УДК 004.94

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ГРУППЫ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ НА ОСНОВЕ МЕТОДОВ РЕПУТАЦИИ, ДОВЕРИЯ И КАЧЕСТВА ДАННЫХ

Чупров С.С. (Университет ИТМО)
Научный руководитель – к.ф.-м.н., доцент Комаров И.И.
(Университет ИТМО)

В работе приведено описание предлагаемого подхода для обеспечения информационной и функциональной безопасности группы беспилотных транспортных средств на основе комбинации методов репутации и доверия и качества данных. Оценка эффективности предложенного подхода была произведена с использованием программных средств имитационного моделирования. Полученные в ходе моделирования результаты позволяют сказать о целесообразности предложенного подхода.

Введение. В последние годы развитие научно-технического прогресса и формирование таких концептов, как Интернет вещей и «Умный город» привели к революции в области беспилотных транспортных средств (БТС). Уже сегодня существуют БТС, способные самостоятельно передвигаться по дорогам общего пользования без воздействия на органы управления со стороны водителя. Концепции внедрения БТС подразумевают использование средств беспроводной коммуникации автомобилями и наличие объектов транспортной инфраструктуры, обеспечивающей БТС необходимой информацией о состоянии дорожного покрытия, погодных условиях, инцидентах на дороге и т.п. Как и в любых компьютерных сетях, такая коммуникация подвержена угрозам безопасности информации при её передаче и обработке. Несмотря на существующие «традиционные» методы защиты информации, такие, как, например криптографические алгоритмы, существуют деструктивные воздействия, против которых такие меры не являются эффективными. Например, такое деструктивное информационное воздействие (ДИВ) может возникнуть, когда БТС, уже авторизованное в системе, начинает передавать участникам движения и объектам транспортной структуры недостоверные данные о своём текущем местоположении или скорости движения. Такое может произойти как по причине случайно возникшей неисправности или выхода из строя какого-либо из элементов БТС, так и по причине вредоносного вмешательства злоумышленника в программно-аппаратные составляющие. Для обнаружения БТС, передающих недостоверные данные и защиты от подобных ДИВ, может быть применена комбинация метода на основе репутации и доверия, а также метода оценки качества данных, которые будут описаны ниже.

Основная часть. Методы на основе репутации и доверия получили популярность в области электронной коммерции, где существует необходимость в присваивании рейтинга множеству пользователей. Такой рейтинг часто определяет добросовестность пользователя в выполнении своих обязательств (например, продавец товара в интернет-магазине).

Метод оценки качества данных предполагает выделение у передаваемой информации и у пользователей различных метрик, которые позволяют оценить релевантность такой информации к контексту и нуждам пользователя, а также её соответствие предъявляемым требованиям. Например, в случае снижения качества изображения, получаемого с камеры БТС, могут возникнуть проблемы в работе системы машинного зрения при распознавании дорожных знаков. В этом случае можно сказать об ухудшении качества получаемой информации.

В рамках работы предлагается использовать комбинацию данных методов для обнаружения БТС, передающих некорректные данные другим участникам движения. Для этого необходимо ввести следующие показатели оценки БТС и передаваемой информации:

- *Truth* – индикатор, характеризующий субъективную оценку данных, переданных от БТС в текущий момент времени;
- *Reputation* – индикатор, характеризующий ретроспективную оценку данных, переданных БТС с начала работы системы;
- *Trust* – индикатор, состоящий из комбинации *Truth* и *Reputation* и характеризующий уровень доверия к БТС в текущий момент времени.

При инициализации группы БТС в начальный момент времени, при передаче первого информационного сообщения, необходимо сформировать показатели *Reputation* и *Trust*. Исходя из введённых выше определений, показатель *Reputation* невозможно оценить без ретроспективной оценки предыдущих данных, передаваемых БТС, показатель *Trust* предполагает наличие показателя *Reputation*, поэтому формирование его оценки также невозможно. В данном случае, для формирования этих показателей в начальный момент времени работы системы, предлагается использовать концепцию оценки качества данных (показатель *DQ*). Предполагается, что все БТС в группе являются гомогенными и имеют одинаковые технические характеристики. Таким образом, выход какого-либо из составных элементов БТС из строя или реализация вредоносного несанкционированного вмешательства непременно вызовут изменения в характеристиках программно-аппаратных средств и/или отклонение от штатных режимов работы БТС. Показатель качества данных представляет собой функцию оценки параметров элементов БТС. При появлении отклонений от эталонных показателей, значение *DQ* изменится, что говорит о возникновении неполадок в работе БТС или вредоносном вмешательстве. В начальный момент времени предлагается показателю *Reputation* присваивать значение *DQ*, что позволит формировать объективную оценку в условиях отсутствия ретроспективной оценки данных, переданных БТС.

Выводы. В качестве оценки эффективности подхода было произведено имитационное моделирование с использованием программного симулятора. Симулятор позволяет моделировать движение группы БТС через перекрёсток автомобильных дорог. Результаты моделирования показали, что предложенный подход позволяет эффективно обнаруживать БТС, передающие недостоверные данные при различном уровне нагрузки трафика.

Чупров С.С. (автор)

Комаров И.И. (научный руководитель)