Проект 1994Р: Формальные методы защиты информации в компьютерных сетях

1 Название проекта/ Номер годового отчета

Задача 2: Разработка математических основ, архитектуры и принципов реализации компонент многоагентной системы обучения обнаружению атак на компьютерные сети.
Отчет №1

2. Головной институт

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

3. Институты-участники

Нет

4. Руководитель , номер телефона, факса, адрес электронной почты

Городецкий Владимир Иванович, (812)-323-3570, (812)-328-0685, gor@mail.iias.spb.su

5. Дата начала осуществления, продолжительность проекта

1 декабря 2000, 36 месяцев

6. Краткое описание плана работ: цель, предполагаемые результаты, научно-технический подход

Краткий план работ

В-1. Разработка онтологии задач обучения, распределение задач обучения между типовыми агентами обучения .	1-3 кварталы
Промежуточный отчет # 1, представляющий результаты исследований по задаче В-1 .	3 квартал
В-2. Разработка архитектуры многоагентной обучающей системы и математических методов, реализующих функциональности типовых обучающих агентов.	4-6 кварталы
Представление статьи в международный журнал.	5 квартал
Промежуточный отчет # 2, представляющий результаты исследований по задаче В-2.	6 квартал
В-3. Разработка протокола взаимодействия интеллектуальных обучающих агентов (протокола переговоров) для обобщения решений отдельных агентов в соответствии с процедурой мета-классификации и разработка архитектуры многоагентной обучающей системы в целом.	7-8 кварталы
В-4. Разработка объектно-ориентированного проекта многоагентной системы обучения обнаружению атак.	6-8 кварталы
В-5. Разработка программного прототипа многоагентной системы обучения обнаружению атак, реализующей основные теоретические решения.	9-11 кварталы
Промежуточный отчет #3, описывающий результаты решения задачи В-4 и частично разработанные программные компоненты многоагентной системы обучения обнаружению атак.	10 квартал
В-6. Оценка свойств, достоинств и недостатков разработанной архитектуры и математических методов, реализованных в компонентах прототипа многоагентной системы обучения обнаружению вторжений в компьютерную сеть.	12 квартал
Итоговый отчет, описывающий результаты моделирования многоагентной системы обучения обнаружению вторжений и итоговое заключение по задаче 2 в целом.	12 квартал

Примечание: Строки таблицы, залитые серым цветом, отвечают исследованиям, запланированным на первый год работы. Задача В.2 в этот период должна быть решена только частично.

Цель проекта

Целями исследований по задаче 2 проекта являются разработка математических основ, многоагентной архитектуры и принципов реализации системы обучения обнаружению атак, функционирующей параллельно с системой защиты компьютерной сети.

Ожидаемые результаты

1. Онтология задач обучения обнаружению вторжений;
2. Распределение задач обучения между типовыми агентами обучения и архитектура их взаимодействия в рамках многоагентной системы обучения;
3. Математические методы и алгоритмы реализации функций типовых агентов обучения различных классов, а также других компонент многоагентной системы обучения, обеспечивающих взаимодействие агентов. Программная реализация компонент многоагентной системы обучения с использованием современных стандартных сред программирования *Visual C++, JAVA 2, SQL Server, XML* и др.
4. Результаты исследований программных компонент многоагентной системы обучения обнаружению атак на компьютерные сети с оценкой преимуществ и недостатков разработанной архитектуры, а также математических методов, реализованных в компонентах программной системы.

Научно-технический подход

Ключевым аспектом этой задачи является выбор адекватных методов обучения среди существующих, и разработка специализированных методов и алгоритмов, которые могли бы обеспечить обучение на основе прецедентов. Прецеденты, специфицирующие вторжения, являются, как правило, упорядоченными последовательностями данных регистрации различной длины, задаваемыми в терминах, возможно, повторяющихся символов. Эти символы соответствуют предобработанным сообщениям входного трафика, поступающего на порт хостов компьютерной сети. В случае распределенной атаки, так же как и в случае нормальных распределенных действий пользователей, ситуацию на сети задает множество таких последовательностей. По этой причине задача обнаружения знаний в данных для обнаружения вторжений является более сложной и менее изученной по сравнению с традиционными задачами обучения.

Методы обучения включают в себя три класса методов. Первый класс методов строится на основе модели атаки а терминах формального контекстно-свободного языка. В этом случае задача обучения может быть сведена к задаче восстановления грамматики на основе прецедентов. Второй класс методов базируется на статистических свойствах прецедентов, определяющих нормальные и аномальные действия пользователей, осуществляющих доступ к ресурсам сети. Третий класс методов ориентирован на решение задач извлечения правил из прецедентов, определенных в терминах высокоуровневых понятий, например, паттернов.

