НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2016 Том 16 № 6 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2016 Vol. 16 No 6 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.056.53

ДИНАМИЧЕСКАЯ АВТОРИЗАЦИЯ НА ОСНОВЕ ИСТОРИИ НОВОСТНЫХ СООБЩЕНИЙ

М.В. Баклановский[a], А.Р. Ханов[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: awengar@gmail.com

Информация о статье
Поступила в редакцию 13.04.16, принята к печати 07.10.16
doi: 10.17586/2226-1494-2016-16-6-1091-1095
Язык статьи – русский

Ссылка для цитирования: Баклановский М.В., Ханов А.Р. Динамическая авторизация на основе истории новостных сообщений // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 6. С. 1091–1095. doi: 10.17586/2226-1494-2016-16-6-1091-1095

Аннотация

Предлагается новая парадигма в области систем контроля доступа с нечеткой авторизацией. Пусть имеется множество объектов, которые находятся в единой сети передачи данных. Решается задача создания протокола динамической авторизации на основе того, насколько точно объект способен описать историю событий (новостей), произошедших в сети ранее. Предложен математический аппарат, позволяющий компактно хранить историю, забывать часть наиболее давних и наименее значимых событий, составлять и проверять данные, необходимые для авторизации объекта в сети. Для этого история новостных сообщений, каждое из которых представляет собой число, разбивается на вектора. Каждый из векторов умножается на некоторое количество стохастических векторов. Известен результат, что если вектора являются разреженными, то путем решения задачи $\boldsymbol{l_1}$-оптимизации они могут быть восстановлены с высокой точностью. Приведены результаты экспериментов по восстановлению векторов, которые показали, что с увеличением числа стохастических векторов увеличивается точность восстановления. Установлено, что первыми восстанавливаются наибольшие по модулю компоненты. Система контроля доступа с предложенной системой динамической авторизации позволит вычислять нечеткие оценки доверия в системах с постоянно меняющимся составом участников, каждый из которых представляет собой маломощный вычислитель.

Ключевые слова

динамическая авторизация, рандомизированные алгоритмы, системы контроля доступа, мультиагентные системы, интернет вещей

Благодарности

Авторы выражают благодарность профессору О.Н. Граничину за консультации по рандомизированным алгоритмам.

DYNAMIC AUTHORIZATION BASED ON THE HISTORY OF EVENTS

M.V. Baklanovsky[a], A.R. Khanov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: awengar@gmail.com

Article info
Received 13.04.16, accepted 07.10.16
doi: 10.17586/2226-1494-2016-16-6-1091-1095
Article in Russian

For citation: Baklanovsky M.V., Khanov A.R. Dynamic authorization based on the history of events. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 6, pp. 1091–1095. doi: 10.17586/2226-1494-2016-16-6-1091-1095

Abstract

The new paradigm in the field of access control systems with fuzzy authorization is proposed. Let there is a set of objects in a single data transmission network. The goal is to develop dynamic authorization protocol based on correctness of presentation of events (news) occurred earlier in the network. We propose mathematical method that keeps compactly the history of events, neglects more distant and least-significant events, composes and verifies authorization data. The history of events is represented as vectors of numbers. Each vector is multiplied by several stochastic vectors. The result is known that if vectors of events are sparse, then by solving the problem of $\boldsymbol{l_1}$-optimization they can be restored with high accuracy. Results of experiments for vectors restoring have shown that the greater the number of stochastic vectors is, the better accuracy of restored vectors is observed. It has been established that the largest absolute components are restored earlier. Access control

system with the proposed dynamic authorization method enables to compute fuzzy confidence coefficients in networks with frequently changing set of participants, mesh-networks, multi-agent systems.

Keywords
dynamic authorization, randomized algorithms, access control systems, multi-agent systems, Internet of things

Acknowledgments
We enclose our gratitude for Prof. O.N. Granichin for consultations about randomized algorithms.

