УДК 004.056 Вестник УрФО № 3(41) / 2021, с. 24–29

Чан З. Х.

DOI: 10.14529/secur210303

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Обеспечение информационной безопасности элементов киберфизических систем является необходимым условием их корректного функционирования. В мобильной распределённой киберфизической системе эта задача осложняется рядом специфических факторов, связанных, в том числе с неконтролируемым доступом к беспроводной среде передачи данных и ограничениями на применение «тяжёлой» криптографии. В статье проанализированы протоколы аутентификации типа «запрос - ответ», приведены результаты исследования различных криптографических механизмов, используемых в таких протоколах, и выявлены угрозы безопасности аутентификации. Работа будет полезна молодым ученым, разрабатывающим методы аутентификации в киберфизической системе, а также специалистам, работающим в области информационной безопасности.

Ключевые слова: *сенсорная сеть, информационная безопасность, аутентификации стороны, криптография, угроза, киберфизическая система.*

Chan Z.H.

AUTHENTICATION PROBLEMS IN WIRELESS SENSOR NETWORKS

Ensuring information security of elements of cyber-physical systems is a prerequisite for their correct functioning. In a mobile distributed cyber-physical system, this task is complicated by a number of specific factors related, including uncontrolled access to wireless data transmission medium and restrictions on the use of "heavy" cryptography. The article analyzes authentication protocols of the "challenge-response" type, presents the results of a study of various cryptographic mechanisms used in such protocols, and identifies threats to the security of authentication. The work will be useful for young scientists who develop authentication methods in a cyber-physical system, as well as specialists working in the field of information security.

Keywords: *sensor network, information security, side authentication, cryptography, threat, cyber-physical system.*

Введение

В киберфизической системе (КФС) [1] аутентификация объекта является необходимым шагом для обеспечения информационной безопасности и корректности функционального взаимодействия. Несмотря на наличие широкого спектра работ в этом направлении, задача разработки метода аутентификации в беспроводных сенсорных сетях остаётся актуальной научно-технической задачей. Причём вопросы выявления проблемы аутентификации для конкретной реализации КФС выходят на первый план с увеличением комплексных рисков эксплуатации таких систем.

Необходимость применения беспровод-

ных сенсорных сетей стала важной в настоящее время и в будущем из-за их уникальных преимуществ: низкая стоимость (установка и эксплуатация), возможность широкого развертывания с самоорганизацией, легким добавлением или исключением агента из сети. Они используются в роботах не только для обмена данными, но и для сбора информации, полученной из окружающей среды, для передачи ее центральному узлу. С точки зрения мобильных агентов к процедуре аутентификации предъявляется ряд дополнительных требований, связанных с ограничением времени и пространства взаимодействия, ограниченностью доступных вычислительных ресурсов и возможностью компрометации объекта путём получения физического доступа к нему [2,3]. Причём для КФС актуальной становится не только аутентификация информационного потока, но и аутентификация собственно агента (устройства) [4].

В зависимости от конкретных условий функционирования КФС реализуются различные механизмы аутентификации взаимодействующих сторон, как правило с сохранением конфиденциальности информации. Выделяют две основные модели аутентификации: модель с непосредственной связью пар агентов [5]; и модель с использованием доверенной третьей стороны [6], что особенно важно при отсутствии зон перекрытия коммуникаций мобильных агентов [7].

Протокол аутентификации типа «запрос – ответ»

Согласно со стандартами ISO / IEC 9798 под аутентификацией сторон понимается как процесс проверки подлинности предлагающего агента [8]. В том числе включает протоколы аутентификации на основе симметричного, асимметричного ключа, хеширование, протоколы с нулевым разглашением знаний.

Протоколы аутентификации типа «запрос – ответ» с использованием симметричных криптосхем основаны на подтверждении путём доказывания знания секрета. Этот секрет может быть создан заранее или сгенерирован доверенной третьей стороной во время сеанса связи. Протоколы аутентификации на основе асимметричного шифрования обеспечивают высокую степень безопасности, но требуют больших вычислительных ресурсов и сложности процесса генерирования ключевой пары. Протоколы аутентификации в беспроводных специальных сетях описаны в таблицах 1,2,3,4,5.

Проблема качества криптографических примитивов

Применение криптографических методов аутентификации обеспечивает более высокий уровень безопасности. Однако облечённый протокол требует небольшого времени обработки оператором для уменьшения задержки. Мы протестировали время отработки некоторых операторов (рисунок 1) с использованием Raspberry Pi3 b +, 1,4 ГГц ЦП, 1024 RAM LPDDR2, Micro SD 8GB. Размер ключа выбирается в соответствии с требованием безопасности [9].

