Схема аутентификации в сетях VANET с использованием инфраструктуры придорожных блоков

К.А. Ковалев[1], А.А. Агафонов[1]

[1]*Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34а, Самара, Россия, 443086*

Аннотация

Сети VANET – это класс автомобильных самоорганизующихся сетей, предназначенных для обмена данными между транспортными средствами и объектами дорожной инфраструктуры. Передача сообщений в такой открытой среде, как VANET, ведет к необходимости рассмотрения ключевых проблем безопасности. Аутентификация, конфиденциальность данных, целостность данных, доступность данных - важнейшие компоненты безопасности в VANET. В статье рассматривается задача аутентификации в сетях VANET и исследуется схема аутентификации с использованием инфраструктуры придорожных блоков (RSU). Экспериментальные исследования в системе моделирования автомобильных сетей Veins показывают преимущество представленной схемы по сравнению с классическим подходом на основе инфраструктуры открытых ключей по критерию потребляемых вычислительных ресурсов.

Ключевые слова

VANET, Аутентификация, RSU, Veins

1. Введение

Автомобильные самоорганизующиеся сети (VANET) являются ключевым компонентом интеллектуальных транспортных систем и в ближайшем будущем могут активно использоваться для повышения безопасности дорожного движения, решения навигационных и других задач в транспортных сетях. В сетях VANET каждой транспортное средство может обмениваться информацией с другими транспортными средствами и объектами инфраструктуры (Road Side Unit – RSU), что, в свою очередь, ведет к необходимости решения задач информационной безопасности: аутентификации, конфиденциальности данных и т.д. Обзор коммуникационных архитектур и основных проблем конфиденциальности и безопасности в сетях VANET представлен в [1]. Для решения задач аутентификации были предложены различные схемы. Подход на основе анонимных ключей основан на использовании большого числа краткосрочных ключей и сертификатов для формирования и проверки подписи сообщения [2]. Подход на основе групповой подписи исследовался в [3]. Сравнение схем на основе инфраструктуры открытых ключей (PKI) и симметричного шифрования представлено в [4]. В схемах, основанных на RSU [5, 6] транспортные средства аутентифицируют друг друга с посредством инфраструктуры придорожных блоков. В статье исследуется схема аутентификации данного типа.

2. Схема аутентификации

Представленная схема аутентификации транспортных средств (ТС) с использованием RSU состоит из следующих шагов:

1) Если ТС V_i обнаруживает блок RSU_j в своем диапазоне связи, инициируется взаимная аутентификация для установки общего секретного ключа P_{ij}^c между V_i и RSU_j с использованием протокола Диффи–Хеллмана. Транспортному средству ставится в соответствие сессионный идентификатор ID_i.

2) При отправке сообщения M_i ТС V_i использует ключ P_{ij}^c для формирования кода аутентификации $HMAC(ID_i || M_i)$ и выполняет широковещательную рассылку информации $ID_i || M_i || HMAC(ID_i || M_i)$.

3) При получении информации от ТС V_i блок RSU_j проверяет код аутентификации с использованием P_{ij}^c. Полученный результат аутентификации $H(ID_i || M_i)$ подписывается закрытым ключом $Pr\,K_j$ блока RSU_j и рассылается в диапазоне связи блока.

4) Когда ТС V_k получает информацию от V_i, оно записывает ее в буфер. Далее, при получении сообщения $H(ID_i || M_i)$ от блока RSU_j выполняется проверка цифровой подписи открытым ключом $Pu\,K_j$ блока RSU_j и извлечение результата аутентификации ТС V_i.

Экспериментальные исследования схемы аутентификации были проведены в системе моделирования Veins. Представленная схема позволила снизить вычислительные затраты на выполнение процедуры аутентификации по сравнению с подходом на PKI.

3. Заключение

В работе исследуется схема аутентификации транспортных средств в сетях VANET посредством инфраструктуры придорожных блоков (RSU). В предложенной схеме проверка подписи сообщений происходит в блоках RSU, что позволяет снизить вычислительные затраты и уменьшить объем передаваемой информации. Экспериментальные исследования представленной схемы аутентификации, реализованной в системе моделирования автомобильных сетей Veins, подтвердили преимущество представленной схемы по сравнению с классическим подходом на основе инфраструктуры открытых ключей по критерию потребляемых вычислительных ресурсов.

4. Благодарности

Работа выполнена при частичной финансовой поддержке гранта РФФИ № 18-29-03135-мк.

5. Литература

[1] Mejri, M.N. Survey on VANET security challenges and possible cryptographic solutions / M.N. Mejri, J. Ben-Othman, M. Hamdi // Vehicular Communications. – 2014. – Vol. 1(2). – P. 53-66. DOI: 10.1016/j.vehcom.2014.05.001.

[2] Raya, M. The security of vehicular ad hoc networks / M. Raya, J.-P. Hubaux // Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks. – 2005. – Vol. 2005. – P. 11-21. DOI: 10.1145/1102219.1102223.

[3] Guo, J. A group signature based secure and privacy-preserving vehicular communication framework / J. Guo, J.P. Baugh, S. Wang // Mobile Networking for Vehicular Environments, MOVE. – 2007. – P. 103-108. DOI: 10.1109/MOVE.2007.4300813.

[4] Ibrahim, S. A comparison on VANET authentication schemes: Public Key vs. Symmetric Key / S. Ibrahim, M. Hamdy // Tenth International Conference on Computer Engineering & Systems (ICCES). – 2015. – P. 341-345. DOI: 10.1109/ICCES.2015.7393072.

[5] Wu, H.-T. RSU-based message authentication for vehicular ad-hoc networks / H.-T. Wu, W.-S. Hsieh // Multimedia Tools and Applications. – 2013. – Vol. 66(2). – P. 215-227. DOI: 10.1007/s11042-011-0792-3.

[6] Bayat, M. NERA: A new and efficient RSU based authentication scheme for VANETs / M. Bayat // Wireless Networks. – 2020. – Vol. 26(5). – P. 3083-3098. DOI: 10.1007/s11276-019-02039-x.