Введение

Системы контроля доступа используются для предотвращения несанкционированных действий пользователей по отношению к ресурсам. Дискреционная и мандатная модели являются традиционными решениями этой проблемы. В этих моделях права доступа к ресурсам напрямую привязываются к пользователям системы. С ростом числа пользователей и ресурсов управление правами становится существенно сложнее, и в этих случаях часто переходят на использование модели ролевого доступа (RBAC) [1]. В этой модели пользователь связывается с множеством ролей, каждой роли соответствуют права доступа к ресурсам. Роли должны быть сформированы заранее, однако не все права и роли необходимы на протяжении всего времени работы пользователя в системе. Более того, множество ролей или сами роли должны изменяться со временем в целях снижения рисков несанкционированной активности. Управление этими изменениями в некоторых случаях становится сложной проблемой, для решения которой была предложена модель доступа, основанная на доверии (TrustBAC) [2]. По определенному набору характеристик для пользователя вычисляется коэффициент доверия. В зависимости от него пользователю присваиваются роли и права. Однако роль, приписанная пользователю, не изменяется. В модели TBFAC [3] оценка доверия выставляется как статически, на основе данных, полученных при аутентификации пользователя, так и динамически, отдельно для каждого ресурса системы на основе характеристик пользователя. В работе была предложена реализация модели на основе нечеткой логики, однако не описаны конкретные данные, на основе которых происходит выставление коэффициентов доверия пользователям.

Модели нечеткой авторизации получили распространение в мультиагентных системах, например, в Mesh-сетях [4–6]. Mesh-сеть – это сеть маломощных устройств, каждое из которых является одновременно и маршрутизатором, и конечным хостом. В работе [7] в рамках протокола предложена система динамической авторизации на основе данных о качестве связи между узлами. При этом история учитывается в силу рекуррентности формул расчета. В работе [8] предложено оценивать доверие алгоритмом, в основе которого лежит нечеткая логика. Построение нечеткой системы оценки доверия также обсуждалось в работах [9–12].

В настоящей работе предложен метод динамической авторизации, в основе которого лежит информация об истории событий, произошедших в сети передачи данных.

Постановка задачи

Имеется множество объектов (узлов), находящихся в единой сети передачи данных. Каждый объект может взаимодействовать с любым другим узлом сети. Новость – это событие в сети. Таким событием может быть как передача пакета данных с полезной нагрузкой, так и служебный трафик с искусственно генерируемыми числами. Последовательность новостей с временными метками – история новостей. Эти данные быстро накапливаются и занимают большие объемы. Хранение таких огромных данных может потребовать существенных ресурсов. Вместо этого по данным вычисляются какие-либо характеристики. История – набор таких характеристик, построенных по последовательности событий. Наша задача – оценить доверие каждому объекту сети в зависимости от его способности описывать эту историю.

Новостной авторизацией назовем совокупность процедур прохождения аутентификации нового объекта и уточнения коэффициентов доверия к объектам, уже прошедшим аутентификацию ранее. При этом объект всегда предоставляет свой образ истории, а коэффициент доверия выставляется в зависимости от того, насколько точно образ соответствует реальной истории новостей.

Для реализации новостной авторизации необходимы следующие алгоритмы:

1. построения характеристик по истории событий;
2. генерации образа;
3. сравнения образа с историей;
4. забывания более ранних событий истории.

Оказывается, что в теории рандомизированного восстановления разреженных сигналов уже создан математический аппарат, позволяющий реализовать новостную авторизацию в условиях сильных ресурсных ограничений.

Новостная авторизация

Пусть имеется вектор $\mathbf{x} \in R^N$. Известно, что не более k компонент вектора являются ненулевыми. Вычислим скалярное произведение вектора на $m<<N$ стохастических векторов $\mathbf{A}_i$. Получим m чисел

$<\mathbf{A}_i,\mathbf{x}> = b_i$. В работах [13, 14] показано, что, зная лишь $\mathbf{A}_i$ и b_i, вектор $\mathbf{x}$ можно восстановить путем решения задачи l_1-оптимизации:

$$\|\mathbf{x}'\|_1 = \sum_j |\mathbf{x}'[j]| \to \min, b_i =< \mathbf{A}_i\mathbf{x} >, j = 1..N, i = 1..m.$$

Изменяя m, можно регулировать точность восстановления $\mathbf{x}$.

