Организация безопасной передачи данных в многоагентных системах контроля и диагностирования информационно-технологических сетей

Д. Г. Буханов, В. М. Поляков

Аннотация. В работе изложено описание протокола образования безопасного канала передачи данных. Подход основан на шифровании и инкапсуляции передаваемого в многоагентных системах IP трафика. Предлагаемый протокол включает в себя брандмауэр, подсистему туннелирования и подсистему шифрования. Представлены результаты экспериментов, которые позволяют оценить временные характеристики работы протокола.
Ключевые слова: *безопасная передача данных, протокол, многоагентные системы.*

Введение

Современное развитие информационных технологий привело к появлению новой отрасли науки и техники: информационно-технологические сети и системы (ИТС), которая является логическим результатом развития вычислительных и информационно-телекоммуникационных сетей. Большое распространение в ИТС получили компьютерные сети на базе Ethernet, Wi-Fi, GSM 3 и последующих поколений. Эти сети имеют многоуровневую организацию и используют в качестве третьего (сетевого) уровня протокол IP. Развитие ИТС затронуло многие отрасли науки, техники и технологий. В свою очередь, это привело к повышению требований надежности и безопасности ИТС. Одним из современных и быстро развивающихся подходов, повышающих надежность и безопасность сетей, является подход, основанный на использовании многоагентных систем контроля и диагностирования ИТС.

При проектировании многоагентных систем диагностирования ИТС возникает задача разработки коммуникационных модулей программных агентов, которые обеспечивают безопасную систему передачи данных.

1. Известные подходы обеспечения безопасной передачи данных

Первые попытки установления научно-технических приоритетов были предприняты обществами и правительствами экономически развитых стран сразу после Второй мировой войны. Наука впервые стала рассматриваться как двигатель научно-технического прогресса, порождающий и развивающий такие важные и новые области экономики, как ядерные и космические технологии. Во время этого периода произошло становление так называемой «большой науки», прежде всего в физике. На следующем этапе практика выбора научно-технических приоритетов концентрировалась на главных, централизованно задаваемых стратегических приоритетах, спускаемых «сверху вниз» (top-down). В последние декады XX столетия начался третий этап, характеризующийся более дифференцированным и децентрализованным выбором научно-технических приоритетов, что было связано с изменением роли университетов, появлением новых организационных форм, таких как научные и технологические фонды, исследовательские центры [18].

Современный подход к выбору научно-технических приоритетов стал более функциональным, чем прежде, и связан с осознанием возрастающей роли *национальной инновационной системы*. Теперь к *тематическим приоритетам* предыдущего периода добавляются *«функциональные» приоритеты* с целью концентрации усилий на совершенствовании общих и структурных характеристик национальной инновационной системы, например, укреплении взаимодействия науки и промышленности, стимулировании создания новых наукоемких организаций и производств. Однако в самое последнее время, из-за критики увлечения функциональными приоритетами, акцент вновь сместился на тематические при-

оритеты, но трактуемые по-новому. Тематические приоритеты не ограничиваются теперь лишь научно-технологическими приоритетами. Возрастает интерес к так называемым *целевым* (mission-oriented) *приоритетам*, которые определяются общественными потребностями.

При анализе инновационной системы принято выделять три уровня ее структуры.

Наиболее высокий политический уровень, называемый также «социетальным», на котором принимаются важнейшие стратегические решения, касающиеся общеэкономического развития государства, разработки научно-технической политики и выбора соответствующих научно-технических приоритетов.

Промежуточный уровень, называемый также институциональным, — министерства, ведомства, государственные научные и технологические фонды, крупные научные центры. Эти субъекты национальной инновационной системы трансформируют общенациональные приоритеты в приоритеты, отвечающие сфере их компетенции.

Низший уровень — отдельные организации научно-технического комплекса, в деятельности которых реализуются приоритеты двух предыдущих уровней системы.

Каждый из этих уровней обладает своей спецификой организации, взаимодействия, схемами информационных процессов, мотивацией и стратегией поведения участников.

