

УДК 003.26.09

**РАЗРАБОТКА ПРОТОКОЛА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ УСТРОЙСТВ В
САМООРГАНИЗУЮЩИХСЯ СЕТЯХ**

Романова У.М. (Университет ИТМО)

Научный руководитель – к.т.н., Таранов С.В.

(Университет ИТМО)

Аннотация: Целью работы является снижение вероятности проведения атак «человек посередине» при аутентификации в самоорганизующихся сетях MANET. Основное содержание исследования посвящено анализу существующих методов аутентификации в самоорганизующихся сетях, а также их преимуществам и недостаткам. Результатом работы является алгоритм протокола взаимной аутентификации устройств в самоорганизующихся сетях MANET.

Введение. Киберпреступность сегодня распространена в разных формах, но одной из старейших и самых опасных является атака типа «человек посередине». Одной из основных мер по защите данных от атак типа «человек посередине» является обеспечение надежной аутентификации пользователя. Существует множество подходов к аутентификации и еще больше реализаций этих подходов, но в сфере самоорганизующейся сети пока не существует ни одного стандарта для аутентификации устройств. Потому что не все классические решения задачи аутентификации подходят для использования в самоорганизующихся сетях. А различные типы систем предъявляют свои уникальные требования к подсистемам аутентификации. Кроме того, активное развитие вычислительной техники позволяет легко взламывать алгоритмы аутентификации, которые еще 10-15 лет назад считались надежными. В связи с этим ведется непрерывная работа в области исследования и разработки методов аутентификации. Постоянно появляются новые и совершенствуются существующие алгоритмы, направленные на обеспечение защищенной аутентификации пользователей. На данный момент не существует универсального решения, которое может обеспечить необходимый уровень защищенности при аутентификации устройств в самоорганизующихся сетях.

Основная часть. В данной работе в качестве решения проблемы аутентификации устройств при проведении атаки «человек посередине» в самоорганизующихся сетях выступает протокол взаимной аутентификации устройств на основе анализа существующих алгоритмов аутентификации с учетом функциональности самоорганизующихся сетей.

Выводы. Результаты данного исследования могут выступать в качестве теоретической основы для проведения дальнейших исследований в области аутентификации в самоорганизующихся сетях MANET, а также имеют ценность для оценки эффективности разработанного протокола с помощью имитационного моделирования самоорганизующейся сети MANET при проведении атаки типа «человек посередине», что и планируется сделать в будущем в рамках данной исследовательской работы.

Романова У.М. (автор)

Подпись

Таранова С.В. (научный руководитель)

Подпись