Как показано на рисунке, время обработ-

Таблица 1

Протокол аутентификации на основе пароля

Агент А	*к* - общий секретный ключ	Агент В
$M = D_k(C)$ Если { $P_b^{'} = P_b$ } то {В аутентифицирован}	<|= [C]	P_b – пароль $C = E_k(P_b)$

Таблица 2

Протокол взаимной аутентификации, основанной на симметричном шифровании

Агент А	*к* - общий секретный ключ	Агент В
	<|= [N_b]	N_b – случайное число
N_a - случайное число $C_1 = E_k(N_a, N_b, B)$	[C_1] =|>	$M_1 = D_k(C_1)$ Если {$N_b^{'} = N_b$}и{$B^{'} = B$} то {А аутентифицирован}
$M_2 = D_k(C_2)$ Если {$N_a^{'}$=N_a}и{$N_b^{''} = N_b$} то {В аутентифицирован}	<|= [C_2]	$C_2 = E_k(N_a, N_b)$

Таблица 3

Протокол взаимной аутентификации, основанной на асимметричном шифровании

Агент А		Агент В
Генерация пары ключей sk_a, pk_a	$[pk_a]=\|>$ $<\|=[pk_b]$	Генерация пары ключей sk_b, pk_b
	$<\|=[N_b]$	N_b – случайное число
N_a - случайное число $C_1 = E_{pk_b}(N_a, N_b, B)$	$[C_1]=\|>$	$M_1 = D_k(C_1)$ Если $\{N_b^{'} = N_b\}$и$\{B^{'} = B\}$ то {А аутентифицирован}
$M_2 = D_k(C_2)$ Если $\{N_a^{'} = N_a\}$и$\{N_b^{"} = N_b\}$ то {В аутентифицирован}	$<\|=[C_2]$	$C_2 = E_{pk_a}(N_a, N_b)$

Таблица 4

Протокол взаимной аутентификации, основанной на основе сертификатов, и цифровой подпись

Агент А		Агент В
Генерация пары ключей sk_a, pk_a Получение сертификат cer_a	$[pk_a]=\|>$ $<\|=[pk_b]$	Генерация пары ключей sk_b, pk_b Получение сертификат cer_b
Получение t_a - метка времени $S_1 = Sign_{sk_a}(t_a, B)$	$[S_1, t_a, B, cer_a]=\|>$	$Ver_{pk_a}(S_1) \overset{?}{=} \{0/1\}$ Если $\{Ver_{pk_a}(S_1) == 1\}$ то {А аутентифицирован}
$Ver_{pk_b}(S_2) \overset{?}{=} \{0/1\}$ Если $\{Ver_{pk_b}(S_2) == 1\}$ то {В аутентифицирован}	$<\|=[S_2, t_b, A, cer_b]$	Получение t_b - метка времени $S_2 = Sign_{sk_b}(, t_b, A)$

Таблица 5

Протокол взаимной аутентификации на основе ключевой хеш-функции

Агент А	k - общий секретный ключ	Агент В
	$<\|=[N_b]$	N_b – случайное число
N_a - случайное число $H_1 = h_k(N_a, N_b, B)$	$[N_a, H_1]=\|>$	$H_1^{'} = h_k(N_a, N_b, B)$ Если $H_1^{'} = H_1\}$, то {А аутентифицирован}
$H_2^{'} = h_k(N_a, N_b, A)$ Если $\{H_2^{'} = H_2\}$, то {В аутентифицирован}	$<\|=[H_2]$	$H_2 = h_k(N_a, N_b, A)$

Разъяснение обозначений

$E_k()$	Шифрование с общим ключом
$D_k()$	Дешифрование с общим ключом
sk	Секретный ключ
pk	Публичный ключ
$Sign_{sk}$	Подпись секретным ключом
Ver_{pk}	Верификация публичным ключом
$h_k()$	Хэш-функция
$E_{pk}()$	Шифрование публичным ключом
$D_{sk}()$	Дешифрование секретным ключом

ки DSA является самым высоким, а время обработки MD5 - самым низким, составляющим всего 0,125 мс. Значительная разница во времени отработки показывает возможность

