PROTECTING INFORMATION ON WIRELESS NETWORKS BY DYNAMIC TRAFFIC ROUTING

Rakhimov Jamshid Norboy o'g'li
Aripova Makhpuza Xashimovna
Tashkent State Technical University named after Islam Karimov, Universitet street, 2, Tashkent 100095, Uzbekistan

Abstract.

The article discusses a method of protecting information during transmission in distributed wireless networks, based on the use of a dynamic traffic routing algorithm under conditions of deliberate attacks.

Key words:

Algorithm, routing, information, mesh networks, traffic.

Развитие информационных технологий ставит актуальные задачи по повышению надежности функционирования компьютерных сетей. Для решения таких задач необходимо изучить существующие сетевые протоколы, сетевые архитектуры, разработать способы повышения безопасности передачи информационных ресурсов по сети.

Выбор в пользу беспроводных технологий позволяет получить преимущества в скорости, мобильности. Появление нового класса широкополосных беспроводных сетей с ячеистой структурой (mesh network) позволило добиться значительного увеличения площади информационного покрытия. Основным преимуществом сетей этого класса является наличие специальных устройств - mesh-порталов, позволяющих интегрировать в mesh-сеть другие беспроводные сети (WiMAX, Wi-Fi, GSM) и Интернет, а следовательно, предоставлять пользователю все возможные услуги этих сетей.

К недостаткам mesh-технологии можно отнести то, что протоколы маршрутизации mesh-сети очень специфичны, и их разработка представляет собой сложную задачу со многими критериями и параметрами. В то же время существующие протоколы требуют значительных улучшений в повышении безопасности и надежности передачи информации.

Сетевых атак, сбоев и отказов сетевого оборудования-основные факторы, влияющие на безопасность передачи информации в распределенных беспроводных сетях. И. Акилдиз, В. Ван, Х. Ван, Т. Dorges, Н. Бен Салем рассматривается проблема обеспечения безопасности передачи информации в распределенных беспроводных сетях. Обеспечение безопасности передачи информации в компьютерной сети означает защиту ее конфиденциальности, целостности и доступности.

Среди методов обеспечения доступности информации в беспроводных сетях исследователи выделяют сочетание различных методов контроля, дублирования и резервирования. Целостность и конфиденциальность информации в беспроводных сетях обеспечивается методами построения виртуальных каналов, основанными на использовании криптографических средств.

Общим недостатком этих методов является снижение производительности сети, связанное с требованиями к дополнительной обработке передаваемой информации. Указанный недостаток особенно критичен для передачи цифровой видеоинформации. Кроме того, совершенствование методов криптоанализа все больше снижает надежность существующих криптоалгоритмов.

Из вышеизложенного следует, что необходимо разработать новые методы защиты информации при передаче в распределенных беспроводных сетях в условиях преднамеренных атак. В связи с этим тема работы актуальна и практически важна.

Предлагаемая методика представлена на рис. 1 в виде IDEF диаграммы.

Методика включает последовательность следующих действий.

1. Анализ топологии распределенной сети. Выбор устройств сети для роли «доверенный сервер».

2. Установка и настройка SMS на доверенных серверах, SMC на рабочих станциях.

3. Выбор параметров передачи SMC.

4. Передача данных через доверенные сервера на основе алгоритма динамической маршрутизации.

5. Прием данных получателем, сбор статистики по построенным маршрутам, оценки реализаций возможных атак.

Главной особенностью предложенного подхода является применение ди-намической маршрутизации для цели защиты информации.

Разработанный алгоритм динамической маршрутизации информации в распределенных беспроводных сетях, описывается следующими этапами.

Шаг 1. Вычисление элементов множеств M и $F_S^{дост}$ в начальный момент времени t_0.

