УДК 535.8, 004.8, 681.5, 681.7

ВЕРИФИКАЦИЯ АГЕНТОВ С ПОМОЩЬЮ ПРОЦЕДУР ДИСКРЕТНОЙ МНОГОЗНАЧНОЙ ЛОГИКИ

А.Ю. Быковский
Физический институт им. П.Н.Лебедева РАН
Россия, 119991, Москва, Ленинский пр., 53
E-mail: bykovskiyay@lebedev.ru

Ключевые слова: дискретная многозначная логика, верификация, модель доверия агентов, идентичность и аутентичность агента.

Аннотация: Дискретная k-значная алгебра Аллена-Живона является удобным средством верификации идентичности и аутентичности автономных агентов, использующих одноразовые случайные ключи, формируемые с помощью устройств квантовой оптики. Представлен ряд процедур и алгоритмов для построения связанных списков логических данных в распределенном сетевом реестре, предложены схемы многоступенчатой взаимной верификации агентов, а также схемы селективной фрагментации и интеграции верифицирующих данных. Дискретный многозначно-логический аналог нечеткого контроллера предназначен для управления схемами верификации маршрута агента, а параметрические T- нормы/T*-конормы могут быть использованы для построения квантового канала конфиденциального управления.

1. Введение

Рост пропускной способности оптических коммуникационных сетей на базе ВОЛС и атмосферных линий [1] в сочетании с современными радиочастотными средствами связи открывает новые возможности для автономных агентов в задачах беспилотного транспорта, логистики, Интернета вещей, производства и медицинского сервиса [2]. При этом квантово-оптические линии распределения ключа [3] лишь ограниченно пригодны для защиты информации в автономных мобильных роботах ввиду возможности постановки шумовых помех и блокировки атмосферных линий вне доверенных объектов. Но при этом многоступенчатые процедуры верификации идентичности и аутентичности агентов могут быть построены с помощью случайных одноразовых ключей, заранее формируемых устройствами квантовой оптики [3]. Это позволяет продвинуться в решении ряда задач позиционно-зависимой криптографии, проверки целостности данных, а также выполнения совместных вычислений без раскрытия данных. Кроме того, интересные разработки были сделаны в сфере применения блокчейна и моделей доверия стационарных агентов для выявления недобросовестных пользователей энергосетей [4]. Но как показывает анализ задач контроля следования агента по маршруту и позиционно-зависимой криптографии [5], кроме блокчейна необходимы более сложные процедуры верификации, выполняемые в широких диапазонах временных и пространственных параметров.

Цель работы – показать новые возможности многозначно-логических моделей для моделирования задач верификации идентичности и аутентичности мобильных агентов с помощью одноразовых случайных ключей.

2. Специфика многозначной алгебры Аллена-Живона

Для многопараметрического моделирования используется дискретная k-значная алгебра Аллена-Живона (ААЖ) [6], где n входных $x_1, \dots, x_n$ и выходная переменная y заданы на множестве $N = \{0,1, \dots, k-1\}$, 0 – абсолютно ложное, а $k-1$ – абсолютно истинное значение. Произвольную функцию $y = f(x_1, \dots, x_n)$ задают с помощью полного множества операторов

(1) $< 0,\ 1, \dots,\ k-1,\ X(a,b),\ *,\ +>$,

состоящего из констант $0, 1, \dots, k-1$, бинарного оператора Min(x_i, x_j), обозначаемого $\star$, бинарного оператора Max(x_i, x_j), записываемого как +, а также унарного оператора Литерал $X(a,b)$, задаваемого выр. (2):

(2) $$X(a,b) = \begin{cases} 0, \text{если } b < x < a \\ k-1, \text{если } a \le x \le b \end{cases},$$

где $b \ge a$, и $a, b \in N = \{0,1, \dots, k-1\}$.

В отличие от булевой логики, таблица истинности функции в ААЖ [x] содержит k^{k^n} строк и позволяет резко поднять размерности модельного пространства [x]. Пример записи логического выражения в ААЖ приведен в разд. 3. На практике функции ААЖ удобнее записывать в виде матриц констант и индексированных параметров (a,b).