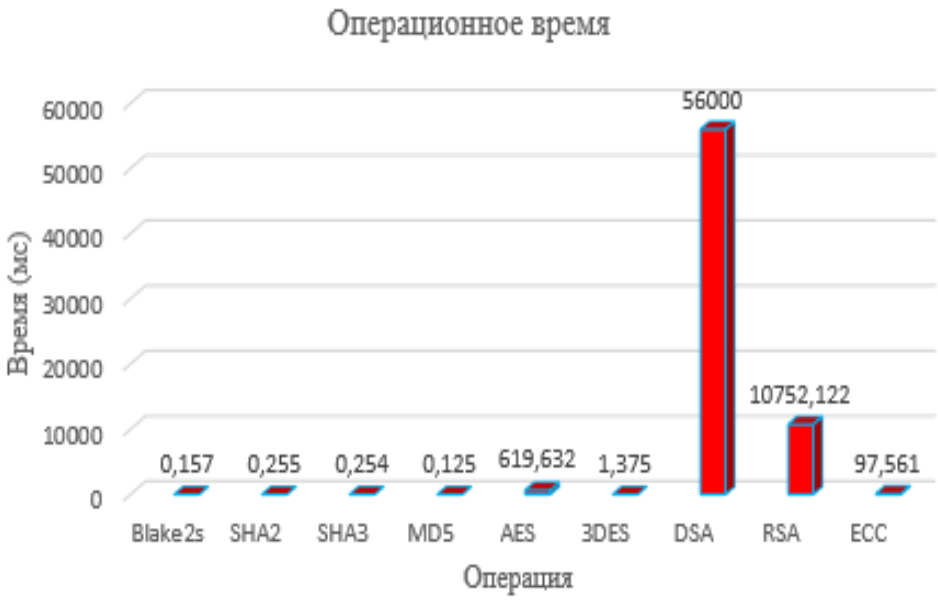

Рис. 1. Примитивное время для криптографической операции

Таблица 6

Сравнение степени использования методов аутентификации в беспроводных сенсорных сетях

Аутентификации в беспроводной сенсорной сети	Уровень вычисления	Уровень безопасности	Уровень ресурсов
Аутентификация на основе пароля	средняя	низкая	средняя
Аутентификация на основе сертификатов и цифровая подпись	высокая	высокая	высокая
Аутентификация, основанная на симметричном шифровании	средняя	высокая	средняя
Аутентификация, основанная на асимметричном шифровании	высокая	высокая	высокая
Аутентификация на основе хеша	низкая	высокая	средняя

применения аутентификация на основе односторонней хеш-функции требует наименьших вычислительных затрат. Ключевая хеш-функция использует общий секретный ключ для вычисления хэш-значения, но необходимо периодически изменять секретный ключ для защиты от некоторых атак. Чтобы решить эту проблему, используется общий секретный ключ в качестве аргумента хэш-функции. Выводы о степени применения методов аутентификации в беспроводных сенсорных сетях представлены в таблице 6.

Специфика аутентификации в беспроводных сенсорных сетях

Используя централизованный подход, агенты должны связываться с сервером, когда требуется аутентификация. Это очень неудобно для динамичного киберпространства, как воздушного аппарата. Более того, серверу аутентификации будет сложно избежать перегрузки при выполнении взаимной аутентификации для агентов в группе. Что касается децентрализованного подхода, проблема распределения групповых секретных ключей должна быть решена, потому что должна быть точка доверия, такая как центральный сервер аутентификации.

Основными проблемами аутентификации в беспроводных сенсорных сетях являются динамичность (часто меняется состояние элементов); ограниченный ресурс, запас энергии, время автономной работы устройств и наличие информационных угроз. В открытых средах злоумышленникам доступны данные сеансов связи, что позволяет осуществлять сбор коммуникационной информации и проводить типовые атаки на протоколы аутентификации, такие как подмена одного

Таблица 7

Угроз аутентификации в беспроводных сенсорных сетях

Причина	Вид воздействия
Несовпадение предъявленного секрета	- Сбой техники (аппаратный или программный) - Попытка злоумышленника (нарушители)
Превышено время аутентификации	- DoS- атака (интенсивность потока заявок) - Внутренний нарушитель
Недостаточно времени для завершения процессы	- Динамичный агент (не завершил процесс аутентификации, находясь в области взаимодействия)
Не выявил обман при проверке ID	- Атака класса «маскарад» (подделка на имя легального агента)
Потеря аутентичный секрет	- Атака злоумышленника

агента другим, сохранение и задержка передачи сообщения, повторение сеансового сообщения, отражение сообщения и комбинированные. Наличие уязвимостей в системе и угроз приводит к тому, что, с одной стороны, необходимо решить проблему сохранения целостности данных, с другой стороны, обеспечить нормальный доступ для легальных агентов на этих данных. Проблема информационных угроз представлена в таблице 7.

Существуют нарушители (законные агенты) и злоумышленники (неавторизованные агенты), влияющие на качество аутентификации. Нарушители могут выявлять «личность» другого агента и отправлять сообщения для обнаружения соседей, «сговориться» и использовать общий секретный ключ с аутентичными агентами. Злоумышленник может стараться идентифицировать секретный ключ и взломать схему аутентификации. Для повышения эффективности процесса обеспечения информационной безопасности во время аутентификации необходимо дифференцировать вредоносные объекты, что позволит разработать специфические механизмы противодействия.

Заключение

В статье проанализирован протокол аутентификации типа «запрос-ответ». Проведен результат исследования криптографических операторов, используемых в таких протоколах, выявлены угрозы процессу аутентификации. Исследование потенциальных проблем аутентификации в беспроводных сенсорных сетях способствует улучшению способности обрабатывать методы и протоколы аутентификации в зависимости от поставленных задач.