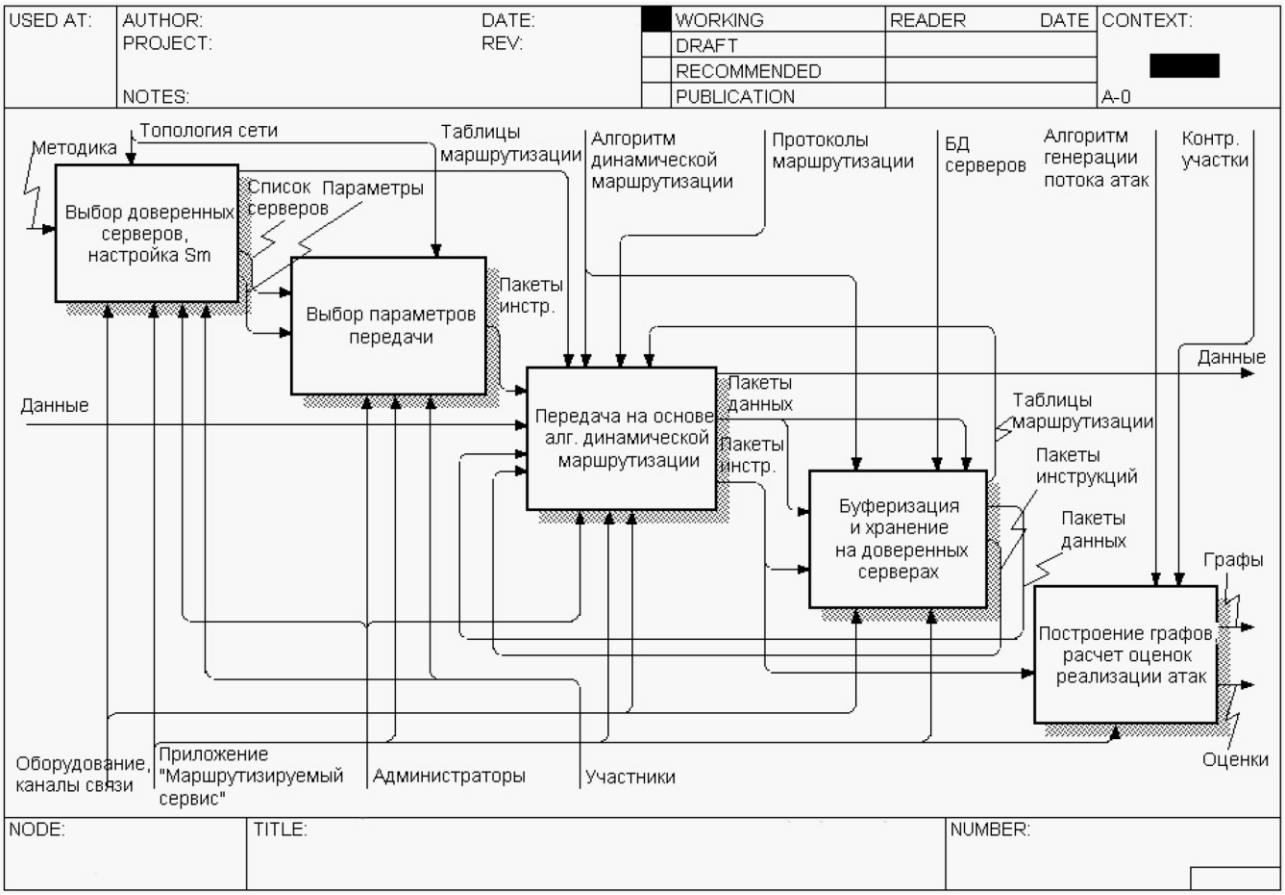

Рис. 1. Методика защиты информации в распределенных беспроводных сетях

Шаг 2. Инициализация передачи. При поступлении запроса S_{MC} на инициализацию сеанса передачи данных выполнить следующие действия:

2.1. запросить значение параметра f; 2.2. создать пакет инструкций, содержащий IP-адрес отправителя, IP-адрес получателя, значение f и раздел «доверенные сервера»; 2.3. используя операцию рандомизации, получить псевдослучайное число k; 2.4. проверить доступность F_{Sk} , если сервер недоступен – вернуться к п.2.3; 2.5. сформировать пакет данных и промаркировать его как пакет S_M; 2.6. отправить пакет данных и пакет инструкций на доверенный сервер F_{Sk}.

