

УДК 004.732

М.Л. Карманов

Протокол маршрутизации для ad-hoc сетей

Описывается метод существенного повышения защищенности протоколов маршрутизации Ad-hoc сетей от внешних воздействий. Ad-hoc сети – это относительно новое направление, предполагающее построение самоорганизующихся вычислительных сетей на базе беспроводных технологий. Изложенный в статье метод позволяет существенным образом повысить устойчивость алгоритмов маршрутизации от внешних воздействий, при этом практически не увеличивая вычислительную сложность и объем служебного трафика.

Ключевые слова: протокол, трафик, маршрутизация, защита информации, устойчивость.

В 90-х годах широкое распространение получили мобильные компьютеры, оснащенные беспроводными интерфейсами. Именно тогда и зародилась идея создания ad-hoc сетей. Ad-hoc сеть подразумевает под собой объединение нескольких мобильных устройств с беспроводными сетевыми адаптерами в единую сеть передачи данных. При этом предполагается, что мобильные устройства принадлежат различным людям и единое централизованное административное управление отсутствует, кроме того, такие сети должны быть самоорганизующимися (самонастраивающимися). Также необходимо учитывать мобильность узлов сети и их ограниченность как в вычислительных, так и в энергоресурсах. Построение ad-hoc сетей порождает множество самых разнообразных проблем. В данной работе рассматривается только вопрос маршрутизации.

В ходе выполненного анализа существующих протоколов маршрутизации, используемых в таких сетях, выяснилось, что все они обладают слабой устойчивостью к ситуациям, при которых один или несколько узлов сети отклоняются от требований протокола. В ряде случаев такое поведение всего лишь одного узла может парализовать работу всей сети.

Был проведен детальный анализ причин неустойчивости протокола к отклонениям отдельных узлов от выполнения протокола. Выяснилось, что для большинства протоколов отклонения в работе сети обусловлены нарушением одного из двух неравенств:

$$D_B(A) > \dots > D_B(N) > \dots > D_B(B); \quad (1)$$

$$S_B(A) \leq \dots \leq S_B(N) \leq \dots \leq S_B(B), \quad (2)$$

где $D_B(N)$ – это расстояние до узла B в некоторой метрике, известное узлу N , а $S_B(N)$ – это мера актуальности информации о маршруте до узла B , известная узлу N .

Затем один из существующих протоколов динамической маршрутизации был существенным образом модернизирован. За основу был взят протокол AODV и в него был внесен ряд изменений. В данной статье приводятся только наиболее существенные из них:

1. Все служебные пакеты инкапсулируются не в протокол UDP, а в протокол канального уровня. Это позволяет локализовать область, в которой могут подделываться адреса отправителей в сообщениях.

2. Введен механизм периодического обмена таблицами маршрутизации между соседними узлами. Тем самым к знаниям узла о топологии сети добавляются также знания его соседей. Это позволяет в большинстве случаев выявлять нарушение неравенств (1) и (2) и блокировать связь с узлом-нарушителем на длительное время.

3. Благодаря периодическому обмену таблицами маршрутизации между соседними узлами, был также введен механизм быстрого восстановления маршрутов в случае нарушения одной из промежуточных связей. При этом многократно сократилось время на восстановление нарушенного маршрута, а также уменьшился объем трафика, передаваемого по сети для восстановления нарушенного маршрута.

4. Изменена метрика сети. Под длиной связи понимается остаточная пропускная способность канала. Это позволило ввести в протокол AODV функции балансировки нагрузки и избавиться от проблемы протокола AODV, связанной с повышенной нагрузкой на каналы передачи данных, находящиеся в центральной части вычислительной сети.

5. Добавлена возможность включения блока данных в пакет запроса построения маршрута, что позволило в случае использования протокола TCP передавать в месте с запросом на построение маршрута и запрос на установление соединения, что примерно на 35%

снизило задержку при установлении соединения с новым узлом, маршрут до которого был ранее не известен.

Также было внесено множество других изменений, некоторые из которых не влияли на защищенность протокола, но увеличивали его эффективность. Общее количество внешних изменений равно шестнадцати.

Было проведено моделирование работы нового протокола и проведен сравнительный анализ с другими протоколами. Наиболее показательными являются следующие результаты, полученные в сравнении со стандартным протоколом AODV:

1. Объем служебного трафика увеличился всего на 13%.
2. Среднее время построения маршрута осталось неизменным.
3. Среднее время восстановления маршрута сократилось на 81%.
4. Количество операций полного восстановления маршрута (инициированных одним из конечных узлов) сократилось на 98%.
5. Средняя задержка в установлении TCP-соединения с новым узлом сократилась на 36%.
6. Воздействие типа Deny-of-service на вычислительную сеть локализовано зоной покрытия приема-передающего устройства, осуществляющего воздействие.
7. Воздействие типа man-in-the-middle локализовано зоной диаметром в 1-2 узла от источника воздействия.

Литература

1. Perkins C.E. Ad hoc On-Demand Distance Vector (AODV) Routing / C.E. Perkins, C.E. Belding-Royer // RFC 3561. – 2003. – July.
2. Broch J. et al. A performance comparison of multi-hop wireless ad hoc network routing protocols / J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J. Jetcheva // Proc. of MOBICOM'98, 1998.
3. Basagni S. et al. Mobility- Adaptive Protocols for Managing Large Ad Hoc Network / S. Basagni, D. Turgut, S.K. Das // Proceedings of the IEEE International Conference on Communications (ICC). – 2001. – P. 1539–1543.
4. Kawadia V. System services for implementing Ad-Hoc routing: Architecture, Implementation and Experiences / V. Kawadia, Y. Zhang, B. Gupta // Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys), June 2003. San Francisco, CA. – P. 99–112.
5. Zhou L. Securing Ad Hoc Networks / L. Zhou, Z.J. Haas // IEEE Networks Special Issue on Network Security. – 2000. November/December.
6. Белов Е.Б. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
7. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во УрГУ, 2003. – 328 с.

Карманов Максим Леонидович

ГОУ ВПО «Южно-Уральский государственный университет»,
аспирант каф. цифровых радиотехнических систем
Эл. адрес: Karmanov.maxim@gmail.com

M.L. Karmanov

Routing in ad-hoc networks

In given article the method of essential increase of security of reports of routeing Ad-hoc of networks from external influences is described. Ad-hoc networks is rather new on-board, assuming construction self-organized computer networks on the basis of wireless technologies. The method stated in article allows to raise essentially stability of algorithms of routeing from external influences, thus, practically without increasing computing complexity and volume of the traffic.

Keywords: protocol, traffic, routing, information security, stability.