Олег В. Казарин[1,2]
[1]*Институт проблем информационной безопасности МГУ имени М.В. Ломоносова, Мичуринский просп., 1, г. Москва, 119192, Россия*
[2]*Институт информационных наук и технологий безопасности РГГУ, ул. Кировоградская, 25, корп. 2, г. Москва, 117534, Россия*
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

СОКРЫТИЕ КООРДИНАТ В ОБОБЩЕННОЙ ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.10

Аннотация. В связи со стремительным развитием систем автопилотируемого транспорта (беспилотных автомобилей, беспилотных летательных аппаратов – дронов) все более актуальной становится задача предотвращения столкновений (задача об опасной близости), тем более в условиях большого количества участников движения и его интенсивности. Если появляется злоумышленник, способный контролировать одного или нескольких участников движения, стратегией которого является создание аварийной ситуации на дороге в виде столкновений беспилотных автомобилей, например, то возникает и необходимость защищаться от такого злонамеренного поведения. Одним из вариантов такой защиты является использование для решения этой прикладной задачи концепции многосторонних конфиденциальных вычислений, в том числе и потому, что будущие системы автопилотирования предполагают в некоторой локальной зоне управления движением возможность взаимодействия участников по схеме «каждый – с – каждым», что является необходимым условием для систем многосторонних конфиденциальных вычислений в условиях разного рода несанкционированных действий.
В отличие от ранее опубликованных результатов с использованием указанной концепции в модели с так называемым получестным противником в настоящей статье впервые предлагаются некоторые решения по защите участников движения от злонамеренного противника, который, раскрыв координаты движущихся объектов, пытается осуществить их столкновение, а также рассматривается расширение этой задачи на трехмерное измерение. В то же время показывается, что при реализации указанных систем на практике, скорее всего, возникнут ситуации, которые не решаются только математическими методами. Существует большой пул проблем, которые должны решаться различными организационно-техническими и управленческими методами. Тем не менее перспективы использования методов доказуемо безопасного сокрытия координат подобного типа выглядят, на взгляд автора, вполне привлекательными для специалистов в области информационной безопасности, связи, транспорта, распределенных систем.
Ключевые слова: системы автопилотируемого транспорта, сокрытие географических координат, конфиденциальные вычисления, конфиденциальное вычисление функции, двусторонние и многосторонние протоколы конфиденциальных вычислений.
Для цитирования: КАЗАРИН, Олег В. СОКРЫТИЕ КООРДИНАТ В ОБОБЩЕННОЙ ЗАДАЧЕ ОБ ОПАСНОЙ БЛИЗОСТИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 108-117, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1165>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.10.

Oleg V. Kazarin[1,2]
[1]*Institute of Information Security Issues, Lomonosov MSU, Michurinsky Pr., 1, Moscow, 119192, Russia*
[2]*Institute for Information Sciences and Security Technologies, RSUH, Kirovogradskaya St., 25, bidg 2, Moscow, 117534,*
e-mail: okaz2005@yandex.ru, http://orcid.org/0000-0002-5098-0962

Coordinate hiding in solving the generalized dangerous proximity problem

DOI: http://dx.doi.org/10.26583/bit.2018.4.10

Abstract. In connection with the rapid development of autopilot transportation systems (driverless cars, unmanned aerial vehicles – drones) all the more urgent becomes the problem of collision avoidance (the problem of dangerous proximity), especially in conditions of a large number of members of the traffic and its high intensity. If there is an attacker who is able to control one or more participants in the traffic, which strategy is to create an emergency on the road or collisions of unmanned vehicles there is a need to protect against such malicious behavior. One of the options of such protection is the use of the concept of

multilateral confidential calculations to solve this particular problem. The future autopilot systems assume in some local traffic control zone the possibility of interaction of participants according to the "everyone-with-everyone" scheme, which is a necessary condition for multilateral confidential computing systems in conditions of various unauthorized actions.
In contrast to the previously published results using this concept in the model with the so-called semi-honest enemy, this article for the first time proposes some solutions to protect the traffic participants from the malicious actor, who, having revealed the coordinates of moving objects, tries to drive them to collision. It is also considered the expansion of this problem to three dimensions. At the same time, it is shown that the implementation of these systems in practice, most likely, does not help to avoid the problematic situations that are not solved only by mathematical methods. There is a large set of problems that must be solved by various organizational, technical and managerial methods. Nevertheless, the prospects of using the methods of provably safe coordinate hiding look, in the author's opinion, quite attractive for experts in the field of information security, communications, transport, and distributed systems.
Keywords: autopilot transport systems, geographic coordinates hiding, secure computation, secure function evaluation, two-party and multi-party protocols of secure computation.
For citation: KAZARIN, Oleg V. Coordinate hiding in solving the generalized dangerous proximity problem. IT Security (Russia), [S.l.], v. 25, n. 4, p. 108-117, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1165>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.10.

