Обнаружение несанкционированного вторжения в беспроводные одноранговые сети

Ву Бао Тао[1], Нгуен Тхи Тху[1], Хоанг Тхи Нгок Зьеп[1], Р.С. Зарипова[2]

[1]Университет Шао-До, Чи Линь, Вьетнам
[2]Казанский государственный энергетический университет, Казань

Аннотация: В статье представлен анализ способов обнаружения вторжений и даны рекомендации по предотвращению вторжений в одноранговых беспроводных сетях. Одноранговые беспроводные сети особенно уязвимы для атак из-за их открытости, динамически изменяющейся топологии, алгоритмов совместной работы, отсутствия централизованного мониторинга, централизованной точки управления и отсутствия четкой защиты. В проводных сетях существуют методы обнаружения вторжений, но они неприменимы в беспроводной среде. В статье также представлен новый метод защиты от вторжений, основанный на обнаружении вторжений в одноранговых беспроводных сетях.
Ключевые слова: безопасность, уязвимость, защита информации, атака, вторжение, беспроводная сеть, мобильная сеть, система обнаружения, IDS, MANET, DoS, DDoS.

С ростом использования беспроводных одноранговых сетей в различных сферах деятельности вопрос обеспечения их информационной безопасности становится всё более актуальным. Уязвимость таких сетей перед атаками и отсутствие эффективных методов их обнаружения требуют проведения комплексного анализа и разработки рекомендаций по предотвращению несанкционированных вторжений [1, 2]. В связи с этим был проведен анализ способов обнаружения несанкционированных вторжений в беспроводных одноранговых сетях и предложены рекомендации по предотвращению вторжений. Также в статье предложен новый метод защиты от вторжений в одноранговых беспроводных сетях, что открывает перспективы для развития более эффективных методов обеспечения информационной безопасности в данном типе сетей.

Компьютерные сети сегодня играют важную роль в современном обществе и часто являются мишенью для злоумышленников [3]. Атаки типа «отказ в обслуживании» (DoS) или «распределенный отказ в обслуживании» (DDoS) показывают, что ни одна открытая компьютерная сеть не

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

застрахована от несанкционированного вторжения. Когда происходит вторжение, определяемое, как набор действий, который пытается поставить под угрозу целостность, надежность и доступность ресурса [4], часто используются методы защиты от вторжения, такие как шифрование и аутентификация. Однако само по себе предотвращение вторжений часто оказывается неэффективным, поскольку системы становятся все более сложными [5], а обеспечение безопасности часто остается на втором плане.

Беспроводные каналы между узлами очень уязвимы для атак. Такими атаками могут быть DoS-атаки, подслушивание, утечка информации, недостоверные данные, идентификация, модифицированные сообщения и др. Подслушивание позволяет получить доступ к конфиденциальной информации и нарушить правила безопасности [6]. Активные атаки позволяют злоумышленникам удалять, редактировать сообщения, изменять сообщения и выдавать себя за узел. Это нарушает целостность, аутентификацию. Защиту от атак на мобильную одноранговую сеть MANET можно разделить на две группы. Пассивные атаки включают в себя только перехват данных, тогда как активные атаки содержат действия, выполняемые нарушителем. То есть узел, подверженный атаке, может нарушить механизм маршрутизации некоторых протоколов [7]. Беспроводные одноранговые сети создают уникальное противоречие: с одной стороны, они обеспечивают гибкость и мобильность, с другой – они подвержены высокому риску несанкционированных вторжений из-за отсутствия централизованной структуры и уязвимости перед динамическими атаками [8]. Поэтому особенно важно разработать эффективные методы обнаружения вторжений и профилактические меры для защиты беспроводных одноранговых сетей.

Рассмотрим метод защиты от вторжений, основанный на обнаружении вторжений в одноранговых беспроводных сетях. В задачу системы обнаружения вторжений входят: мониторинг данных, обнаружение

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

вторжений в систему и инициирование соответствующего реагирования, например, инициирование автоматического возмездия злоумышленнику.

