STUDIA INFORMATICA 2012
Volume 33 Number 2B (106)

Marcin STRZAŁEK, Piotr PAŁKA
Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej

PROBLEMATYKA POUFNOŚCI, AUTENTYCZNOŚCI, INTEGRALNOŚCI ORAZ NIEZAPRZECZALNOŚCI DANYCH W SYSTEMACH WIELOAGENTOWYCH[1]

Streszczenie. W pracy rozważana jest problematyka bezpieczeństwa komunikacji w systemach wieloagentowych. Dodatek do systemu JADE, o nazwie JADE-S, dostarcza odpowiednich narzędzi do zapewnienia bezpieczeństwa w systemie wieloagentowym. Jest on rekomendowany do realizacji bezpieczeństwa w systemach wieloagentowych opartych na JADE. W pracy opisano, w jaki sposób mogą być zapewnione odpowiednie poziomy poufności, niezaprzeczalności oraz autentyczności wysyłanych komunikatów. Ponadto, rozważa się możliwość negocjacji poziomu zabezpieczeń oraz odpowiedniego algorytmu szyfrowania.

Słowa kluczowe: bezpieczeństwo, poufność, niezaprzeczalność, autentyczność, systemy wieloagentowe

THE ISSUE OF CONFIDENTIALITY, AUTHENTICATION, INTEGRITY AND DATA NON-REPUDIATION IN THE MULTIAGENT SYSTEMS

Summary. The paper considers the issue of security of communication in multi-agent systems. JADE-S framework provides the appropriate tools to ensure security in a multi-agent system. It is recommended to implement security in multi-agent systems based on JADE. Aim of this study is to describe how appropriate levels of confidentiality, non-repudiation and data authentication can be provided. Moreover, we consider the possibility of negotiating an appropriate level of security and encryption algorithm.

Keywords: security, confidentiality, non-repudiation, authentication, multi-agent systems

[1] Praca naukowa finansowana ze środków na naukę w latach 2009 – 2011, jako projekt badawczy nr N N516 375736.

1. Wprowadzenie

Systemy wieloagentowe coraz częściej znajdują zastosowanie w różnych dziedzinach naszego życia. Znane z literatury zastosowania tychże systemów to systemy symulacyjne, diagnostyczne, monitorujące i sterowania [8, 9]. Szeroką gamą potencjalnych zastosowań są także systemy handlowe, działające zarówno w konfiguracji scentralizowanej (systemy aukcyjne) [5, 6], jak i rozproszonej (systemy negocjacyjne) [10, 11]. Architektura sieciowa systemu wieloagentowego, wykorzystująca Internet jako główny kanał komunikacji, jest narażona na ataki, jest więc potencjalnym słabym punktem bezpieczeństwa całego systemu. Nieautoryzowany dostęp i ingerencja w zasoby wyspecjalizowanego systemu wieloagentowego mogą spowodować ogromne straty, nieograniczające się do finansowych. Konsekwencją ataku na system wdrożony w szpitalu może być publikacja danych wrażliwych pacjentów oraz modyfikacja informacji diagnostycznych, prowadząca do błędów w dalszym leczeniu. Również w systemach handlowych, w których wysoko cenioną cechą jest bezpieczeństwo, kradzież danych może mieć katastrofalne skutki dla przedsiębiorstwa, którego dane „wyciekły". Należy więc zapewnić odpowiedni poziom bezpieczeństwa transakcji zachodzących w systemie wieloagentowym.

1.1. Systemy wieloagentowe

System wieloagentowy jest systemem złożonym z dwóch lub większej liczby autonomicznych (niezależnych) komponentów, zwanych agentami [14]. Agenty podejmują decyzje w imieniu podmiotu, którego interesy reprezentują, tak aby zrealizować zadane cele. Wszystkie agenty wchodzące w skład systemu wieloagentowego mogą na siebie oddziaływać przez wzajemną komunikację. System taki powinien realizować pewne cele nadrzędne i funkcjonować zgodnie z intencjami projektanta systemu, przy czym system nie realizuje tych celów bezpośrednio, lecz przez indywidualne cele każdego z agentów oraz ich wzajemne interakcje. Cele indywidualne poszczególnych agentów są zazwyczaj rozbieżne. Ponadto, cel każdego agenta może być (i zazwyczaj jest) jego informacją prywatną.