Внимание, уделяемое систематизации подходов к выбору научно-технических приоритетов, особенно возросло в большинстве развитых стран в связи с децентрализацией принятия решений в соответствии с принципами нового общественного управления [20]. Это обусловлено ростом числа субъектов различных иерархических уровней управления, начиная с нижних и промежуточных, вносящих вклад в постановку приоритетов. Появилась необходимость в новых принципах распределения задач между уровнями управления, согласованных с общими стратегическими целями и общими ресурсными ограничениями. Ключевую роль в научно-технологической политике стали играть программные принципы, в рамках которых согласовываются исследовательские работы, выполняемые на нижних уровнях, и приоритеты верхнего уровня, обеспечиваемые финансовыми ресурсами.

Подходы к разработке и проведению в жизнь инновационно-технологической политики в разных странах существенно различаются. На них сказываются национальные традиции, историческое наследие и политическое развитие каждой страны. Страны, например, такие как Франция, национальные политики которых ориентированы на осуществление крупных целевых программ, отличаются от стран, таких как США, Германия, политики которых ориентированы на создание экономического и правового климата, способствующего повсеместному распространению нововведений.

Вместе с тем можно констатировать, что в настоящее время практически во всех развитых странах, несмотря на имеющиеся различия, подходы к определению научно-технических приоритетов в значительной мере базируются на осмыслении потребностей национальной инновационной системы. Именно это является общим, объединяющим признаком, который позволяет провести сопоставление национальных подходов к выбору научно-технических приоритетов [19].

2. Структура системы обеспечения безопасной передачи данных

Предлагается подход для обеспечения безопасных коммуникаций программных агентов в режиме реального времени, направленный на выполнение следующих требований:

- обеспечение свойства perfect forward secrecy (PFS);
- обеспечение стойкости алгоритма шифрования к криптоанализу;
- обеспечение противостояния DDoS-атакам.

Для решения задачи образования безопасного канала передачи данных в многоагентных системах предлагается протокол NCTP (Network Cryptography Tunneling Protocol), которой работает поверх IP протокола. Структура программного агента показана на рис. 1.

Агент состоит из модуля формирования, хранения и интерпретации правил (Rules base), модуля принятия диагностических решений (Logical solver) и коммуникационного модуля (Communication agent's module). Модуль Logical solver формирует команды (out command message) для отправки другим программным агентам, а так же выполняет обработку принятых команд от них (in command message). Примером такой команды может быть сообщение агенту списка узлов подозреваемых в сетевой атаке и т. д. В коммуникационном модуле реализован протокол передачи данных с образованием защищенного канала.

Основной принцип работы протокола основан на закрытии транспортных портов (TCP port) защищаемых приложений и шифровании трафика от этих приложений при передаче по открытому каналу. Распределение трафика по приложениям на узле выполняет сам NCTP. Он состоит из следующих подсистем: брандмауэр, подсистема туннелирования и подсистема шифрования. Каждая из них является обособленной и способна модифицироваться, не затрагивая остальные.

