Новое исследование раскрывает проблемы систем распознавания, способные привести к ДТП.

Команда исследователей из известных университетов, включая SUNY Buffalo, Iowa State, UNC Charlotte и Purdue, смогла превратить автономный автомобиль, управляемый платформой Apollo от китайского интернет-гиганта Baidu, в опасную угрозу для других участников дорожного движения, обманув его многосенсорную систему при помощи подручных средств.

«Многочисленные эксперименты на реальных автономных автомобилях показали, что предложенная атака может непрерывно скрывать целевое транспортное средство от системы восприятия беспилотного автомобиля с помощью всего двух небольших враждебных объектов», — объяснили исследователи. Их работа была опубликована на 30-й ежегодной Международной конференции по мобильным вычислениям и сетям.

В то время как другие исследователи ранее сосредотачивались на программных уязвимостях в системах автономных автомобилей, эта команда расширила методы манипуляции и обманула системы, применяющие одновременно LiDAR, камеру и радар.

Новая атака применяет отражение миллиметровых волн от гладкой металлической поверхности для манипуляции беспилотными системами. Для этого исследователи использовали «дешёвые» и «легко изготовляемые» объекты, такие как картон, металлическая фольга и разноцветные изображения.

«Размещая гладкую металлическую поверхность между радаром и целевым транспортным средством под определённым углом, можно отклонить передаваемые миллиметровые волны от приёмника радара, что приводит к снижению энергии эхо-сигналов от транспортного средства», — пояснили авторы исследования. «Когда энергия становится ниже определённого порога, целевое транспортное средство скрывается от радарного восприятия».

Цветные пятна на целевом автомобиле искажают значения пикселей входного изображения и влияют на восприятие камерой Apollo, а отражения запутывают работу лазеров LiDAR. Таким образом, все три сенсорные системы начинают сбоить и теряют автомобиль с радара.

Исследователи предполагают, что такую атаку можно проводить с помощью дронов, которые «скрывают» вторичное транспортное средство от беспилотного автомобиля,

проецируя или неся враждебный объект:

При помощи такой системы всего пара дронов, управляемых злоумышленниками, способна спровоцировать серьёзное дорожно-транспортное происшествие и тут же скрыться в неизвестном направлении, не оставив и следа.

Тем временем, в отсутствие дронов систему можно установить и на задней части транспортного средства и даже замаскировать под рекламный баннер, как это показано на изображении ниже:

Хотя в атаке применялись платформы Baidu Apollo, использованная стратегия теоретически может быть применена и к другим системам обнаружения, используемым в беспилотных автомобилях.

Тем временем, в Китае такие атаки могут привести к по-настоящему серьёзным последствиям, так как беспилотные такси там активно используются с ноября 2021 года, охватывая свыше 10 городов.