Специфика ААЖ заключается в необходимость определять арифметические операции (+/ -, $\cdot/\div$) как отдельные логические функции, которые удобнее выполнять обособленно, в рамках гетерогенной логической архитектуры агента [7]. В этой схеме ААЖ используется в основном для управления структурой традиционных булевых и нечетких вычислений. Также в ААЖ удобно использовать коррелированные (т.е. взаимно-зависимые) переменные [8] для описания больших диапазонов значений пространственно-временных переменных, где, например, пространственную координату представляют $x = x^{(1)} \times 1 + x^{(2)} \times 10 + \cdots x^{(p)} \times 10^p$, а обратный переход к физической переменной требует суммирования.

3. Схемы верификации и построение связных списков

Многоступенчатая сетевая верификация агентов [8-10] обсуждается для двух типичных случаев, представленных на рис. 1.

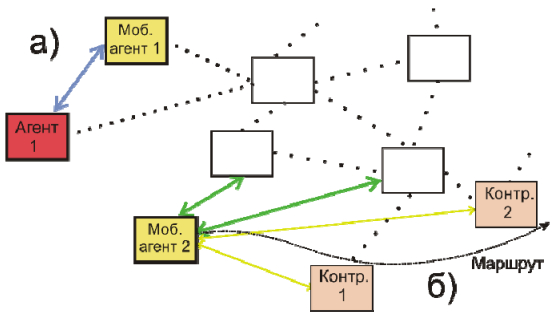

Рис. 1. Схемы взаимодействия агентов при сетевой верификации мобильного агента. В случае а) оба агента принадлежат к одной мультиагентной системе (МАС), при этом агент 1 удаленно проверяет идентичность/аутентичность мобильного агента 1 (показано голубой стрелкой). В схеме б) мобильный агент 2 при движении по маршруту обменивается данными как с контрольными точками 1, 2, … из той же МАС (желтые стрелки), так и со сторонними сетевыми узлами, привлеченными на договорной основе (зеленые стрелки).

Первый из них обозначен а) и рассматривает верификацию агентом 1 удаленного мобильного агента 1, относящегося к той же мультиагентной системе. Процесс их обмена данными показан синей стрелкой, а взаимная верификация сводится к комбинации нескольких процедур на базе ААЖ и использует схему случайного предсказателя [11]. Используются алгоритмы сравнения данных без их раскрытия [10], подтверждения данных значениями хэш функции случайного предсказателя [8, 9], а при необходимости – кодирование по схеме «одноразового шифроблокнота» [3]. Схема удаленного сравнения параметров двумя агентами без раскрытия данных [10] показана на рис. 2.

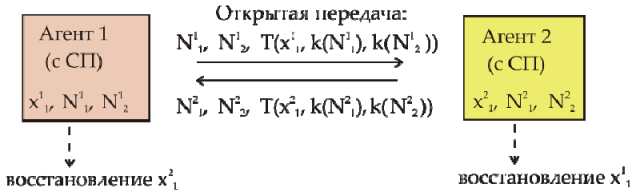

Рис. 2. Схема удаленного сравнения версий значения переменной x_1, имеющихся у агентов 1 и 2, осуществляемая по открытому каналу без раскрытия данных [10]. При этом агент 1 имеет версию $x_1^{(1)}$, агент 2 – версию $x_1^{(2)}$, а оба агента должны использовать случайный предсказатель (СП) [5, 11].

Вторая из типичных схем на рис. 1 обозначена б) и рассматривает движение мобильного агента 2 по заданному маршруту [8, 9]. Этот агент проводит взаимную верификацию с участием двух типов внешних устройств – с контрольными точками 1,2,… из той же МАС (желтые стрелки), а так же с сетевыми узлами с ограниченным уровнем доверия, привлекаемыми на основании взаимных или коммерческих услуг (зеленые стрелки). Сторонние узлы требуются здесь для реализации такого элемента блокчейна [12], как распределенный сетевой реестр логических данных, который формируется в сторонних узлах для защиты критических данных путем формирования копий связанных списков [8, 9]. В случае сбоев или конфликтов интересов версии критических и подтверждающих данных запрашивают из сетевых копий реестра, а корректность полученных сведений определяется мажоритарным значением. Логическое выражение связанного списка $h^{(m,s)} = F_{ldg}\left(m, t, \boldsymbol{e}_m, \boldsymbol{e}_{m-s}, \boldsymbol{h}_m, \boldsymbol{h}_{m-s}\right)$ формируют как функцию -значной логики, переменными которой являются номер записи m, последняя и предшествующая записи $\boldsymbol{e}_m$ и $\boldsymbol{e}_{m-s}$, t – время, $\boldsymbol{h}_m$ и $\boldsymbol{h}_{m-s}$ – случайно заданные хэши, присылаемыми внешними устройствами [8]. Последняя из сделанных записей записывается как терм произведения