1.2. Standaryzacja komunikacji międzyagentowej

Aby możliwa była efektywna i jednoznaczna komunikacja pomiędzy agentami, należy je umieścić w pewnym środowisku, które dostarczy im standardów komunikacji. Rzeczywistym standardem dostarczającym rozwiązania szkieletowego, w ramach którego agenty mogą funkcjonować, są standardy zdefiniowane przez FIPA (ang. *Foundation of Intelligent Physical Agents*) [1]. FIPA, jako organizacja promująca wykorzystywanie środowisk wieloagento-

wych, opracowała wiele standardów dotyczących komunikacji międzyagentowej, sprecyzowała akty komunikacyjne (ang. *Communicative Acts*), zidentyfikowała i zaproponowała pewne schematy wymiany komunikatów (ang. *Interaction Protocols*) oraz opracowała zestaw języków treści dla komunikatów (ang. *Content Languages*). Te trzy elementy stanowią łącznie język komunikacji agentów FIPA-ACL (ang. *Agent Communication Language*).

2. Bezpieczeństwo

W rozdziale tym przedstawione zostały standardy oraz zalecenia dotyczące zachowania zasad bezpieczeństwa w systemach komputerowych oraz wieloagentowych. Opisano także realizację tych zaleceń w systemie opartym na standardach opracowanych przez FIPA.

2.1. Bezpieczeństwo według ISO 7498-2

Powszechnie zaakceptowanym standardem w bezpieczeństwie komputerowym jest ISO 7498-2 Architektura Bezpieczeństwa (ang. *Security Architecture*), część 2 z ISO 7498, który zawiera opis podstawowego modelu referencyjnego OSI [3]. W standardzie tym zdefiniowano następujące podstawowe usługi bezpieczeństwa:

- Uwierzytelnianie (ang. authentication) – określa możliwość weryfikacji autentyczności komunikatu. Dzielimy ją na dwie kategorie:
  - uwierzytelnianie jednostki (ang. *entity authentication*) – zweryfikowanie zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych,
  - uwierzytelnianie pochodzenia (ang. *origin authentication*) – zweryfikowanie źródła odebranych danych.
- Kontrola dostępu (ang. *access control*) – zapobieganie nieautoryzowanemu dostępowi do zasobów, włączając w to zapobieganie wykorzystaniu zasobów w nieautoryzowany sposób.
- Poufność danych (ang. *data confidentiality*) – informacja nie jest dostępna, ani nie zostanie ujawniona nieautoryzowanym osobom, jednostkom lub procesom.
- Integralność danych (ang. *data integrity*) – dane nie zostały zmodyfikowane lub zniszczone w nieautoryzowany sposób.
- Niezaprzeczalność (ang. *non-repudiation*) – brak możliwości wyparcia się jednego z uczestników komunikacji swego uczestnictwa w wymianie danych.
- Dostępność (ang. *availability*) – właściwość bycia osiągalnym oraz użytecznym zawsze, gdy jest takie zapotrzebowanie.

2.2. Bezpieczeństwo według FIPA

W 2002 roku FIPA opublikowała dokument opisujący standard bezpieczeństwa w systemach wieloagentowych [2]. Informacje w nim zawarte są niestety jedynie pobieżne i przedstawiają tylko pewne zalecenia dotyczące bezpieczeństwa. Zgodnie z informacjami zawartymi w tym dokumencie, FIPA nie dysponuje żadnym silnym modelem bezpieczeństwa dla agentów. Wynika to przede wszystkim z tego, że problem, gdzie i jak dodać zabezpieczenia do systemu opartego na FIPA ACL, jest niezwykle złożony. Ustalono jednak, że system może zostać wzbogacony o wymagania bezpieczeństwa na poziomach innych niż ACL. W dokumencie tym przedstawionych zostało kilka kluczowych wymagań dla bezpieczeństwa systemu wieloagentowego. Są to:

- Identyfikacja – zdolność do określenia tożsamości obiektów w systemie. Przez identyfikację obiektu, inny obiekt, który się z nim komunikuje, może określić, jakie polityki są znaczące przy interakcji z tym obiektem. Identyfikacja opiera się na referencjach, które są weryfikowane przez CA (ang. *Credential Authority*).
- Kontrola dostępu – na podstawie tożsamości obiektu określa, które polityki zastosować do danego obiektu. Polityki te mogą zostać wykorzystane do zarządzania zasobami, do określenia typu dostępu, do określenia poleceń, jakie mogą być wywoływane, lub do kontrolowania innych aspektów związanych z dostępem.
- Integralność – możliwość określenia, czy fragment aplikacji, wiadomości lub innych danych nie został zmodyfikowany w trakcie przesyłania od nadawcy do odbiorcy. Integralność jest zwykle realizowana przez wykorzystywanie danych podpisanych cyfrowo, które są następnie sprawdzane przez odbiorcę. Innym mechanizmem wykorzystywanym w tym celu jest m.in. zastosowanie funkcji haszujących.
- Poufność – możliwość stwierdzenia, że tylko osoby uprawnione do odczytu aplikacji, wiadomości lub innych danych, będą mogły je odczytać. Dla wszystkich pozostałych informacje są niemożliwe do odczytania. Poufność często jest realizowana przez zastosowanie szyfrowania danych lub wykorzystywanie szyfrowanych kanałów komunikacyjnych.

2.3. Realizacja bezpieczeństwa w implementacji JADE-S

JADE (ang. *Java Agent Development Framework*) jest oprogramowaniem w całości zaimplementowanym w Javie. Jego zadaniem jest ułatwienie implementacji systemów wieloagentowych przez dostarczenie dużej liczby bibliotek zgodnych ze standardami FIPA. JADE-S jest dodatkiem do JADE, który zapewnia wsparcie w zakresie bezpieczeństwa systemów wieloagentowych [4]. Pozwala on chronić systemy wieloagentowe oparte na JADE przeciw

różnym atakom. Dodatek ten zapewnia realizację podstawowych aspektów bezpieczeństwa: uwierzytelnianie, kontrolę dostępu, integralność oraz tajność wiadomości.

3. Protokół interakcji do negocjacji poziomu zabezpieczeń

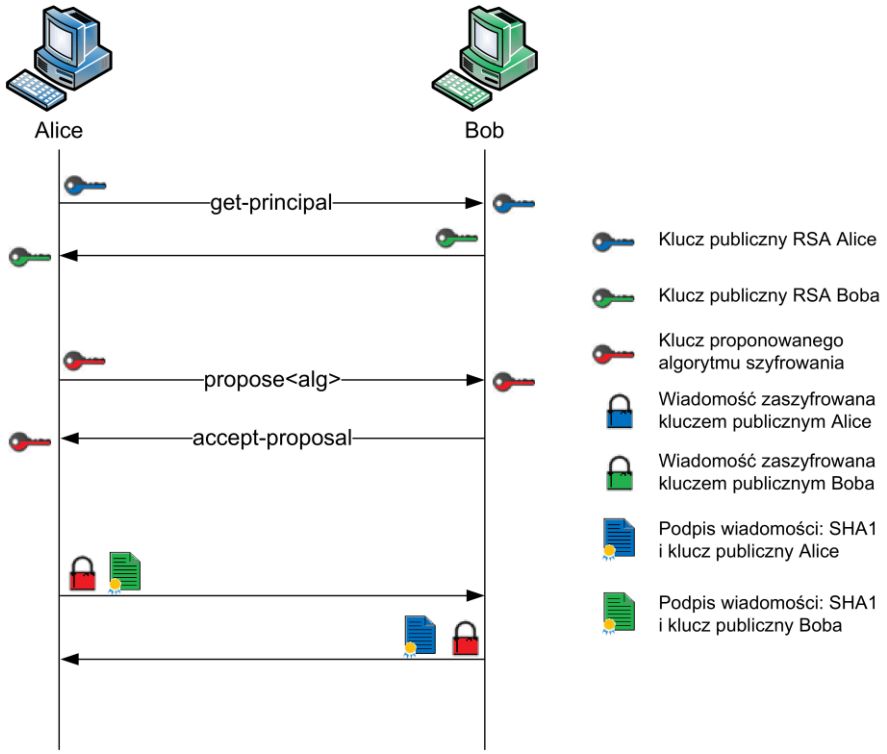
Bezpieczeństwo przesyłanych wiadomości zostało uznane za najistotniejszy element tej pracy. Właśnie ta funkcjonalność jest kluczowa pod względem problemów poufności, autentyczności i niezaprzeczalności w systemach wieloagentowych. Przez realizację szyfrowania i podpisywania mogą zostać rozwiązane wszystkie wspomniane problemy bezpieczeństwa. Dodatek JADE-S dostarcza mechanizmów pozwalających na: uwierzytelnianie agentów, kontrolę dostępu, zarówno na poziomie platformy, jak i kontenera, oraz na bezpieczeństwo przesyłanych danych. Bezpieczeństwo przesyłanych danych zapewnione jest oprzez szyfrowanie wiadomości za pomocą różnych szyfrów (RSA, DSA, AES, Blowfish, DES, TripleDES) i podpisywanie wiadomości [12]. Podpisywanie wiadomości w testowanej aplikacji jest zapewniane za pomocą algorytmu SHA1-RSA.

