УДК 621.391 + 004.58

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В САМООРГАНИЗУЮЩИХСЯ АВТОМОБИЛЬНЫХ СЕТЯХ VANET

Р.А. Бельфер, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.; a.belfer@yandex.ru
А.С. Моёров, инженер департамента информационной безопасности ООО «ITS – Системная интеграция»

Ключевые слова: *угроза, особенности угроз, информационная безопасность, самоорганизующаяся сеть, нарушитель.*

Введение. Среди перспективных технологий беспроводных самоорганизующихся сетей связи особое место занимают автомобильные сети связи VANET (Vehicular Ad-hoc Networks) [1], предназначенные для повышения эффективности и безопасности дорожного движения. В настоящее время в мире при поддержке индустрии, государственных и академических институтов реализуются несколько научно-исследовательских проектов, в основе которых лежит принятый в апреле 2010 г. стандарт IEEE 802.11p [2]. Указанный стандарт разработан для поддержки связи между машинами и объектами дорожной инфраструктуры, а также непосредственно между автомобилями, движущимися со скоростями до 200 км/ч на расстоянии до 1000 м.

Основные цели использования сетей VANET [3]:

- помощь водителю (навигация, предотвращение столкновений и смена полос);
- информирование (получение данных об ограничении скорости или проведении ремонтных работ);
- предупреждение (информация о препятствиях или состоянии дорог, в том числе о послеаварийных ситуациях).

Для беспроводных самоорганизующихся сетей связи, к которым, кроме VANET, относятся также сенсорные, ячеистые, или mesh-сети, MANET [4], особенно важно обеспечение информационной безопасности, причем для VANET реализация этой задачи имеет определенную специфику. Для

этой технологии характерны высокая динамическая природа сети, частая смена топологии, непостоянные пользователи и кратковременные связи между пользователями [5]. Еще одна особенность VANET – большое число взаимодействующих объектов в течение короткого времени.

Настоящая работа посвящена анализу особенностей угроз информационной безопасности в сетях VANET.

Требования к информационной безопасности. Анализ работ [5–7] позволяет суммировать требования к информационной безопасности сетей VANET.

Подлинность источника сообщений. Узлы сети VANET должны реагировать только на сообщения, посланные зарегистрированными пользователями. Для этого необходима гарантия отсутствия в сети узлов, имеющих несколько разных уникальных меток и выдающих себя за легитимные узлы. Следовательно, оператору предстоит внедрить на сети механизм установления подлинности источника сообщения.

Целостность сообщений. Сообщение не должно быть изменено во время передачи. Это требование в совокупности с обеспечением подлинности источника сообщений гарантирует получение легитимного сообщения.

Невозможность отказа от авторства. Водитель, пославший сообщение, не должен иметь возможность отказаться от факта передачи сообщения, который может сыграть решающую роль при определении реальной последовательности событий в расследовании инцидентов.

Соблюдение ограничений на допустимый интервал времени на получение информации. Получатель сообщения должен быть уверен, что интервал времени между созданием, отправкой и получением сообщения не превышает допустимого интервала: это может служить подтверждением легитимности принятого им сообщения.

Контроль доступа. Необходимо обеспечить защиту доступа пользователя в сеть с предоставлением ему несанкционированных привилегий и услуг.

Конфиденциальность сообщений. Это требование не является обязательным для всех пользователей. Однако в случае, когда обмен информацией происходит между пользователями службы безопасности, оно приобретает нормативный характер.

Приватность. Речь идет о защите данных о местоположении пользователя.

Особенности угроз информационной безопасности. Угрозу информационной безопасности в сети VANET представляют самые разные нарушители. Это, в частности, могут быть недобросовестные водители. Большинство водителей-абонентов сети VANET – законопослушные граждане, они должны соблюдать, как мы полагаем, правила безопасного взаимодействия с другими участниками сети, однако среди них могут найтись и такие, кто попытается извлечь из данной услуги максимальную личную выгоду. Как вариант, например, можно предположить ситуацию, когда водитель посылает ложную информацию, чтобы направить трафик по другому маршруту и освободить себе путь.

Цель мошенников, использующих прослушивание, собрать информацию о водителях, чтобы с ее помощью анализировать поведение участников дорожного движения и потоки трафика. Еще одна категория злоумышленников – инсайдеры, которые, работая в автомобильных компаниях, производят установку и настройку модулей для построения сети VANET.

И нельзя не отметить, что большими финансовыми и прочими возможностями по созданию инструментов для реализации угроз информационной безопасности в сетях VANET обладают криминальные элементы.

Угрозы информационной безопасности, характерные для сетей VANET, имеют свою специфику. Для успешного противодействия этим угрозам следует принимать во внимание противоречивость требований к гарантии подлинности источника сообщений и приватности в сетях VANET. Гарантией того, что определенные узлы именно те, за кого себя выдают, может служить выполнение требования, чтобы любое сообщение принималось на обработку, только если подтверждается подлинность источника этого сообщения. Однако таким образом можно узнать местоположение автомобиля, а это уже приватные данные пользователя. Значит, система обеспечения безопасности должна быть спроектирована так, чтобы разрешать анонимный обмен сообщениями, но при этом допускать возможность идентификации узлов в отдельных случаях, например при расследовании инцидентов.

Высокая мобильность и частая смена пользователей могут привести к угрозе отказа в обслуживании. В автомобильных сетях VANET узлы движутся с огромной скоростью. При этом быстро меняется число соседних узлов, преобладают разовые и кратковременные взаимодействия пользователей. Как результат – между водителями формируется большой поток сообщений, вызывающий перегрузки и угрозу отказа в обслуживании. К перегрузкам, следствием которых является угроза отказа в обслуживании, также ведет высокая вероятность всплеска трафика при аварии и других причинах (пробках). Все это, помимо прочего, может привести к возникновению угрозы нарушения качества обслуживания.

Следует особо отметить такую особенность сети VANET, как зависимость от глобальных навигационных систем. Любые ошибки в этих системах сказываются на функционировании VANET, что связано с угрозой получения недостоверных данных, необходимых в аварийных ситуациях.

Выводы. Отмеченные особенности угроз информационной безопасности сетей VANET не позволяют применить существующие механизмы защиты, используемые в других беспроводных самоорганизующихся сетях. Считаем целесообразным продолжить дальнейшие исследования, направленные на разработку механизмов защиты информационной безопасности в сетях VANET.

ЛИТЕРАТУРА

1. **Кучерявый А.Е., Винель А.В., Ярцев С.В.** Особенности развития и текущие проблемы автомобильных беспроводных сетей VANET //Электросвязь. – 2009. – № 1.
2. IEEE Std. 802.11-2010, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Wireless Access in Vehicular Environments.
3. **Glass S., Portmann M., Muthukkumarasamy V.** Securing Route and Path Integrity in Multihop Wireless Networks //Security of Self-Organizing Networks. MANET, WSN, WMN, VANET. – CRC Press, 2010.
4. **Бельфер Р.А.** Угрозы информационной безопасности в беспроводных самоорганизующихся сетях //Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение», «Технические средства и системы защиты информации». – 2011.
5. **Gokhale V., Ghosh S.K., Gupta A.** Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks //Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. – CRC Press, 2010.
6. **Raya M., Hubaux J.-P.** Securing vehicular ad hoc networks // Journal of Computer Security. – 2007. № 15.
7. **Parno B., Perrig A.** Challenges in securing vehicular networks // Fourth Work-shop on Hot Topics in Networks, 2005.

Получено 27.02.12