1. Введение и неформальная постановка задачи исследования

Задача об опасной близости возникает сегодня в авиации, на автомобильном, водном и железнодорожном транспорте. Еще более актуальной она станет уже в недалеком будущем – при реализации систем управления беспилотными автомобилями, беспилотными летательными аппаратами, безэкипажными надводными и подводными судами. Предотвращение столкновений движущихся объектов – это сложный, распределенный организационно-технологический процесс между различными участниками движения. Особую управленческую проблематичность такому процессу придают непреднамеренные и тем более злонамеренные деструктивные информационно-технические воздействия на этот процесс. Решение таких задач ведется на разных направлениях, в том числе и на научном.

В этом случае может анализироваться следующая проблемная ситуация. Рассматриваются два типа движущихся точечных объектов: *объект-запрос* (или просто – *запрос*) движется снизу-вверх (с юга на север) в прямоугольнике и *объект-данные* (или просто – *объект*) движутся слева-направо (с запада на восток) в этом же прямоугольнике [1 – 3]. При этом предположим, что траектории объектов, движущихся в одном из этих направлений внутри прямоугольника, не пересекаются. *Задача об опасной близости* (или *задача о предотвращении столкновений*) заключается в перечислении для каждого запроса тех и только тех объектов, которые будут находиться в некоторый момент времени в процессе своего движения на расстоянии не более, чем заданное расстояние r, где r – радиус круга с центром, представляющим собой движущийся объект (см. рис. 1). На рис. 2 представлено расширение этой задачи на трехмерное пространство.

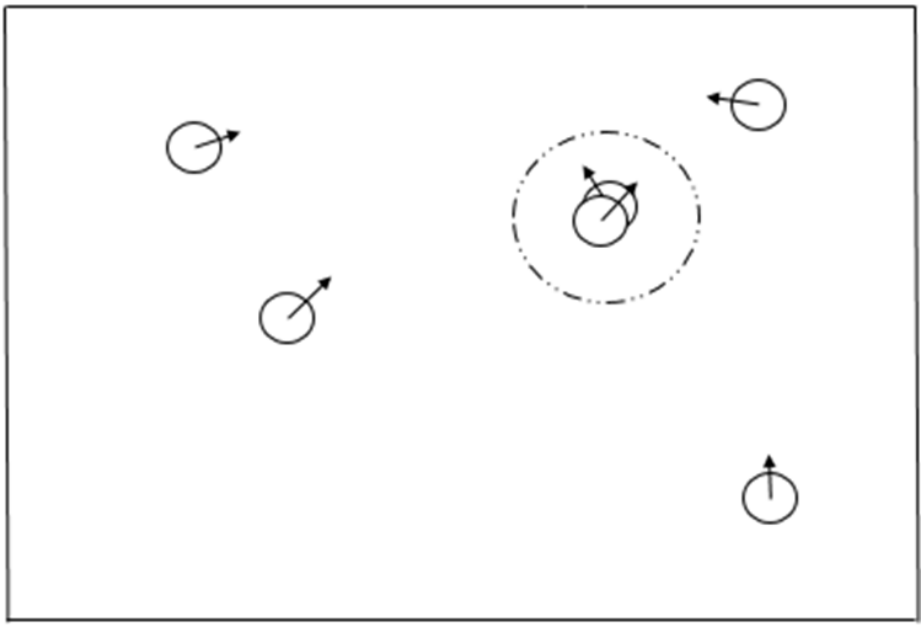

Рис. 1. Иллюстрация движения точечных объектов в двухмерной задаче об опасной близости (Fig. 1. Illustration of a movement of point objects in a two-dimensional problem on dangerous closeness)

