ЭАФ,90%	91%
6	EE-4,94%	ЭАФ,89%	91%
5	EE-2,91%	ЭАФ,91%	91%

Подробные результаты в таблице 1 не приводятся из-за ограниченного объема данной статьи. В таблице 1 приведены только наилучшие результаты по трем категориям – лучший метод, лучший фильтр и общий результат.

Из анализа результатов следует, что для длинных паролей лучшим фильтром является ДПФ, а на коротких паролях лучше себя проявляют эвристические алгоритмы. Наблюдаемая нелинейность качества распознавания обусловлена тем, что наиболее точно индивидуальные особенности пользователя проявляются в переходах с одного слова фразы на другое, в то время как набор в пределах одного слова определяется опытом набора текста.

Таким образом, применение алгоритмов распознавания образов к системам аутентификации позволяет с высокой точностью аутентифицировать пользователей по их клавиатурному почерку. Качество распознавания одного пользователя достигает 95% даже для небольших паролей, поэтому разработанный алгоритм может быть применен как для контроля традиционной процедуры аутентификации, так и для замены парольных систем:

Литература
1. Фор А., Корман А., Деинни-Папен М., Современная математика, М., Мир, 1986.
2. Фор А., Восприятие и распознавание образов, М., Машиностроение, 1989.

САМООБУЧАЮЩАЯСЯ НЕЙРОННАЯ СИСТЕМА ДЛЯ АВТОНОМНОГО УПРАВЛЕНИЯ МОБИЛЬНЫМ РОБОТОМ

Игнатюк О.Н.
Электронно-механический факультет,
Брестский политехнический институт, Московская 267,
224017 Брест, Республика Беларусь
cm@brpi.belpak.brest.by

Ключевые слова: нейронные сети, самообучение, мобильный робот

Введение

Самообучение характеризуется способностью системы обучаться при взаимодействии с внешней средой. В результате самообучения происходит самоорганизация системы с целью адаптации к внешней среде. Самообучение позволяет освободить оператора от процесса обучения и является важным фактором для эволюции системы. Так, при функционировании робота в разных условиях точность информации от сенсорных устройств может быть различной. В результате возникает необходимость корректировать знания, заложенные в систему, с целью адаптации к внешней среде. Особенно актуальным это является при функционировании робота в агрессивных средах или на других планетах, где невозможно предусмотреть все аспекты ситуационного взаимодействия робота с окружающей обстановкой. Рассмотрим основные принципы реализации концепции самообучения для мобильных роботов.

Общая архитектура системы

Общий подход к построению самообучающейся системы состоит в том, что начальные знания робота могут пополняться и корректироваться в процессе функционирования. При этом здесь предполагается, что базовые знания робота содержатся в блоках 1–3 и 6 (рис. 1), которые определяются логическим путем, как было показано в предыдущих разделах. Тогда задача состоит в том, чтобы в процессе функционирования робота обучить многослойный персептрон (блок 4) для обеспечения робастного управления на узких интервалах движения. Схема