(3) $$p.t._m = h_m^{(m,1)} \star X_m(m,m) \star X_t(t_m,t_m) \star$$
$$\star X_{e,1,m}\left(e_{1,m},e_{1,m}\right) \star \ldots \star X_{e,1,p}\left(e_{p,m},e_{p,m}\right) \star$$
$$\star X_{h,1,m}\left(h_{1,m},h_{1,m}\right) \star \ldots \star X_{h,Q,m}\left(h_{Q,m},h_{Q,m}\right) \star$$
$$\star X_{e,1,m-1}\left(e_{1,m-1},e_{1,m-1}\right) \star \ldots \star X_{e,p,m-1}\left(e_{p,m-1},e_{p,m-1}\right) \star$$
$$\star X_{h,1,p}\left(e_{1,m-1},e_{1,m-1}\right) \star \ldots \star X_{h,Q,m-1}\left(e_{Q,m-1},e_{Q,m-1}\right).$$

Усложненный вариант реестра [9]

$$h^{(out)} = F_{ll}(m,t,\ \boldsymbol{e}_m, \boldsymbol{e}_m^{(e)}, H_m^{(int)} h_{1,m}, \ldots, h_{Q,m},\ \boldsymbol{e}_{m-1}, \boldsymbol{e}_{m-1}^{(e)}, H_{m-1}^{(int)} h_{1,m-1}, \ldots, h_{Q,m-1})$$

помимо параметров внутренних подсистем агента $\boldsymbol{e}_m$ и их хэшей $H_m^{(int)}$ может содержать некоторые физические и технические параметры работы сторонних устройств $\boldsymbol{e}_m^{(e)}$ (номера аппаратных модулей, лицензии, местоположение, и.т.д.). В реестр можно включать данные модулей квантовых измерений [9]. В качестве ключей доступа к реестру используются случайно заданные значения хэширующих функций.

5. Модель доверия агента

Для имитации поведения человека используется модель доверия (или модель риска) агента, показанная на рис. 3. В ней успешность набора всех выполненных верификационных процедур первоначально оценивается логической функцией $F_{\text{ув}}$, выходной параметр которой описывает итоговый коэффициент успешности верификации. Этот сигнал далее вводится в дискретный аналог нечеткого контроллера [10], корректирующего работу агента с помощью небольшого набора жизненно-важных параметров (датчики исправности энергосистемы и линий связи, параметры обнаружения физических угроз, коэффициент успешности верификации).

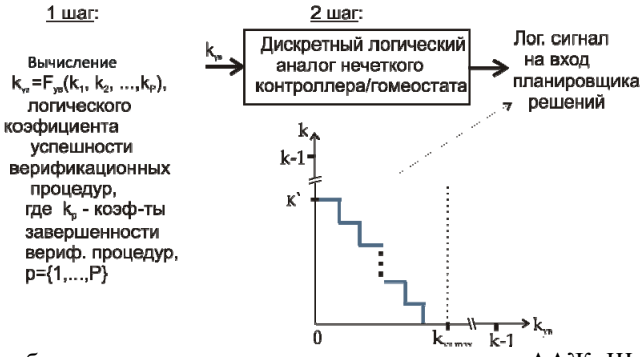

Рис. 3. Схема обработки параметров модели доверия агента в ААЖ. Шаг 1 – вычислить логическое значение коэффициента успешности задействованных верификационных процедур. Шаг 2 – ввести результат шага 1 в дискретный аналог нечеткого контроллера [10]. Ступенчатая кривая задает выходной сигнал коррекции верифицирующего контроллера.

Такой дискретный аналог нечеткого контроллера [10] приближенно имитирует работу контура поддержания гомеостаза в живом организме, используя для простоты небольшое число уровней истинности (~10). Если вместо операторов MIN/MAX в контуре нечеткого управления использовать Т-нормы и Т*-конормы [10], то можно дополнительно реализовать квантовый канал для скрытного переключения кубитами.