В основу архитектурных решений положена технология многоагентных систем. Обоснование и разработка конкретной архитектуры будет выполняться на основе декомпозиции общей задачи обучения на множество подзадач в соответствии с онтологией атак, и распределением этих подзадач среди типовых программных агентов обучения, каждый из которых будет использоваться для клонирования ряда специализированных агентов. Каждый специализированный агент при этом настроен на обнаружение частного класса зависимостей (паттернов, логических правила, определенных над паттернами и др.) из данных фиксированного формата (последовательности событий, множества паттернов, подмножества правил и др.).

В математическом описании процедур взаимодействия агентов обучения обнаружению атак, в особенности, распределенных атак, будет использоваться идея мета-классификации, реализуемой на основе многоуровневого обучения, которая предлагает перспективный подход к объединению знаний, полученных из различных источников.

7. Ход выполнения технических работ за первый год (для годовых отчетов за второй год)

8. Ход выполнения технических работ за рассматриваемый год

Ход выполнения работ полностью соответствует плану работ как по содержанию, так и по срокам завершения предусмотренных этапов работ.

Основные достижения за прошлый год

Основные достижения за прошлый год связаны с решением запланированных задач. Эти задачи и полученные по ним результаты перечисляются ниже.

На первый год исследований была запланирована задача В-1 "Разработка онтологии задач обучения, распределение задач обучения между типовыми агентами обучения. Она включает в себя решение следующих частных подзадач:

1. Анализ структуры данных регистрации.
2. Разработка многоуровневой онтологии задач обучения.
3. Разработка концептуальных моделей типовых агентов многоагентной обучающей системы.

Кроме того, план работ предполагает также проведение частичных исследований по задаче В-2 "Разработка архитектуры многоагентной обучающей системы и математических методов, реализующих функциональности типовых обучающих агентов", полное решение которой запланировано к концу 6 квартала. Поскольку результаты по последней задачи носят предварительный характер и выполнены не в полном объеме, они далее не рассматриваются.
Основные результаты, полученные в рамках вышеназванных задач в течение первого года исследований, таковы.

1.Анализ структуры и особенностей данных, используемых для обучения

Как правило, информация, получаемая из одного источника, не содержит достаточно свидетельств, позволяющих уверенно и своевременно обнаруживать атаки и факты нарушения политики безопасности. Для построения эффективной системы обнаружения вторжений и обучающей системы необходимо использовать взаимосвязанный комплекс данных регистрации, полученных от разнообразных источников и представляющих данные на различных уровнях обобщения (на сетевом уровне, уровне операционной системы, на уровне приложений и на уровне дополнительных источников). Обращение к нескольким источникам информации может значительно повысить достоверность решений, связанных с обнаружением атак и защитой компьютерной сети.

Концептуальный анализ любой проблемы обучения включает, прежде всего, анализ источников знаний. В рассматриваемой задаче главными источниками данных являются экспериментальные данные, описывающие деятельности пользователей и "историю" вторжений, которые совместно описывают данные регистрации, соответствующие случаям, интерпретируемым как "нормальная деятельность", "подозрительная деятельность" и "атака". Поскольку в проекте система обнаружения вторжений рассматривается как мультисенсорная система объединения знаний, полученных из различных источников, то соответствующая задача обучения является задачей распределенного обнаружения знаний, которая реализуется на основе многоагентной архитектуры.

Известные алгоритмы обучения обнаружению атак являются вычислительно сложными. Существенного снижения сложности можно достигнуть за счет предварительного анализа информативности данных и выявления потенциально наиболее представительных атрибутов и признаков деятельности субъектов (внутренних и внешних по отношению к защищаемой системе), которые проявляются в данных регистрации. В качестве таких признаков целесообразно выделять повторы определенных событий и их комбинации, неправильные команды и команды, неадекватные текущей ситуации, признаки, свидетельствующие об использовании известных уязвимостей, о неадекватности параметров и содержания сетевого трафика, заметные отклонения значений атрибутов, характеризующие профиль работы субъектов системы (например, время и дата работы, адрес субъекта, используемые субъектами сервисы, характеристики системных ресурсов, в том числе, данные о загрузке центрального процессора, обращении к оперативной и дисковой памяти, к файлам, телекоммуникационным портам и т. д.) и необъяснимые проблемы (например, выход из строя маршрутизатора, перезагрузка сервера, невозможность запуска системного сервиса и др.). Вовлечение экспертов на данном этапе обучения может существенно сократить перебор паттернов и размерность данных, используемых для обучения.