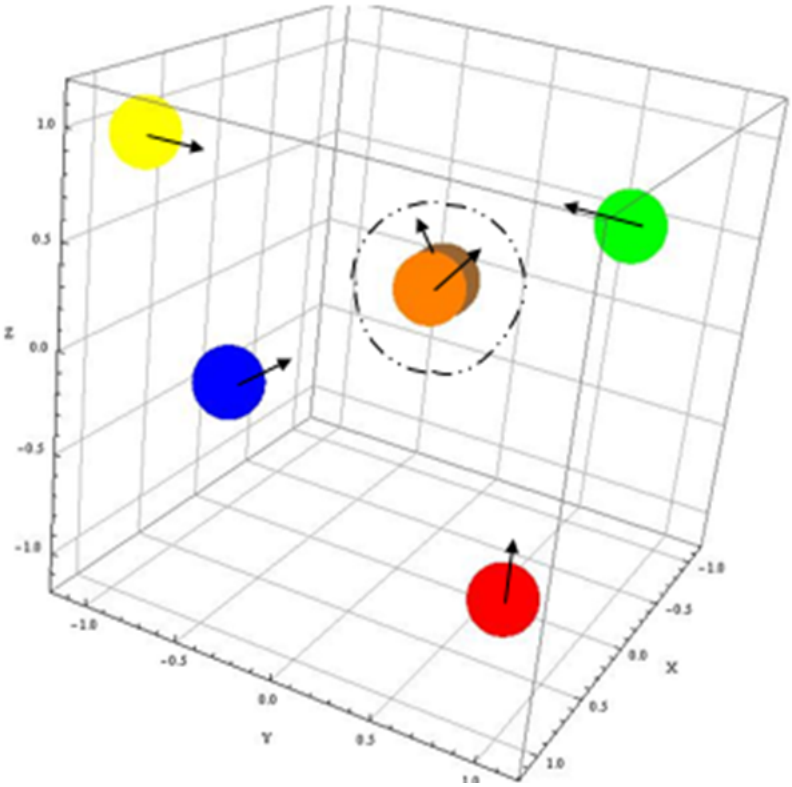

Рис. 2. Иллюстрация движения точечных объектов в трехмерной задаче об опасной близости (Fig. 2. Illustration of a movement of point objects in a three-dimensional problem on dangerous closeness)

Предположим далее, что при движении объектов и запросов нам необходимо обеспечить не только невозможность их столкновения, но и *обеспечить конфиденциальность местоположения объектов и запросов* при этом. Для этого может использоваться концепция *многосторонних конфиденциальных вычислений*, суть которых может сводиться к *следующей постановке задачи*. Имеется процесс интерактивного

взаимодействия (распределенный протокол взаимодействия) объектов и запросов между собой, для управления которым необходимо реализовать функциональность f,[1] с выполнением условий:

- *корректности,* когда f должна обеспечивать невозможность столкновения, даже если некоторая ограниченная часть объектов и запросов отклоняется от предписанных им действий;
- *конфиденциальности*, когда в результате взаимодействия ни один из объектов и запросов не получает никакой не предназначенной ему информации о других объектах и запросах.

Например, злоумышленник, контролирующий некоторую ограниченную часть объектов и запросов, получив такую информацию, предположим, координаты движения каких-либо объектов и запросов, может несанкционированно повлиять на процесс их взаимодействия с целью создания конфликтной ситуации (столкновения) с их участием.

2. Основные определения, модели, используемые протоколы

Основные определения, модели, используемые протоколы, формальная постановка задачи об опасной близости, в том числе и в конфиденциальном сценарии, а также основные подходы к доказательству безопасности протоколов (распределенных алгоритмов) ее решения приведены в работах [4 – 7]. Далее будут даны необходимые определения для решения задачи конфиденциального вычисления манхэттенского расстояния и конфиденциального вычисления пересечения двух окружностей. Будут также рассмотрены модели получестных и злонамеренных противников и сценарии их поведения при решении указанных задач.

Решение *задачи конфиденциального вычисления манхэттенского расстояния* можно описать в следующей постановке. Есть два участника, имеющие у себя конфиденциальные координаты (x_1,y_1) и (x_2,y_2). Обоим задано расстояние – ρ_m. Цель протокола, который далее будет обозначаться как протокол **ПВМР**, состоит в решении задачи, выполняется ли условие: $|\rho_m-|x_1-x_2||<|y_1-y_2|$, без раскрытия значений этих координат. Обозначается это следующим образом: b=**ПВМР**$((x_1,y_1),(x_2,y_2))$, где b=true, условие выполняется, b=false, в противном случае. В основе этого протокола лежит протокол Яо – протокол *конфиденциального вычисления функции сравнения двух чисел* [8].