Верифицирующий модуль агента желательно выполнить в виде обособленного защищенного контроллера, целостность сопряженных с ним подсистем агента также следует верифицировать, а массив случайных ключей в нем следует регулярно пополнять от доверенного устройства. Для реализации простых версий обсуждаемого контроллера можно использовать специальную двух-чиповую микроконтроллерную плату с ОЗУ, ПЗУ [8,9] и соответствующими микроассемблерными программами.

5. Заключение

Методы дискретной k −значной алгебры Аллена-Живона в сочетании с квантово-оптическими схемами генерации массивов случайных одноразовых ключей предоставляют новые возможности для построения схем взаимной верификации аутентичности и целостности данных в автономных агентах. Такие процедуры могут использовать как взаимодействие агентов между собой, так и с лояльными сетевыми узлами. Принцип блокчейна используется для построения связанных списков распределенного логического реестра критических данных, коллективно формируемого внешними сетевыми узлами. Записи реестра комбинируют критические данные,

случайные значения хэширующих функций и документируемые параметры внутренних подсистем агентов. Для многоступенчатого подтверждения подлинности рассмотрена схема обмена верифицирующими данными без раскрытия этих данных. Модель доверия включает логическую функцию, оценивающую успешность всех верификационных процедур, и дискретный аналог нечеткого контроллера, вычисляющий корректирующие сигналы. Обсуждаются микроконтроллерная платформа и микроассемблерные программы, необходимые для реализации указанных процедур в рамках ААЖ. Предложен вариант построения квантового канала управления для дискретного аналога нечеткого контроллера.

Список литературы

1. Chi N., Zhou Y., Wei Y., Hu F. Visible Light Communication in 6G: Advances, Challenges, and Prospects // IEEE Veh. Technol. Mag. 2020. Vol. 15, No. 4. P. 93-102.
2. Sharma S., Kaushik B. A survey on internet of vehicles: Applications, security issues & solutions // Veh. Commun. 2019. Vol. 20. P. 100182.
3. Bykovsky A.Y., Kompanets I.N. Quantum cryptography and combined schemes of quantum cryptography communication networks // Quantum Electron. 2018. Vol. 48. P. 777–801.
4. Zhuang P., Zamir T., Liang H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. // IEEE Trans. Ind. Inform. 2020. Vol. II-17. P. 3-19.
5. Bykovsky A.Yu. Multiple-Valued Logic for The Implementation of Random Oracle and Position-Based Cryptography // J. Russ. Laser Res. 2019. Vol. 40. P. 173-183.
6. Allen C.M., Givone D.D. The Allen-Givone Implementation Oriented Algebra. In Computer Science and Multiple-Valued Logic: Theory and Applications; Rine, D.C., Ed.; Amsterdam, The Netherlands: North Holland, 1984. P. 262-283.
7. Bykovsky A.Yu. Heterogeneous network architecture for integration of AI and quantum optics by means of multiple-valued logic // Quantum Rep. 2020. Vol. 2. P. 126-165.
8. Bykovsky A.Yu. Multiple-Valued Logic Modelling for Agents Controlled via Optical Networks. // *Appl. Sci.* 2022. Vol. 12, No. 3. P. 1263. https://doi.org/10.3390/app12031263.
9. Bykovsky A.Yu., Vasiliev N.A. Data verification in the agent, combining blockchain and quantum keys by means of multiple-valued logic // Appl. Syst. Innov.., 2023. Vol. 6, No. 2. P. 51. https://doi.org/10.3390/asi6020051.
10. Bykovsky A.Yu., Vasiliev N.A. Parametrical T-gate for joint procession of quantum and classic optoelectronic signals // J. Multidis. Sci. J. 2023. Vol. 6, No. 3. P. 384-410. https://doi.org/10.3390/j6030026.
11. Boneh D., Dagdelen M., Fischlin M., Lehmann A., Schaffner C., Zhandry M. Random oracles in a quantum world; Advances in Cryptology // Proc. of the 17th Int. Conf. on the Theory and Appl. of Cryptology and Inf. Security, Seoul, Korea, 4-8 December, 2011. P. 41-69.
12. Singh J., Sinha A., Goli P., Subramanian V., Shukla S.K., Vyas O.P. Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology. // Int. J. Inf. Secur. 2021. P. 1-20.