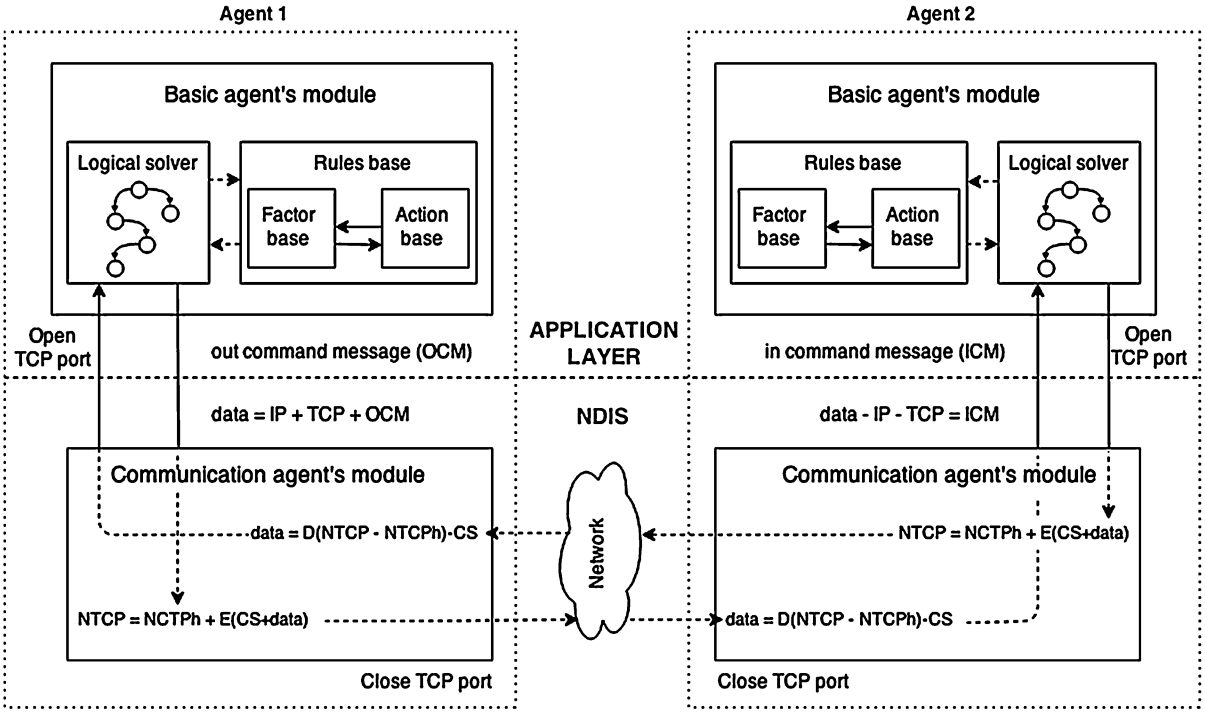

Рис. 1. Структура программного агента

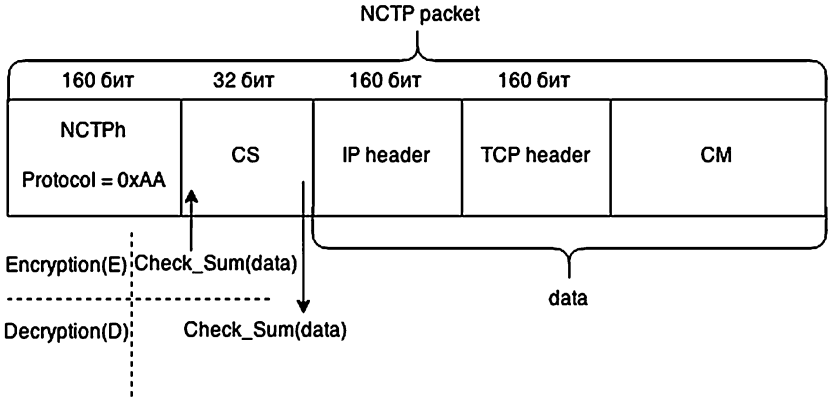

Рис. 2. Структура NCTP пакета

Брандмауэр представляет собой систему блокировки защищаемых портов. Одновременно он выполняет функцию приема, фильтрации и отправки сообщений. Для реализации в операционных системах семейства Windows использована библиотека windivert[11], которая является надстройкой над NDIS. Она позволяет перехватывать и блокировать входящий и исходящий трафик на сетевом уровне.

Система туннелирования представляет собой инкапсуляцию пакетов верхних уровней в пакеты уровней, расположенных ниже. При отправке происходит инкапсуляция защищаемого трафика в протокол NCTP, а при получении пакета протокола NCTP происходит выделение трафика из него.

Структура пакета NCTP протокола показана на рис. 2. IP header, TCP header формируются протоколами сетевого и транспортного уровня соответственно. В поле CM (command message) содержатся команды передаваемые между агентами. В поле CS записана контрольная сумма.

Сформированный пакет NCTP состоит из двух частей:

$$NCTP = NCTPh + E(CS + data, key);$$

где NCTPh — заголовок протокола NCTP, используемый для совместимости с коммуникационным оборудованием; E(CS + data, key) — функция шифрования над полями контрольной суммы и data;

Check_Sum(data) — функция формирования контрольной суммы; data — открытый TCP пакет с передаваемыми данными; key — ключ шифрования для функции E().