Решение *задачи конфиденциального вычисления пересечения двух окружностей*, которая решается посредством двустороннего интерактивного протокола, было предложена в работе [9]. Протокол можно описать в следующей постановке. Есть два участника, имеющие у себя конфиденциальные координаты центров окружностей (x_1,y_1) и (x_2,y_2). Обоим задан радиус этих окружностей – ρ_o.[2] Цель протокола, который далее будет обозначаться как протокол **ПП2О**, состоит в решении задачи, имеют ли окружности с этими координатами их центров пересечение, без раскрытия значений этих координат. Обозначается далее это следующим образом: b=**ПП2О**$((x_1,y_1),(x_2,y_2))$, где b=true, окружности с этими центрами пересекаются, b=false, в противном случае. В основе этого протокола лежит протокол Ду - Аталлаха – *протокол конфиденциального вычисления скалярного произведения 2-х векторов* [10].

В *модели получестного противника* (*Semi - Honest Adversary*) противник контролирует некоторых участников протокола и далее участники точно следуют транскрипции протокола, за некоторым исключением, – получестные участники протокола могут записывать и сохранять информацию на всех промежуточных этапах вычислений и попытаться что-либо узнать о конфиденциальном входе «контрагента» из нее (хотя в случае честного поведения они должны стирать такую информацию).

[1] Функциональность, обеспечивающая невозможность столкновения.

[2] В оригинальной работе [9] – для каждой из окружностей задан свой радиус ρ_1 и ρ_2.

В модели *злонамеренного противника* (*Malicious Adversary*) противник контролирует некоторых участников протокола, которые независимым образом отклоняются от предписанных инструкций протокола.

В случае успешной стратегии получестного противника, который получил контроль над одним или несколькими[3] из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) взаимодействия, нарушив таким образом правила обеспечения конфиденциальности местоположения объектов и запросов (если они установлены). В случае успешной стратегии злонамеренного противника, который получил контроль над одним или несколькими из объектов и запросов, противник раскроет координаты движения честного(-ых) участника(-ов) и таким образом повлияет на скорость движения подконтрольного(-ых) ему объектов и запросов с тем, чтобы создать опасную близость (столкновение).

Протоколы конфиденциальных вычислений должны противостоять и первому, и второму типу противников, в том числе и при многостороннем взаимодействии с большим количеством участников движения и его интенсивностью и с установленным порогом на количество участников движения, находящихся под контролем противника.

3. Протоколы конфиденциального предотвращения столкновения КПС

3.1 Описание двустороннего протокола **КПС**

Протокол π далее именуется *протоколом конфиденциального предотвращения столкновения* и обозначается **КПС**, а по сложившейся в современной криптографии традиции участники протоколов в двухстороннем сценарии именуются **А** (Алисой) и **В** (Бобом).

В протоколе **КПС** необходимо определить, существует ли момент времени t, удовлетворяющий b=**ПП2О**$((x_1,y_1),(x_2,y_2))$ или b=**ПВМР**$((x_1,y_1),(x_2,y_2))$, где b=true, без раскрытия Бобу координаты $(x_{\mathbf{A}},y_{\mathbf{A}})$ и, соответственно, Алисе координаты $(x_{\mathbf{B}},y_{\mathbf{B}})$.

Протокол **КПС**

Конфиденциальный вход Алисы: $(x_{\mathbf{A}},y_{\mathbf{A}})$; *конфиденциальный вход Боба*: $(x_{\mathbf{B}},y_{\mathbf{B}})$.

Следующие шаги выполняются l раз, где шаг устанавливается каким-либо очевидным образом между моментом появления **А** на границе зоны (на границе прямоугольника) и моментом пересечения траектории движения **В** плюс один шаг.

1. Алиса и Боб выполняют протокол **ПП2О** (или протокол **ПВМР**) со своими входами $(x_{\mathbf{A}},y_{\mathbf{A}})$ и $(x_{\mathbf{B}},y_{\mathbf{B}})$ соответственно.[4]

2. Как только выходом протокола **ПП2О** (или протокол **ПВМР**) становится значение «true», то существует момент времени t, при котором возможно столкновение.

3. Если такой момент t существует, то присвоить b:=true, в противном случае b:=false.

Выход протокола. Если b=true, выдать «команду на понижение скорости» Алисе, если b=false, в противном случае.

3.2 Решение задачи об опасной близости для многих участников

Пусть множество J состоит из пронумерованных объектов, находящихся в опасной близости: $J(\rho,q,V)=\{o_i\in V \mid \exists\, t:\ \text{true}=\mathbf{ПП2О}((x_i,y_i),(x_j,y_j)),\ i,j=1,2,...\}$.. *Библиотека* V является множеством объектов, находящихся в текущий момент времени t внутри рассматриваемого прямоугольника. Тройку (ρ,q,V) будем называть *задачей об опасной близости для многих участников.*

Алгоритмом А решения задачи об опасной близости будем называть совокупность процедур поиска, вставки и удаления в множестве *J. Вставка* объекта o в множество J является такое его преобразование, при котором библиотека V преобразуется в $V\cup\{o\}$

[3] Числом не более заданного порога.