Система обнаружения доступа определяется как серия автоматических предупреждений о вторжении. IDS – это защитная система, которая обнаруживает злоумышленные действия в сети и пытается предотвратить эти действия (рис. 1, 2). У системы есть две возможности: обнаруживать и предотвращать вторжения. Инструменты IDS могут различать, является ли источник атак внешним или внутренним. Операционная модель IDS позволяет обнаруживать вторжения на основе собранных данных. Большие данные являются решающим фактором. В системе IDS установлен один или несколько алгоритмов обнаружения вторжений. Система охранной сигнализации автоматически уведомит администратора об уязвимостях в сети.

Рис. 1 – Архитектура IDS для одноранговых беспроводных сетей

Можно выделить следующие виды обнаружений:

– обнаружение аномалий. Когда в системе существует нормальная рабочая линия, то любая деятельность, отклоняющаяся от этого базового уровня, считается вторжением. Деятельность не считается противозаконной;

– обнаружение неправильного использования. Любая деятельность в интернете заранее определяется как законная или незаконная. Следовательно, любая операция, противоречащая этим определениям, будет обнаружена и признана недопустимой для использования в сети;

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

– обнаружение на основе описательной информации. Определяется набор ограничений, которые описывают точное поведение программы или протокола. Далее отслеживается, соответствует ли выполнение программы заданным ограничениям.

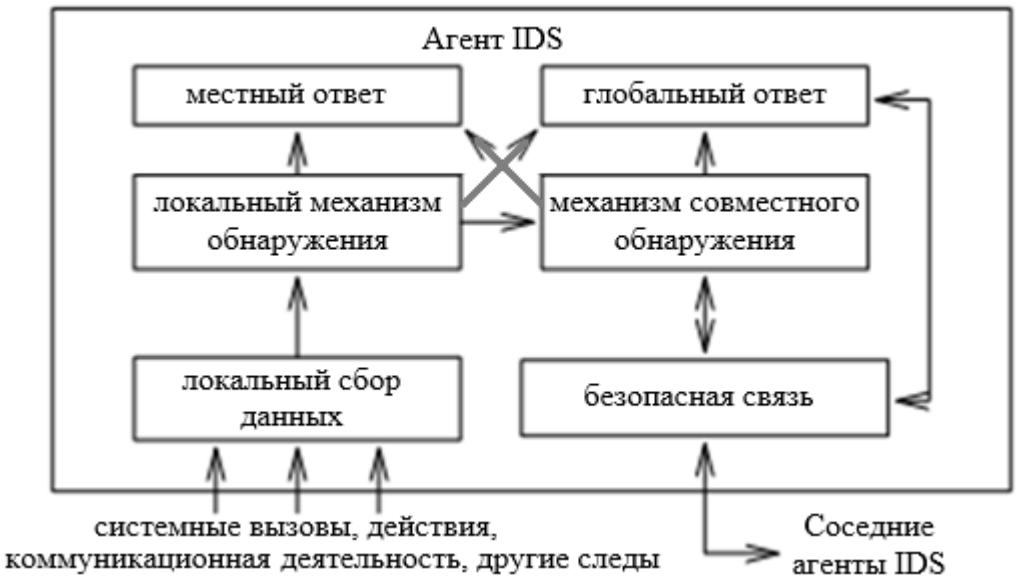

Рис. 2 – Модель системы IDS

Система обнаружения доступа для мобильных одноранговых сетей MANET. Пионеры обнаружения доступа к сетям MANET Чжан и Ли предложили интерактивную модель обнаружения вторжений, в которой каждый узел сети участвует в процессе обнаружения вторжений и реагирования на них [9]. В этой модели агент IDS работает на каждом мобильном узле и выполняет функции сбора данных и обнаружения вторжений. Внутренняя структура агента IDS состоит из 6 частей (рис. 3). Каждый узел самостоятельно осуществляет обнаружение вторжений и взаимодействует со своими соседями в более широком диапазоне. Каждый агент IDS, расположенный в каждом узле сети, также работает независимо и отслеживает внутреннюю активность, включая действия пользователя, системы и другие действия, обнаруживает вторжения и инициирует ответные меры. Агенты IDS соседних сетевых узлов участвуют в действиях по глобальному обнаружению доступа при получении уведомления о локальном

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

вторжении. Модуль сбора локальных данных собирает местные статистические данные. Локальный механизм обнаружения использует файл журнала, содержащий все системные действия для обнаружения локальных вторжений. Модуль локального ответа активирует локальные операции, т.е. агент IDS оповещает локальных пользователей, в то время, как глобальный агент объединяет сетевые узлы для выполнения предупреждений.