При приеме NCTP пакета из сети происходит выделение блока data:

$$data = D(NCTP - NCTPh, key) - CS;$$

где D(NCTP – NCTPh, key) — функция расшифрования принятого тела NCTP пакета; key — криптографический ключ; CS — поле контрольной суммы в принятом пакете.

Для выявления пакетов, которые может модифицировать злоумышленник, происходит проверка соответствия полученной контрольной суммы и записанной в пакете.

Для обработки только тех пакетов, которые поддерживают NCTP протокол, поле Protocol в IP заголовке помечается не зарезервированным флагом 0xAA. Пакет с таким флагом обработается требуемым способом. Полученное сообщение data является в свою очередь TCP пакетом, отправленным агентом на передающей стороне. Оно будет передано сетевому уровню драйвера NDIS, который завершит отправку доставкой сообщения агенту на приемной стороне. Такая реализация системы туннелирования потенциально защищает приложения от SYN flood, UDP flood атак, так как исключает открытые порты транспортного уровня при взаимодействии агентов.

Система шифрования представляет собой симметричный алгоритм шифрования. Для реализации был выбран алгоритм поточного шифрования xsalsa, представленный в [12]. Предлагается также использовать salsa20/8 или ChaCha, сравнительная характеристика которых приведена в работе [13]. Эти алгоритмы являются более быстрыми. В работе [14] описан метод их криптоанализа. В предлагаемом подходе была использована библиотека sodium [15], основанная на библиотеке NaCl, но в отличие от нее, совместима с большинством операционных систем [16]. Ее использование дает возможность реализовать, описанный выше протокол, не только в качестве нативного приложения Windows, но и как систему туннелирования для браузеров, а также как сервис для мобильных операционных систем. Так как не было опубликованных прецедентов взлома ключа этого алгоритма, можно считать его абсолютно безопасным.

3. Экспериментальные результаты

На основе описанного подхода были проведены эксперименты, в которых оценивалось время передачи данных по сети с использованием защищенного канала и их избыточность. Эксперименты проводились при следующих настройках:

- изолированная среда передачи данных, состоящая из двух компьютеров, двух коммутаторов подключенных последовательно; в такой среде отсутствовал любой другой трафик, кроме исследуемого;
- OpenVPN был настроен на использование локальных ключей шифрования, алгоритм шифрования DES, тип соединений TCP;
- VipNET был настроен на алгоритм шифрования AES с использованием локальных ключей;
- NCTP был настроен на алгоритм шифрования xsalsa20 с использованием локальных ключей;
- все эксперименты проводились при одной конфигурации ОС Windows 7.

На рис. 3 изображен график зависимости среднего времени передачи данных от размера передаваемых данных.

Из графиков видно, что система на основе NCTP показывает лучшее время передачи в сравнении с OpenVPN при любых размерах данных, а в сравнение с VipNet при размере поля данных больше 1200 байт.

На рис. 4 показано наихудшее время передачи данных, заданного размера при проведении 100 сессий передачи.

Тенденция относительно среднего времени остается неизменной, но разброс времени при линейном увеличении размера происходит нелинейно. Это свидетельствует о нестабильности и непредсказуемости поведения исследуемых систем. Считается, что чем более сглаженной выглядит линия графика, тем более стабильно ведет себя система.

На рис. 5 показаны графики аппроксимированных полиномом пятой степени производной функций времени передачи данных от размера данных.