[4] Если x и y представлены географическими координатами, то $0<x<360$ и $0<y<180$ (с точностью до 1 градуса) или $0<x<3600000$ и $0<y<1800000$ (с точностью до 1 секунды).

и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V). А *удаление* объекта o из множества J является такое его преобразование, при котором библиотека V преобразуется в $V\backslash\{o\}$ и алгоритм A при этом решает задачу *поиска* для задачи (ρ,q,V).

Формулировку задачи об опасной близости в терминах информационных графов, можно найти в [1], где информационный граф рассматривается как модель данных с возможностью поиска, вставки и удаления в нем. В этой же работе предлагаются алгоритмы решения задачи об опасной близости путем ее сведения к задаче одномерного интервального поиска и доказываются утверждения о существовании таких алгоритмов с *логарифмической сложностью операций поиска, вставки и удаления*.

Таким образом, решение задачи об опасной близости для многих объектов сводится к реализации операций поиска, вставки и удаления над множеством J с библиотекой V (решению задачи одномерного интервального поиска в информационном графе), а конфиденциальность координат этих объектов по-прежнему можно обеспечить использованием протокола **КПС**.

3.3 Решение задачи об опасной близости для разных измерений

Цель протокола для решения задачи об опасной близости на прямой состоит в решении задачи, выполняется ли условие: $|x_1-x_2|<\rho_m$, не раскрывая значения координат. В этом случае такая задача может ставиться в двухмерном пространстве, если на плоскости объекты движутся строго вдоль одной из осей.

В случае трехмерного пространства ставится задача, выполняется ли условие: $|x_1-x_2|+|y_1-y_2|+|z_1-z_2|<\rho_m$, не раскрывая значения координат. Здесь также можно свести эту задачу к одномерному или двумерному случаю, если предположить, что объекты движутся строго в одной плоскости и вдоль двух или одной осей соответственно (для двумерного случая – см. рис. 3).

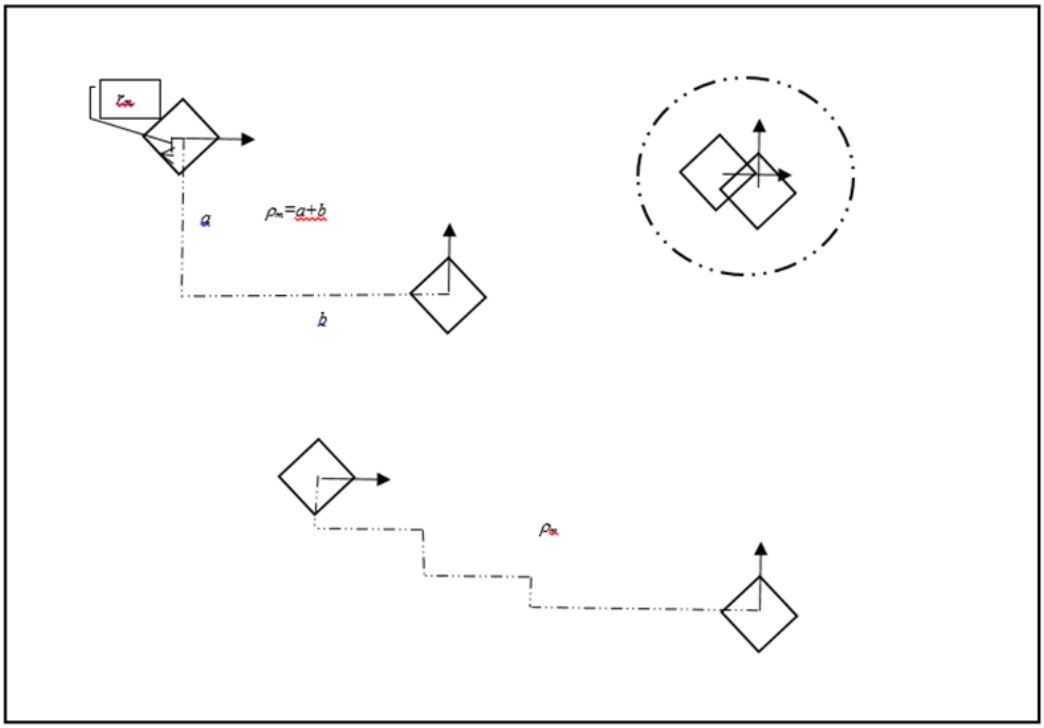

Рис. 3. Иллюстрация вычислений расстояний ρ_m для объектов с радиусом по Манхэттену r_m
(Fig. 3. Illustration of computation of distances ρ_m for objects with a Manhattan radius r_m)