Пусть история – это последовательность чисел на шкале времени. Разобьем шкалу на интервалы длины N, если на этом интервале не более k событий, то он является k-редкой последовательностью. Сгенерируем m векторов $\mathbf{A}_i$ размерности N. Вычислим m скалярных произведений $<\mathbf{A}_i,\mathbf{I}> = b_i$, где $\mathbf{I}$ – интервал на временной шкале. Пары $(\mathbf{A}_i, b_i)$ являются описанием истории событий на $\mathbf{I}$. На рис. 1 приведена схема работы с историей новостных сообщений. Каждая точка на временной шкале – событие (число). На каждом интервале не более 5 событий, значит k=5. События каждого интервала хранятся в виде множества пар $H_l = \{(\mathbf{A}_i, b_i)\}$, i=1..m, которое является характеристикой l-го временного интервала.

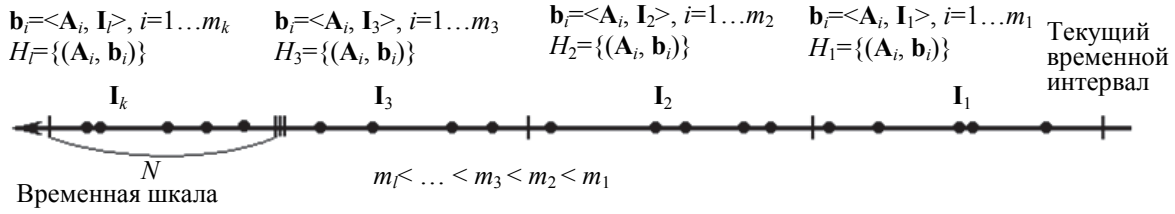

Рис. 1. Схема работы алгоритма новостной авторизации

С течением времени для забывания событий более давних интервалов произвольные пары из H_l удаляются. Каждый объект сети хранит свое множество пар H_l для каждого временного интервала, так как каждый из них по-своему забывает историю. Исходя из этого, любое подмножество объектов сети, которое содержит больше пар для некоторого интервала $\mathbf{I}_l$, обладает большим знанием о событиях этого интервала, чем подмножество объектов (или один объект), содержащее меньше пар. Образ истории – это конкретный набор H_l для объекта сети. Для того чтобы подмножеству узлов сети авторизовать новый объект (который на время покидал сеть), выбирается «встречающий» объект, который получает от остальных дополнительные знания об истории. Далее «встречающий» и вновь пришедший восстанавливают некоторый интервал $\mathbf{I}_l$ (или несколько интервалов). После этого «встречающий» задает вопросы о событиях в сети на интервале $\mathbf{I}_l$**.** В зависимости от количества верных ответов узлу будет выставлен коэффициент доверия.

Так как m<<|$\mathbf{I}_l$|, история хранится более компактно, чем если бы хранились целые вектора длины N. Если бы история хранилась как массив событий с временными метками, то «забывание» приводило бы к исчезновению событий из истории, в то время как удаление пар $(\boldsymbol{A}_i, b_i)$ приводит лишь к менее точному их восстановлению. Вектора $\boldsymbol{A}_i$ должны быть одинаковы на всех узлах. Для их хранения можно использовать детерминированный алгоритм генерации случайных чисел.

Эксперимент по восстановлению разреженного сигнала

Пусть мы имеем интервал истории длиной 200 тактов, на которых произошло ровно 20 событий. Каждое событие – число от 1 до 256. Какое количество стохастических векторов нужно, чтобы хранить такую историю?

Был проведен эксперимент по восстановлению разреженного сигнала $\mathbf{x} \in R^N$ длины N=200 с k=20 ненулевыми компонентами. Ненулевые позиции в векторе выбирались произвольно, в них находились произвольные числа от 1 до 256. На рис. 1 показан график зависимости ошибки восстановления $||\mathbf{x}–\mathbf{x}'||_1$ от m.