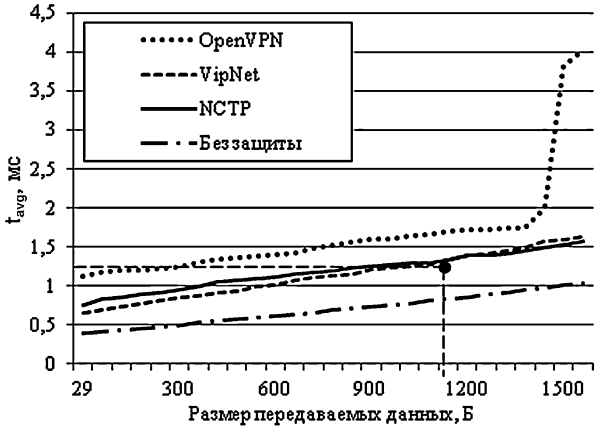

Рис. 3. Зависимости среднего времени передачи данных от размера данных

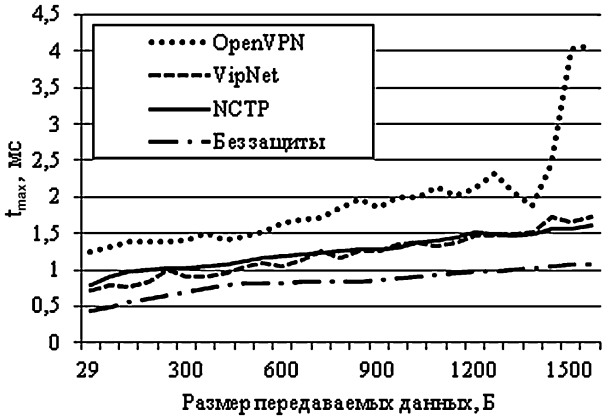

Рис. 4. Зависимости максимального времени передачи данных от размера данных

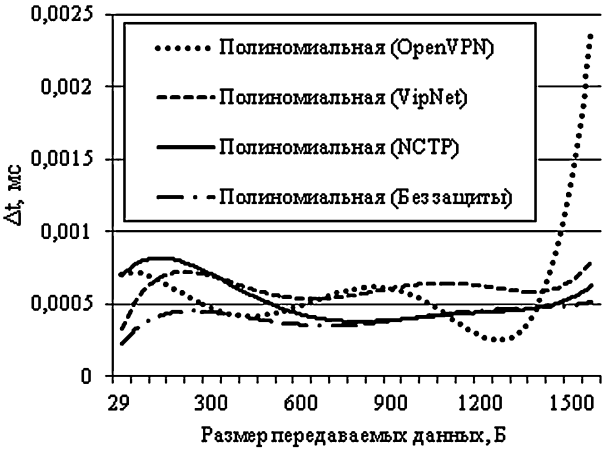

Рис. 5. Графики трендов времени передачи данных от размера данных

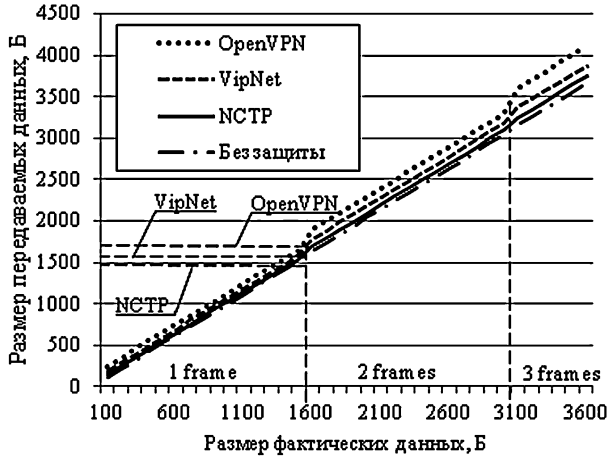

Рис. 6. Зависимости избыточности информации передаваемой по сети от фактических данных

Эти графики показывают основные тенденции изменения скорости в зависимости от увеличения размера передаваемых данных. NCTP показывает линейное приращение, при размере блока данных больше 800 байт. Он совпадает с графиком без использования шифрования. Это означает, что изменение скорости передачи данных при увеличении размера происходит линейно и следовательно предсказуемо. Данное свойство позволяет использовать протокол NCTP в системах передачи реального времени.

Из графиков на рис. 6 следует, что NCTP использует меньшее количество избыточной информации для передачи, чем VipNet и OpenVPN. Это влияет на скорость передачи данных по сети, а так же снижает потенциальную уязвимость управляющей информации пакетов.

На основе представленных результатов экспериментов, можно оценить временные характеристики предложенного протокола NCTP. Было выявлено, что протокол NCTP показывает сопоставимые с рассмотренными аналогами результаты при небольших размерах пакета. Если размер блока данных больше 1200 байт, то протокол NCTP показывает лучшее время по сравнению с другими системами.