Протокол **КПС** позволяет решать эти задачи, а протокол **ПП2О**, в случае существования его расширения на 3-мерный случай (на поверхность шара, на сферу), также позволит решать задачу об опасной близости «не через» вычисления манхэттенского расстояния для поверхности куба.

4. Варианты поведения злонамеренного противника в задаче об опасной близости

Обобщенное описание модели злонамеренного противника в конфиденциальных вычислениях может быть следующим [11, 12]. Рассматривается сеть взаимодействующих участников вычислений. Некоторые из них могут в некоторый момент времени приостановить отправку своих сообщений. В то же время предполагается, что они продолжают получать сообщения и могут выдавать «некую информацию» в свои выходные каналы. В другом варианте злонамеренного поведения нечестные участники могут произвольным образом сотрудничать друг с другом с целью получения необходимой для них информации или с целью нарушения процессов вычислений и взаимодействия. Они также могут «объединять» свои входы и изменять их.

Противники могут быть *статическими* и *динамическими*. *Статическим противником* является противник, который «сотрудничает» с фиксированным количеством нечестных участников («подкупленных» противником). При действиях *динамического противника* количество нечестных участников может меняться (в том числе непредсказуемым образом). Множество статических нечестных участников фиксировано в начале и процессе вычислений, множество динамических нечестных участников может меняться, как может меняться и характер их поведения.

Кроме того, противник может быть *пассивным* и *активным*, а также с *априорными* и *апостериорными* протокольными и раундовыми действиями. Пассивный противник не может изменять сообщения, циркулируемые в сети. Активный противник может знать все о внутренней конфигурации сети, может читать и изменять все сообщения нечестных участников и может выбирать сообщения, которые будут посылать нечестные участники при вычислениях. Активный динамический противник может в начале каждого раунда «подкупить» несколько новых участников. Таким образом, он может изучить информацию, получаемую ими в текущем раунде, и принять решение «подкупить» ли ему нового участника или нет. Такой противник может собирать и изменять все сообщения от нечестных участников к честным. Действия аналогичного характера активный противник может выполнить не только в течение раунда (в его начале и конце), но и до начала выполнения протокола и после его завершения. Противник называется *t-противником*, если он сотрудничает с t нечестными участниками.

В данной работе исследуются *следующие сценарии поведения злонамеренного противника* в задаче об опасной близости. Участники движения, контролируемые противником, могут:

- отказаться участвовать в протоколе, когда он инициируется, или преждевременно его прервать;
- отклоняться от инструкций протокола;
- изменять свои координаты или участвовать в протоколе с координатами других участников;
- пытаться раскрыть конфиденциальные координаты честных участников.

В конце концов, задача злонамеренного противника заключается в создании опасной ситуации посредством столкновения при движении участников взаимодействия.

Предположительно, используя представленные здесь протоколы для модели получестного противника, можно создавать протоколы, решающие задачи противодействия злонамеренному t-противнику и для случая с двумя участниками, и для случая со многими участниками. В случае обнаружения точечных объектов, подконтрольных последнему, они также заносятся в множество J для библиотеки V, даже, если не находятся в опасной близости.

В работах [13 – 15], например, приведены протоколы, – аналоги протокола Яо, в которых одна из сторон нарушает корректность протокола, отклоняясь некоторым образом от правильных его инструкций, а другая сторона обнаруживает это с высокой вероятностью. При этом доказательство безопасности таких вычислений может строиться через доказательство (вычислительной) неразличимости вычислений в идеальной модели

(в модели с полностью доверенной дополнительной стороной) и реальной модели вычислений [11, 12].