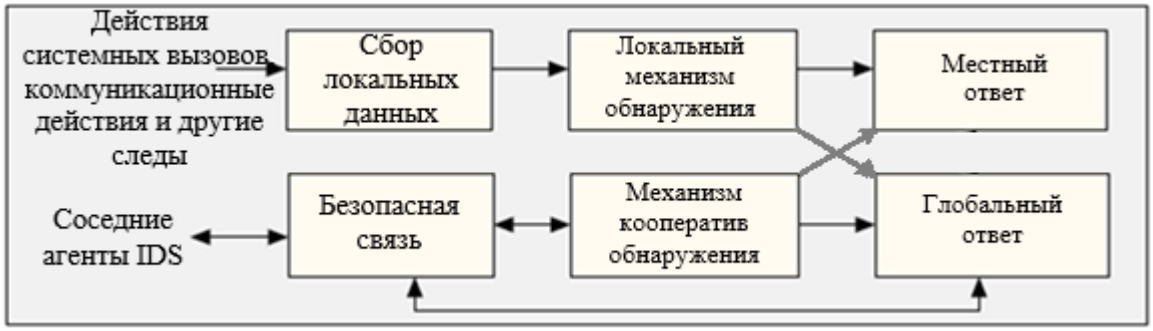

Рис. 3. – Система обнаружения вторжений для MANETS

Система IDS, основанная на протоколе AODV. Бхаргава и др. [10] представили модель обнаружения и предотвращения вторжений – IDRM. Это модель обнаружения и реагирования на вторжения, повышающая безопасность протоколов векторной маршрутизации по запросу в одноранговых сетях. В этой модели каждый сетевой узел использует информацию от соседних сетевых узлов для обнаружения неправильных действий. Когда на каком-либо узле в сети происходит неправильное действие, эта информация будет отправлена другим узлам для предотвращения этого действия. Другие узлы, получившие эту информацию, проверят свое локальное значение Malcount и добавят ответы. В модели IRM узел понимает, что другой узел удовлетворен, увеличивая свой Malcount до значения, превышающего пороговое значение. В таком случае он передает эту информацию всей сети, отправляя пакет MAL. Если у другого узла также есть подозрения, что обнаруженный узел является скомпрометированным, он сообщит о подозрениях, отправив пакет REMAL. Если переданы два и более пакета, система найдет способ изолировать узлы, отправившие этот пакет.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Некоторые из инсайдерских атак включают неправильную доставку запроса, DoS, выдачу себя за другое лицо и компрометацию пункта назначения.

Способы выявления инсайдерских атак:

– неправильное распределение маршрутов запросов. Злонамеренный узел может часто создавать ненужные маршруты. Когда узлы в сети получают количество запросов маршрута, превышающее определенный порог, от любого узла в сети, то делается вывод, что этот узел является вредоносным;

– атака типа «отказ в обслуживании». Злонамеренный узел атакует DoS, передавая поддельные пакеты данных и используя все сетевые ресурсы. DoS может быть вызван неправильной маршрутизацией сообщений или пакетов данных. Эту форму атаки можно обнаружить, если узел генерирует контролируемое пороговое количество пакетов в течении периода времени;

– компрометация места назначения. Эта атака обнаруживается, когда узлы не получают ответов от мест назначения в течении периода времени. Соседние узлы создают зонды, отправляя пакеты запроса на соединение;

– олицетворение. Этой формы можно избежать, если отправитель шифрует пакеты данных своим закрытым ключом, а другие сетевые узлы расшифровывают открытым ключом отправителя.