Если требуется дальнейшая передача данных – вернуться к п.2.5;2.7. завершить работу S_{MC}.

Шаг 3. Динамическая маршрутизация на доверенном сервере F_{Si}: 3.1. переформировать матрицу маршрутизации в случае, если разность текущего времени и времени последнего изменения M_i больше t. При получении пакетов S_M - перейти к п.3.2; 3.2. открыть полученный пакет инструкций, в раздел «доверенные сервера» добавить IP-адрес F_{Si}; 3.3. если количество записей в разделе «доверенные сервера» равно f, отправить пакеты данных, относящиеся к данному пакету инструкций, на IP-адрес получателя и вернуться на п.3.1; 3.4. используя операцию рандомизации, получить псевдослучайное число k; 3.5. проверить доступность F_{Sk}, если сервер недоступен –

вернуться к п.3.4; 3.6. проверить наличие информации о F_{Sk} в разделе «доверенные сервера»; если F_{Sk} присутствует в данном разделе – вернуться к п.3.4; 3.7. отправить пакет инструкций и относящиеся к нему пакеты данных на доверенный сервер F_{Sk}; вернуться на п.3.1.

Шаг 4. Получение пакета данных и пакета инструкций S_{MC}, определяемым IP-адресом получателя.

В заключение следует отметить, что согласно исследованиям, выполненным в работе, получены следующие результаты. 1. Проанализированы рекомендации стандартов IEEE 802.11 по защите информации в распределенных беспроводных сетях. 2. Исследованы алгоритмы динамической маршрутизации трафика в распределенных сетях. 3. Исследованы методы защиты информации в распределенных беспроводных сетях. 4. Построен алгоритм динамической маршрутизации информации при передаче в распределенных беспроводных сетях в условиях воздействия преднамеренных атак. 5. На базе алгоритма разработано приложение «маршрутизируемый сервис», реализующее методику защиты информации при передаче в распределенных беспроводных сетях.

Список литературы

1. Никонов В.И. Маршрутизация в беспроводных сетях нового поколения // Системы управления и информационные технологии. Научно-технический журнал. – Воронеж: издательство «Научная книга», 2010. – №1.1(39). – С. 170-173.
2. Никонов В.И. Методы защиты информации в распределенных компьютерных сетях с помощью алгоритмов маршрутизации // Доклады Томского государственного университета систем управления и радиоэлектроники. Научный журнал. – Томск: издательство ТГУСУР, 2010. – № 1 (21) , часть 2. – С. 219-224.
3. Маркелов, К. С. Безопасность беспроводных сетей / К. С. Маркелов, А. Б. Нейман. — Текст: непосредственный // Молодой ученый. – 2012. – №4 (39). – С. 63-66.
4. Монин С. Защита информации и беспроводные сети / С. Монин // Компьютер Пресс #4/2005 [Электронный ресурс]. – Режим доступа: http://www.redcenter.ru/?did=822&p_realm=print1

References

1. Nikonov V.I. Routing in new generation wireless networks // Control systems and information technologies. Scientific and technical journal. Voronezh: publishing house "Scientific book", 2010. No. 1.1 (39). pp. 170-173.
2. Nikonov V.I. Methods of information protection in distributed computer networks using routing algorithms // Reports of the Tomsk State University of Control Systems and Radioelectronics. Science Magazine. Tomsk: publishing house TSUSUR, 2010. No. 1 (21), part 2. pp. 219-224.
3. Markelov, KS Security of wireless networks / KS Markelov, AB Neiman. - Text: direct // Young scientist. 2012. No. 4 (39). pp. 63-66.
4. Monin S. Information security and wireless networks / S. Monin // Computer Press # 4/2005 [Electronic resource]. Access mode: http://www.redcenter.ru/?did=822&p_realm=print1