Основные особенности и трудности рассматриваемой задачи обучения обусловлены распределенным характером и наличием зависимостей временного характера. Такие данные в проекте представляются в терминах обобщенной модели временных последовательностей событий, которая определяет структуру паттернов подлежащих обнаружению в процессе обучения.

2. Разработка многоуровневой онтологии задач обучения.

Непротиворечивая и согласованная работа крупномасштабной распределенной системы, основанной на знаниях, может быть обеспечена только в том случае, если распределенные сущности, составляющие систему, в состоянии понимать друг друга. В соответствии с современными представлениями, такая работа может быть организована наилучшим образом, только с помощью подхода, базирующегося на использовании онтологий. Именно онтология в состоянии обеспечить совместную непротиворечивость локальных баз знаний, целостность знаний и однозначную и корректную интерпретацию терминов, составляющих язык обмена сообщениями между сущностями распределенной системы.

Многоуровневая онтология задачи обучения обнаружению вторжений объединяет в единую взаимосвязанную систему комплекс базовых понятий, формирующих верхние уровни модели знаний, с которыми манипулируют компоненты разрабатываемой системы. Эта онтология охватывает понятия из *проблемной* онтологии "Data fusion" & "Data fusion learning", а также из онтологии *предметной* области "Intrusion detection". Разработанная онтология служит базисом для построения верхнего уровня представления распределенных знаний, которые являются общими ("*shared knowledge*") для компонент системы обучения обнаружению вторжений. Этот уровень знаний позволяет, к одной стороны, обеспечить целостность распределенной базы знаний, а с другой стороны, "взаимопонимание агентов" при обмене сообщениями.

3. Разработка концептуальных моделей типовых агентов многоагентной обучающей системы

Обучаемая система обнаружению вторжений, рассматривается как мультисенсорная система объединения данных, полученных из различных источников. Эта система формирует решения на основе многоуровневой модели обработки входных данных (входного трафика сети и данных аудита). Применительно к такому взгляду на обучаемую систему разработана концептуальная модель многоагентной системы обучения.

В процессе исследований проанализированы структуры данных обучения и выбрано множество адекватных методов (алгоритмов) обучения, которые позволяют справиться с рассматриваемой задачей обучения. Это множество включает в себя как некоторые из известных методов (например, некоторые из множества *ID3*, *C4.5*, *AQ*, *CN2*, *бустинг*, а также методологию мета-классификации), так и методы, которые разработаны или разрабатываются исполнителями данного проекта (например, метод визуального аналитического обнаружения закономерностей – –*VAM*-метод, классификации, алгоритм *GK2*, алгебраические байесовские сети).

Определен состав типовых классов (классов агентов) многоагентной системы обучения обнаружению вторжений, а также их функциональности и роли в системе обучения. Множество классов агентов включает в себя

- Класс агентов управления данными обучения;
- Класс агентов тестирования классификаторов;
- Класс агентов формирования мета-данных и
- Классы обучающих агентов, а именно, (а) класс *агентов,* предназначенных для обучения классификаторов атак, входные данные которых представлены последовательностями событий, упорядоченных во времени и (б) класс *агентов,* предназначенных для обучения классификаторов, которые работают с описанием атак в форме вектора признаков.

9. Существующее положение дел с выполнением технических работ

Ход выполнения работ полностью соответствует предусмотренному плану и в коррекции не нуждается.

10. Сотрудничество с зарубежными партнерами

В соответствии с планом работ партнеру представлены два промежуточных отчета (1 июня 2001 и 1 декабря 2001), в которых полностью представлены соответствующие результаты исследований.

Исполнители проекта совместно с представителем партнера участвовали в Европейской школе по многоагентным системам. В марте 2001 была организована командировка руководителя проекта в организацию партнера для обсуждения предстоящих исследований. Представитель партнера посещал Институт в мае 2001 г. Планируется большой семинар по обсуждению результатов исследований за первый год в феврале 2002 в организации партнера в США.

11. Выявленные проблемы и предложения относительно их устранения

Нет

12. Перспективы дальнейшего развития разработанной технологии/научного исследования

Будут обсуждаться на встрече с партнеров в марте 2002 г.

Приложение 1. Наглядные материалы, прилагаемые к основному тексту

Нет

Приложение 2. Другая дополнительная информация к основному тексту

Краткое содержание Промежуточных отчетов, представленных партнеру

Промежуточный отчет №1

Приложение 3. Резюме статей и докладов, опубликованных за рассматриваемый год

Список публикаций

1. В.И. Городецкий, О.В. Карсаев, И.В.Котенко, А.В. Хабалов, Л.Попьяк, В.Скормин. Многоагентная содель защиты компьютерной сети: Демонстрационный пример. *Proceedings of the International Workshop "Mathematical Methods, Models and Architectures for Computer Network Security. Lecture Notes in Computer Science*, vol. 2052, Springer Verlag, 2001, pp.39-50.