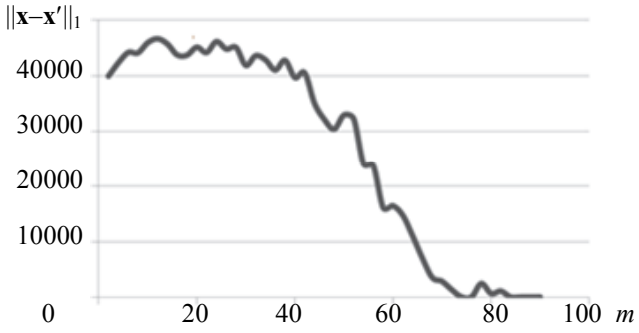

Рис. 2. Зависимость ошибки восстановления сигнала от m

По графику на рис. 2 видно, что при изменении m от 30 до 80 ошибка восстановления сигнала уменьшается постепенно. На рис. 2 изображены восстановленные вектора $\mathbf{x}'$ при различных значениях m. Для каждого m выбиралось по 15 наборов стохастических векторов $\boldsymbol{A}_i$, i=1..m.

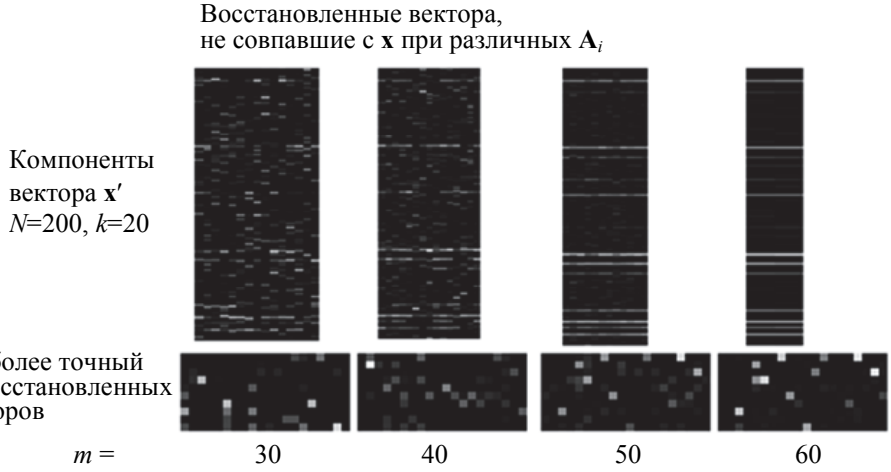

Рис. 3. Сверху – восстановленные вектора из 200 компонент. Снизу – наиболее неточный по l_1-метрике вектор в виде прямоугольника 10×20

По рис. 2 видно, что с увеличением m в первую очередь восстанавливаются наибольшие по модулю компоненты вектора $\mathbf{x}$.

Таким образом, историю длины 200 с не более чем 20 событиями могут хранить от 30 уравнений. Если уравнений более 80, то история восстанавливается точно. Для хранения данного интервала истории от 30 до 80 уравнений должны быть распределены между узлами. Каждое уравнение хранятся в виде пары (i,b_i), где i – номер стохастического вектора; b_i – скалярное произведение $\mathbf{A}_i$ на вектор сигнала $\mathbf{x}$. При восстановлении $\mathbf{x}$ «вспоминаются» в первую очередь наибольшие по модулю числа-события, именно они должны участвовать в процессе аутентификации вновь пришедшего объекта.

Заключение

В работе был опробован математический аппарат, позволяющий в будущем реализовать протокол динамической авторизации. В основе этого протокола будут лежать следующие операции:

1. построение характеристик истории новостных сообщений;
2. сохранение образа истории на узлах сети;
3. авторизация нового узла сети в зависимости от знания истории новостных сообщений;
4. забывание более ранних временных фреймов.