5. Математический и физический миры

Рассматриваемые выше модели конфиденциальных вычислений описывают идеализированную («математическую») ситуацию в задаче об опасной близости. В физическом, реальном мире естественно все намного сложнее. Вот только несколько вопросов, на которые приходится отвечать в случае, если точечные объекты – это беспилотные автомобили в будущей системе автопилотирования:

- как обеспечить конфиденциальность координат беспилотного автомобиля, если сам автомобиль, скорее всего, будет иметь государственный номер, а следовательно, можно однозначно идентифицировать его владельца;
- как обеспечить эту конфиденциальность, если в локальной зоне управления большинства городов есть система видеонаблюдения[5] (даже цвет и марка автомобиля, могут также дать существенную информацию об автомобиле)[6];
- в случае использования в качестве основного криптографического примитива схем шифрования с открытым ключом [7], как реализовать оперативную «онлайн» инфраструктуру открытых ключей в локальной зоне управления движением;
- насколько значение предиката b=**ПВМР**$((x_1,y_1),(x_2,y_2))$ является существенным знанием для злоумышленников, говорящим о нахождении участников движения на расстоянии друг от друга, менее чем ρ_m, и позволяющим создать опасную ситуацию на дороге;
- существуют ли другие (некриптографические) методы решения исследуемой задачи, например, введение цифровых псевдонимов для участников или значительное намеренное огрубление результатов измерений координат местоположения или что-то подобное) и др.

Ответы на эти и другие подобного рода вопросы, на взгляд автора, являются безусловно интересными и заслуживающими пристального внимания специалистов в области информационной безопасности, связи, транспорта, распределенных систем.

Заключение

Представленные здесь соображения по решению задачи сокрытия координат участников взаимодействия позволяют «двигаться» в направлении создания практических протоколов для многосторонних конфиденциальных вычислений в модели со злонамеренным противником[7] для двух- и трехмерного пространства (то есть, с обеспечением конфиденциальности 2-х и 3-х географических координат точечных объектов.

При «перемещении» предлагаемых решений в реальный физический мир, скорее всего, появится множество проблем, связанных с практической реализацией протоколов конфиденциальных вычислений для (пока) гипотетических информационных систем подобного типа[8], которые наверняка возникнут вместе с конкретной моделью противника,

[5] Таким образом, противник, «подкупив», например, Боба и «взломав» систему видеонаблюдения, может получать конфиденциальные входы Алисы, а следовательно, может попытаться получить секретный ключ используемой схемы гомоморфного шифрования [7] и делать дальше «все, что ему вздумается». Или без «вскрытия» протокола **КПС** Боб может создать опасную ситуацию для Алисы, имея в своем распоряжении ее конфиденциальные входы, полученные от «взломанной» системы видеонаблюдения и т.д. и т.п.

[6] В этом смысле интересна система автопилотируемых летательных аппаратов (дронов), которые уже сейчас трудно поддаются визуальной идентификации.

[7] Тем более что теоретические результаты в области конфиденциальных вычислений предполагают (при некоторых условиях) возможность построения компиляторов, которые преобразуют любые протоколы для модели с получестным противником в эквивалентные протоколы для двух моделей со злонамеренным противником. См. аргументацию в [12, § 3.6].

[8] Подобные системы все чаще называются киберфизическими.

конкретной технической реализацией протоколов в конкретной информационной системе и конкретной физической среде.

СПИСОК ЛИТЕРАТУРЫ:

1. Скиба Е. А. Логарифмическое решение задачи об опасной близости // Интеллектуальные системы. 2007. 11: 1 – 4. С. 693 – 719.
2. Снегова Е. А. Критерий сводимости задачи об опасной близости к одномерному интервальному поиску // Дискретная математика. 2011. Т. 23. Вып. 5. С. 138 – 159.
3. Снегова Е. А. Сложность задачи о предотвращении столкновении // Автореферат диссертации на соискание ученой степени кандидата физико-математических наук. МГУ имени М.В. Ломоносова, 2012. URL: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (дата обращения: 20.06.2018).
4. Казарин О. В. Практически реализуемые системы многосторонних конфиденциальных вычислений // Защита информации. INSIDE. 2016. № 3. С. 36 – 42.
5. Казарин О.В. О возможности сокрытия местоположения абонента сотовой связи с использованием методов конфиденциальных вычислений // Вопросы защиты информации. 2016. № 1. С. 39 – 47.
6. Казарин, Олег. Конфиденциальные вычисления в задаче об опасной близости. Безопасность информационных технологий, [S.l.], v. 24, n. 1, p. 39-48, apr. 2017. ISSN 2074-7136. Доступно на: . Дата доступа: 04 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.1.05.
7. Казарин О.В. Многосторонние конфиденциальные вычисления в задаче об предупреждении столкновений // Вестник компьютерных и информационных технологий. 2017. № 6. С. 50 – 56.
8. Yao A.C. Protocols for secure computations (extended abstract) // Proc. of 23-rd IEEE Symp. on Foundations of Computer Science. 1982. P. 160 – 164.
9. Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles // Journal of Information & Computational Science. 2011. № 8. P. 29 – 40.
10. Du W., Attalach M. J. Privacy-preserving cooperative scientific computations // Proceeding of the 2002 Workshop on New Security Paradigms – NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press. P. 127 – 135.
11. Казарин О.В. Теория и практика защиты программ. Доступно на: <http://ru.b-ok.org/book/629866/b75031>. Дата доступа: 19 october 2018.
12. Казарин О. В. Методология защиты программного обеспечения. – М.: МЦНМО, 2009. – 464 с.
13. Kreuter B., Shelat A., Shen C. Billion-gate secure computation with malicious adversaries// Proceedings of USENIX Security'12. 2012. P. 285 – 301.
14. Lindell Y., Pinkas B. An efficient protocol for secure two-party computation in the presence of malicious adversaries // Proceedings of the 26-th Annual International Conference on Advances in Cryptology – EUROCRYPT'07. 2007. P. 52 – 78.
15. Mohassel P., Franklin M. Efficiency tradeoffs for malicious two-party computation // Proceedings of Public Key Cryptography-PKC'06. 2006. P. 458 – 473.