Абстракт. В статье рассматривается многоагентная модель системы защиты компьютерной сети, которая состоит из набора автономных интеллектуальных агентов, распределенных по хостам защищаемой компьютерной сети и кооперирующихся с целью принятия совместных непротиворечивых решений. В статье делается акцент на архитектуре, программной реализации и компьютерном моделировании демонстрационного примера, построенного с целью изучения возможностей мнеогоагентных систем защиты сетей. В статье описывается концептуальная модель и архитектура отдельных специализированных агентов и системы в целом, а также технология ее программной реализации. Описывается также сценарий моделирования, модель входного трафика, а также особенности работы распределенной системы. Основное внимание уделено взаимодействию агентов в процессе распределенного обнаружения вторжений. Обсуждаются перспективы использования такой модели защиты компьютерных сетей.

2. В.И. Городецкий, О.В. Карсаев, И.В.Котенко, А.В. Хабалов. MAS DK: инструментарий для разработки многоагентных систем и примеры приложений. В трудах международной конференции "Искусственный интеллект в XXI веке" (*ICAI' 2001*), Изд. Физико-математической литературы, Москва, стр. 249-262, 2001.

Абстракт. В статье рассматривается предлагаемая авторами технология и реализующий эту технологию инструментарий разработки многоагентных систем MASDK. Данный инструментарий базируется на использовании набора инвариантных компонентов, объединенных в виде “Типового агента”. Процесс разработки многоагентной системы рассматривается как развитие “Типового агента” в классы специфических агентов приложения. Формирование классов агентов приложения предполагает определение сценариев их поведения и схемы взаимодействия. Совокупность последних формируется и хранится в “Системном ядре” – специализированной базе данных ИР МАС. Статья также содержит краткое описание трех разрабатываемых с помощью ИР МАС прототипов прикладных систем: (1) планирования операций и составления расписаний, (2) извлечения закономерностей из экспериментальных данных, (3) обнаружения вторжений в компьютерные сети.

3. Городецкий В.И., Карсаев О.В., Котенко И.В., Хабалов А.В. Инструментарий для разработки многоагентных систем. International Workshop of Central and Eastern Europe on Multi-agent Systems *(CEEMAS-2001),* Krakow, Poland, September 2001 (Будет опубликована также в серии "*Lecture Notes In Artificial Intelligence*" в 2002).

Абстракт. В статье представляется разработанная технология и инструментальное программное средство для проектирования и разработки многоагентных систем, основанных на знаниях. Программный инструментарий включает две компоненты: "Типовой агент" и "Набор инструментов для разработки многоагентных систем". Первая компонента представляет собой набор классов Visual C++ и Java, которые инвариантны по отношению к приложениям и допускают поэтому повторное использование. Вторая компонента состоит из нескольких специализированных редакторов, снабженных понятным пользовательским интерфейсом, которые используются для формального описания типовых классов агентов и типовых структур данных, формирующих конкретное приложение из типового агента. Это формальное описание затем инсталлируется на конкретную компьютерную сеть. Разработанная технология и набор инструментов для разработки и программной реализации многоагентных систем использованы для создания ряда приложений из области защиты компьютерных сетей, планирования операций и извлечения знаний из данных.

4. Городецкий В.И., Самойлов В.В. Визуальный синтез классифицирующих предикатов и их использование в процедурах мета-классификации. Известия ТРТУ, №4, 2001, стр. 5-15.

Абстракт. Рассматривается задача извлечения знаний из распределенных баз данных, когда в базе данных имеются атрибуты, измеренные в числовой шкале и при этом размерность баз данных достаточно велика. Ключевыми компонентами предложенного подхода являются две процедуры: (1) процедура визуальной разработки классифицирующих предикатов, которые принадлежат классу произвольных формул, заданных над множеством предикатов с линейными арифметическими термами. Эта процедура дает возможность строить разделяющие границы достаточно общего вида, включая нелинейные и невыпуклые, а также дает возможность формировать многосвязные области локализации кластеров данных; (2) процедура построения мета-классификатора, который обрабатывает решения, даваемые различными классификаторами, сгенерированными на основе первой процедуры. Использование мета-классификации дает возможность строить точные и эффективные классификаторы, обладающие свойствами масштабируемости, расширяемости и адаптивности.

Менеджер задачи 2 проекта
профессор
В.И.Городецкий