Преимущества данного подхода в том, что:

- в сети нет единого узла, отвечающего за авторизацию, «встречающий» выбирается динамически, а информация хранится сразу во всех узлах;
- генерация ключа происходит непрерывно и децентрализовано, ключом фактически является история новостных сообщений во всей сети.

Система нечеткого контроля доступа на основе новостных сообщений применима в мультиагентных системах при взаимодействии маломощных вычислителей. Такие системы состоят из взаимодействующих друг с другом устройств, их состав может периодически меняться. На практике такие сети являются основой «интернета вещей», «умного» дома, динамическая авторизация позволяет решить проблемы с безопасностью, возникающие при построении таких систем.

Новостная авторизация позволит строить системы компьютерной безопасности по-новому, на основе нечетких критериев и оценок, подстраивать их под изменяющиеся внешние условия и настраивать отдельно для каждого случая их применения. Например, в системе подавления вредоносных программ CODA [15] в качестве естественных новостных сообщений взяты системные вызовы процессов программ. На их основе строятся оценки, позволяющие выставлять коэффициент доверия процессам.

Литература

1. Sandhu R.S., Coyne E.J., Feinstein H. L., Youman C.E. Computer role-based access control models // Computer. 1996. V. 29. N 2. P. 38–47. doi: 10.1109/2.485845
2. Sudip C., Indrajit R. TrustBAC – integrating trust relationships into the RBAC model for access control in open systems // Proc. ACM Symposium on Access Control Models and

References

1. Sandhu R.S., Coyne E.J., Feinstein H. L., Youman C.E. Computer role-based access control models. *Computer*, 1996, vol. 29, no. 2, pp. 38–47. doi: 10.1109/2.485845
2. Sudip C., Indrajit R. TrustBAC – integrating trust relationships into the RBAC model for access control in open systems. *Proc. ACM Symposium on Access Control Models and*

Technologies (SACMAT '06). Lake Tahoe, USA, 2006. P. 49–58.
3. Su R., Zhang Y., He Z., Fan S. Trust-based fuzzy access control model research // Lecture Notes in Computer Science. 2009. V. 5854. P. 393–399. doi: 10.1007/978-3-642-05250-7_42
4. IEEE 802.11s Mesh Networking. Network standard. IEEE, 2011.
5. Akyildiz I.F., Wang X., Wang W. Wireless mesh networks: a survey // Computer Networks. 2005. V. 47. P. 445–487. doi: 10.1016/j.comnet.2004.12.001
6. Lou W., Ren K. Security, privacy, and accountability in wireless access networks // IEEE Wireless Communications. 2009. V. 16. N 4. P. 80–87. doi: 10.1109/MWC.2009.5281259
7. Wang X. A Systematic Security Approach in Wireless Mesh Networks. PhD in Computer Science. Iowa State University, 2009.
8. Lin H. Hu J., Ma J., Xu L., Nagar A. A role based privacy-aware secure routing protocol for wireless mesh networks // Wireless Personal Communications. 2014. V. 75. N 3. P. 1611–1633. doi: 10.1007/s11277-013-1171-3
9. Mahalle P.N., Thakre P.A., Prasad N.R., Prasad R. A fuzzy approach to trust based access control in internet of things // Proc. 3rd Int. Conf. on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2013. Atlantic City, USA, 2013. doi: 10.1109/VITAE.2013.6617083
10. Ben Saied Y., Olivereau A., Zeghlache D., Laurent M. Trust management system design for the Internet of Things: a context-aware and multiservice approach // Computers and Security. 2013. V. 39. P. 351–365. doi: 10.1016/j.cose.2013.09.001
11. Chen D., Chang G., Sun D., Li J., Jia J., Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things // Computer Science and Information Systems. 2011. V. 8. P. 1207–1228. doi: 10.2298/CSIS110303056C
12. Bao F., Chen I.-R. Dynamic trust management for Internet of Things applications // Proc. Int. Workshop on Self-Aware Internet of Things. San Jose, USA, 2012. doi: 10.1145/2378023.2378025
13. Granichin O., Volkovich V., Toledano-Kitai D. Randomized Algorithms in Automatic Control and Data Mining. NY: Springer-Verlag, 2015. 251 p. doi: 10.1007/978-3-642-54786-7
14. Граничин О.Н., Павленко Д.В. Рандомизация получения данных и ℓ_1-оптимизация (опознание со сжатием) // Автоматика и телемеханика. 2010. № 11. С. 3–28.
15. Баклановский М.В., Ханов А.Р. Поведенческая идентификация программ // Моделирование и анализ информационных систем. 2014. Т. 21. №6. С. 120–130.