REFERENCES:

[1] Skiba E.A. Logarithmic solution of the problem on dangerous closeness. Intellektual'nye sistemy, 2007, Vol. 11: 1–4. pp. 693–719. (in Russian).
[2] Snegova E.A. A criterion of reduction of the problem on dangerous closeness to the one-dimensional interval search. Diskretnaya matematika, 2011, Vol. 23, no. 5, pp. 138 – 159. (in Russian).
[3] Snegova E.A. Complexity of the problem on dangerous closeness. PhD thesis. Moscow: Izdatel'stvo MGU im. M. V. Lomonosova, 2012. Available at: http://mech.math.msu.su/~snark/files/vak/arzg0.pdf (accessed: 20.06.2018). (in Russian).
[4] Kazarin O.V. Real-life systems of multy-party secure computation. Zashhita informatsii. INSIDE, 2016, no 3, pp. 36 – 42. (in Russian).
[5] Kazarin O.V. On the possibility of hiding the geolocation of a subscriber of a cellular network using methods of secure computation. Voprosy zashhity informatsii, 2016, no 1, pp. 39 – 47. (in Russian).
[6] Kazarin, Oleg. Institute of Information Security Issues, Lomonosov MSU. IT Security (Russia), [S.l.], v. 24, n. 1, p. 39-48, apr. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/54>. Date accessed: 04 july 2018. doi:http://dx.doi.org/10.26583/bit.2017.1.05.
[7] Kazarin O.V. Multi-party secure computation in the problem of collisions prevention. Vestnik komp'yuternyh i informacionnyh tekhnologij. 2017. no 6. pp. 50 – 56. (in Russian).
[8] Yao A.C. Protocols for secure computations (extended abstract). Proc. of 23-rd IEEE Symp. on Foundations of Computer Science. 1982. P. 160 – 164.
[9] Yang B., Sun A., Zhang W. Secure two-party protocols on planar circles. Journal of Information & Computational Science. 2011. № 8. P. 29 – 40.

[10] Du W., Attalach M. J. Privacy-preserving cooperative scientific computations. Proceeding of the 2002 Workshop on New Security Paradigms – NSPW'2002, Virginia Beach, VA, 23–26 September 2002, New York, NY, ACM Press. P. 127 – 135.
[11] Kazarin O.V. Theory and practice of software protection. Доступно на: <http://ru.b-ok.org/book/629866/b75031>. Дата доступа: 19 october 2018. (in Russian).
[12] Kazarin O.V. Methodology of software protection. – M.: MTSNMO, 2009. – 464 p. (in Russian).
[13] Kreuter B., Shelat A., Shen C. Billion-gate secure computation with malicious adversaries. Proceedings of USENIX Security'12. 2012. P. 285 – 301.
[14] Lindell Y., Pinkas B. An efficient protocol for secure two-party computation in the presence of malicious adversaries. Proceedings of the 26-th Annual International Conference on Advances in Cryptology – EUROCRYPT'07. 2007. P. 52 – 78.
[15] Mohassel P., Franklin M. Efficiency tradeoffs for malicious two-party computation. Proceedings of Public Key Cryptography-PKC'06. 2006. P. 458 – 473.

Поступила в редакцию - 04 июля 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – July 04, 2018. The final version – November 01, 2018.