Выводы

Предложенный протокол NCTP показывает лучшие временные характеристики передачи данных в сравнении с рассмотренными аналогами. Предложенный подход обеспечивает защиту от типовых Dos атак на участвующих во взаимодействии программных агентов. Использование криптостойкого алгоритма шифрования обеспечивает защиту передаваемых данных от просмотра (sniffing). Проведенные эксперименты показывают возможность использования NTCP в качестве механизма образования безопасного канала передачи данных в многоагентных системах реального времени контроля и диагностирования информационно-технологических сетей.

В дальнейшем развитие данного подхода связано с совершенствованием существующих алгоритмов аутентификации и систем обмена криптографическими ключами.

Литература

1. Сайт VipNet. http://www.infotecs.ru
2. *Aumasson J. P.* New features of Latin dances: analysis of Salsa, ChaCha, and Rumba / J. P. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Software Encryption. Springer Berlin Heidelberg, 2008. P. 470–488.
3. *Bernstein D. J.* Salsa20 specification / D. J. Bernstein // eSTREAM Project algorithm description. 2005. http://www.ecrypt.eu.org/stream/salsa20pf.html

4. *Bittau A.* The Case for Ubiquitous Transport-Level Encryption / A. Bittau, M. Hamburg, M. Handley, D. Mazieres, D. Boneh // USENIX Security Symposium. 2010. P. 403–418.
5. Сайт Electronic Frontier Foundation. HTTPS everywhere. https://www.eff.org/https-everywhere
6. *Jackson C.* Forcehttps: protecting high-security web sites from network attacks / C. Jackson, A. Barth // Proceedings of the 17th international conference on World Wide Web. ACM. 2008. P. 525–534.
7. *Li Z.* Analysis and classification of ipsec security policy conflicts / Z. Li. X. Cui, L. Chen // Frontier of Computer Science and Technology, 2006. FCST'06. Japan-China Joint Workshop on. IEEE, 2006. P. 83–88.
8. *Liu J.* A real-time network simulation infrastructure based on OpenVPN / J. Liu, Y. Li. N. Van Vorst, S. Mann, K. Hellman // The Journal of Systems and Software. 82, 2009 P. 473–485.
9. Сайт OpenVPN — The Open Source VPN. https://openvpn.net
10. *Radhakrishnan S.* TCP fast open / S. Radhakrishnan, Y. Cheng, J. Chu, A. Jain, B. Raghavan // Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies. ACM, 2011. P. 21
11. *Rescorla E.* Datagram transport layer security version 1.2. / E. Rescorla, N. Modadugu. https://tools.ietf.org/html/rfc6347
12. Сайт Securing ZeroMQ: the Sodium Library. http://hintjens.com/blog:35
13. Сайт The Sodium crypto library (libsodium) http://doc.libsodium.org
14. *Tsunoo Y.* Differential cryptanalysis of Salsa20/8 / Y. Tsunoo, T. Saito, H. Kubo, T. Suzaki, H. Nakashima // Workshop Record of SASC. 2007. P. 12
15. *Vratonjic N.* The inconvenient truth about web certificates / N. Vratonjic, J. Freudiger, V. Bindschaedler, J. P. Hubaux // Economics of Information Security and Privacy III. Springer New York, 2013. P. 79–117.
16. Сайт WinDivert 1.1: Windows Packet Divert. https://reqrypt.org/ windivert.html

Буханов Дмитрий Геннадьевич. Старший преподаватель Белгородского ГТУ им. В. Г. Шухова. Окончил в 2011 году Белгородский ГТУ. Количество печатных работ: 13. Область научных интересов: сетевые технологии, методы диагностики компьютерных сетей, безопасные протоколы передачи информации. E-mail: db.old.stray@gmail.com

Поляков Владимир Михайлович. Зав. кафедры Белгородского ГТУ им. В. Г. Шухова. К. т. н., доцент. Окончил в 1981 году Харьковский авиационный институт им. Н. Е. Жуковского, Количество печатных работ: 60. Область научных интересов: многоагентные системы, информационная безопасность. E-mail: p_v_m@mail.ru