Technologies, SACMAT '06. Lake Tahoe, USA, 2006, pp. 49–58.
3. Su R., Zhang Y., He Z., Fan S. Trust-based fuzzy access control model research. *Lecture Notes in Computer Science*, 2009, vol. 5854, pp. 393–399. doi: 10.1007/978-3-642-05250-7_42
4. *IEEE 802.11s Mesh Networking*. Network standard. IEEE, 2011.
5. Akyildiz I.F., Wang X., Wang W. Wireless mesh networks: a survey. *Computer Networks*, 2005, vol. 47, pp. 445–487. doi: 10.1016/j.comnet.2004.12.001
6. Lou W., Ren K. Security, privacy, and accountability in wireless access networks. *IEEE Wireless Communications*, 2009, vol. 16, no. 4, pp. 80–87. doi: 10.1109/MWC.2009.5281259
7. Wang X. *A Systematic Security Approach in Wireless Mesh Networks*. PhD in Computer Science. Iowa State University, 2009.
8. Lin H. Hu J., Ma J., Xu L., Nagar A. A role based privacy-aware secure routing protocol for wireless mesh networks. *Wireless Personal Communications*, 2014, vol. 75, no. 3, pp. 1611–1633. doi: 10.1007/s11277-013-1171-3
9. Mahalle P.N., Thakre P.A., Prasad N.R., Prasad R. A fuzzy approach to trust based access control in internet of things. *Proc. 3rd Int. Conf. on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2013*. Atlantic City, USA, 2013. doi: 10.1109/VITAE.2013.6617083
10. Ben Saied Y., Olivereau A., Zeghlache D., Laurent M. Trust management system design for the Internet of Things: a context-aware and multiservice approach. *Computers and Security*, 2013, vol. 39, pp. 351–365. doi: 10.1016/j.cose.2013.09.001
11. Chen D., Chang G., Sun D., Li J., Jia J., Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. *Computer Science and Information Systems*, 2011, vol. 8, pp. 1207–1228. doi: 10.2298/CSIS110303056C
12. Bao F., Chen I.-R. Dynamic trust management for Internet of Things applications. *Proc. Int. Workshop on Self-Aware Internet of Things*. San Jose, USA, 2012. doi: 10.1145/2378023.2378025
13. Granichin O., Volkovich V., Toledano-Kitai D. *Randomized Algorithms in Automatic Control and Data Mining*. NY, Springer-Verlag, 2015, 251 p. doi: 10.1007/978-3-642-54786-7
14. Granichin O.N., Pavlenko D.V. Randomization of data acquisition and $\ell 1$-optimization (recognition with compression). *Automation and Remote Control*, 2010, vol. 71, no. 11, pp. 2259–2282. doi: 10.1134/S0005117910110019
15. Baklanovsky M.V., Khanov A.R. Identification of programs based on the behavior. *Modeling and Analysis of Information Systems*, 2014, vol. 21, no. 6, pp. 120–130.

v

Авторы

Баклановский Максим Викторович **–** старший преподаватель, Университет ИТМО, Санкт-Петербург, 191002, Российская Федерация, mb@cit.ifmo.ru

Ханов Артур Рафаэльевич **–** тьютор, Университет ИТМО, Санкт-Петербург, 191002, Российская Федерация, awengar@gmail.com

Authors

Maxim V. Baklanovsky **–** senior lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation, mb@cit.ifmo.ru

Arthur R. Khanov **–** tutor, ITMO University, Saint Petersburg, 197101, Russian Federation, awengar@gmail.com