Перспективными направлениями исследований являются: разработка методики автоматизированной генерации протоколов аутентификации в группировках агентов – беспилотных транспортных средств в зависимости от условий и требований к функционированию КФС; и, связанное с этим формирование библиотек (шаблонов) примитивов, содержащих верифицированные компоненты протоколов взаимодействия таких агентов.

Литература

1. A. Humayed, J. Lin, F. Li and B. Luo. Cyber-Physical Systems Security—A Survey // IEEE Internet of Things Journal, Dec. 2017, vol. 4, no. 6, pp. 1802-1831, DOI: 10.1109/JIOT.2017.2703172.

2. Комаров И. И., ЮРЬЕВА Р. А., ДРАННИК А.Л., МАСЛЕННИКОВ О. С. Постановка задачи обеспечения информационной безопасности роевых робототехнических систем //Наука и бизнес: пути развития. – 2015. – №. 3. – С. 53.

3. Чан З., Комаров И. И., Швед В.Г. Аутентификация агентов в группе БПЛА на основе социальных механизмов // Защита информации. Инсайд - 2019. - № 6(90). - С. 66-71.

4. А. В. Черемушкин, "Криптографические протоколы: основные свойства и уязвимости // прикладная дискретная математика, 2009, приложение № 2, ст.115–150. DOI: 10.1016/j.procs.2016.06.038.

5. A. H. Moon, U. Iqbal, and G. M. Bhat. Mutual entity authentication protocol based on ECDSA for WSN // Procedia Computer Science, 2016, vol. 89, pp. 187–192.

6. Ullah, S., Li, XY. & Lan, Z. A novel trusted third party based signcryption scheme // Multimedia Tools and Applications, 2020, vol. 79, p. 22749 – 22769, DOI: 10.1007/s11042-020-09027-w.

7. M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles // IEEE Internet of Things Journal, 2020 DOI: 10.1109/JIOT.2020.3010893.

8. ISO/IEC 9798:2010 Information technology – Security techniques – Entity authentication.

9. Рекомендация по размеру криптографического ключа. Интернетный ресурс – [Режим доступно] https://www.keylength.com/en/compare/

References

1. A. Humayed, J. Lin, F. Li and B. Luo. Cyber-Physical Systems Security — A Survey // IEEE Internet of Things Journal, Dec. 2017, vol. 4, no. 6, pp. 1802-1831, DOI: 10.1109 / JIOT.2017.2703172.

2. Komarov I. I., YUR'YEVA R. A., DRANNIK A.L., MASLENNIKOV O. S. Postanovka zadachi obespecheniya informatsionnoy bezopasnosti royevykh robototekhnicheskikh sistem //Nauka i biznes: puti razvitiya. – 2015. – №. 3. – S. 53.

3. Chan Z., Komarov I. I., Shved V.G. Autentifikatsiya agentov v gruppe BPLA na osnove sotsial'nykh mekhanizmov // Zashchita informatsii. Insayd - 2019. - № 6(90). - S. 66-71.

4. A. V. Cheremushkin, "Kriptograficheskiye protokoly: osnovnyye svoystva i uyazvimosti // prikladnaya diskretnaya matematika, 2009, prilozheniye № 2, st.115–150. DOI: 10.1016/j.procs.2016.06.038.

5. A. H. Moon, U. Iqbal, and G. M. Bhat. Mutual entity authentication protocol based on ECDSA for WSN // Procedia Computer Science, 2016, vol. 89, pp. 187-192.

6. Ullah, S., Li, XY. & Lan, Z. A novel trusted third party based signcryption scheme // Multimedia Tools and Applications, 2020, vol. 79, p. 22749 - 22769, doi: 10.1007 / s11042-020-09027-w.

7. M. N. Aman, U. Javaid, and B. Sikdar, "A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles // IEEE Internet of Things Journal, 2020 DOI: 10.1109 / JIOT.2020.3010893.

8. ISO / IEC 9798: 2010 Information technology – Security techniques – Entity authentication.

9. Rekomendatsiya po razmeru kriptograficheskogo klyucha. Internetnyy resurs – [Rezhim dostupno] https://www.keylength.com/en/compare/

ЧАН Зуи Хань, инженер, аспирант факультета безопасности информационных технологий, университет информационных технологий, механики и оптики (национальный исследовательский университет). 197101, г. Санкт-Петербург, Кронверкский проспект, д. 49-А. Email: viewtheworld93@gmail.com.

CHAN Zui Han, engineer, PhD student of the Faculty of Secure Information Technologies, University of Information Technologies, Mechanics and Optics (National Research University). 197101, St. Petersburg, Kronverkskiy prospect, 49-A. Email: viewtheworld93@gmail.com.