Таким образом, обнаружение несанкционированных вторжений в беспроводных одноранговых сетях представляет сложную и важную задачу, требующую системного подхода. Разработка и внедрение новых методов защиты от вторжений, основанных на обнаружении в одноранговых беспроводных сетях, является необходимым шагом в направлении обеспечения их информационной безопасности. Данный анализ способов обнаружения вторжений и рекомендации по предотвращению вторжений в одноранговых беспроводных сетях представляет собой важный вклад в область информационной безопасности и может послужить основой для дальнейших исследований и разработок в данной области.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Литература

1. Юсупова Р.И., Зарипова Р.С. Подходы к оценке надежности информационных систем // Научно-технический вестник Поволжья. 2023. № 12. С. 659-661.

2. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети интернет и контрмеры (обзор) / Инженерный вестник Дона. 2019. № 3. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

3. Дадашова А.С., Николаева С.Г., Джабагова С.С. Информационная безопасность и системный анализ: стратегии защиты и анализ рисков // Научно-технический вестник Поволжья. 2023. № 12. С. 239-241.

4. Гибадуллин Р.Ф., Вершинин И.С., Глебов Е.Е. Разработка приложения для ассоциативной защиты файлов // Инженерный вестник Дона. 2023. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462.

5. Gibadullin R.F., Nikonorov V.V. Development of the system for automated incident management based on open-source software // Proceedings – 2021 International Russian Automation Conference, RusAutoCon. 2021. pp. 521-525.

6. Нгуен Фук Хау, Нгуен Тхи Ань Туйет, Зарипова Р.С. Zero Trust как инструмент защиты информационных активов компаний // Научно-технический вестник Поволжья. 2023. № 12. С. 656-658.

7. Аникин И.В., Катасёв А.С., Черняков А.С. Модель и программный комплекс анализа атак на web-приложения // Научно-технический вестник Поволжья. 2023. № 7. С. 17-20.

8. Нгуен Фук Хау, Ле Дюк Хуи, Нгуен Тхуй Чанг, Зарипова Р.С. Обнаружение уязвимостей и применение методов обеспечения безопасности веб-сайта // Инженерный вестник Дона. 2024. №2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9017.

9. Zhang Y., Lee W. Intrusion Detection in Wirele Ad Hoc Networks. 6th Int'l. Conf. Mobile Comp. and Net. 2000. pp. 275–83.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

10. Bhargava S., Agrawal D.P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks. VTC 2001 Fall. vol. 4. 2001. pp.2143–47.

References

1. Yusupova R.I., Zaripova R.S. Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 12. pp. 659-661.

2. Menciev A.U., CHebieva H.S. Inzhenernyj vestnik Dona. 2019. № 3. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

3. Dadashova A.S., Nikolaeva S.G., Dzhabagova S.S. Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 12. pp. 239-241.

4. Gibadullin R.F., Vershinin I.S., Glebov E.E. Inzhenernyj vestnik Dona. 2023. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462.

5. Gibadullin R.F., Nikonorov V.V. Proceedings – 2021 International Russian Automation Conference, RusAutoCon 2021. 2021. pp. 521-525.

6. Nguyen Phuc Hau, Nguyen Thi Anh Tuyet, Zaripova R.S. Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 12. S. 656-658.

7. Anikin I.V., Katasyov A.S., CHernyakov A.S. Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 7. pp. 17-20.

8. Nguyen Phuc Hau, Le Duc Huy, Nguyen Thuy Trang, Zaripova R.S. Inzhenernyj vestnik Dona. 2024. №2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9017.

9. Zhang Y., Lee W. Intrusion Detection in Wirele Ad Hoc Networks. 6th Int'l. Conf. Mobile Comp. and Net. 2000. pp. 275–83.

10. Bhargava S., Agrawal D.P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks. VTC 2001 Fall. vol. 4. 2001. pp.2143–47.

Дата поступления: 13.02.2024

Дата публикации: 19.03.2024

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024