Ponieważ każdy z agentów może posiadać różne preferencje dotyczące metod szyfrowania wiadomości, rozważamy negocjację poziomu zabezpieczeń w komunikacji między agentami. Dzięki takiemu rozwiązaniu, w środowisku rozproszonym, każda para agentów będzie mogła komunikować się bezpiecznie, zgodnie z wynegocjowanymi algorytmami bezpieczeństwa. Pełny opis pozostałych zagadnień związanych z bezpieczeństwem w systemach wieloagentowych znajduje się w pracy [13].

3.1. Negocjacje poziomu zabezpieczeń

Negocjacje poziomu zabezpieczeń sprowadzają się do ustalenia metody szyfrowania, jaka będzie wykorzystywana w ich dalszej komunikacji. Na początku, pomiędzy agentami następuje wymiana kluczy publicznych RSA, wygenerowanych podczas uruchamiania agenta. Informacje te przesyłane są w sposób niezabezpieczony. Jest to jedyna wada utworzonego rozwiązania, gdyż klucze mogą zostać podmienione za pomocą ataku man-in-the-middle. Następnie odbywa się właściwa negocjacja poziomu zabezpieczeń. Innym rozwiązaniem jest przesyłanie kluczy publicznych do zaufanych agentów. Agenty chcące negocjować poziomy zabezpieczeń, muszą korzystać z ontologii *SecurityNegotiation*, która dostarcza odpowiednich pojęć służących poprawnemu zrozumieniu poszczególnych etapów negocjacji. Każda wiadomość, która zawiera propozycję negocjacji zabezpieczeń, jest zbudowana następująco. Jej performatywa, *propose*, informuje o tym, że jest to wiadomość, która określa rozpoczęcie procesu negocjacji poziomu zabezpieczeń. Ontologia, z której korzysta agent, to *SecurityNegotiation*. Ontologia ta definiuje

odpowiednią klasę *SecurityDefinition*, która zawiera odpowiednie do tej negocjacji informacje. Przesłany w treści komunikatu obiekt klasy *SecurityDefinition* zawiera nazwę algorytmu szyfrowania (dopuszczalna jest także wartość NONE, oznaczająca brak szyfrowania) oraz klucz powiązany z proponowanym algorytmem. Jeśli agent, z którym nawiązano połączenie, zgadza się na dalszą konwersację (przesyła komunikat *accept-propose*), wówczas dalsza część konwersacji jest szyfrowana za pomocą przesłanego klucza nadawcy.



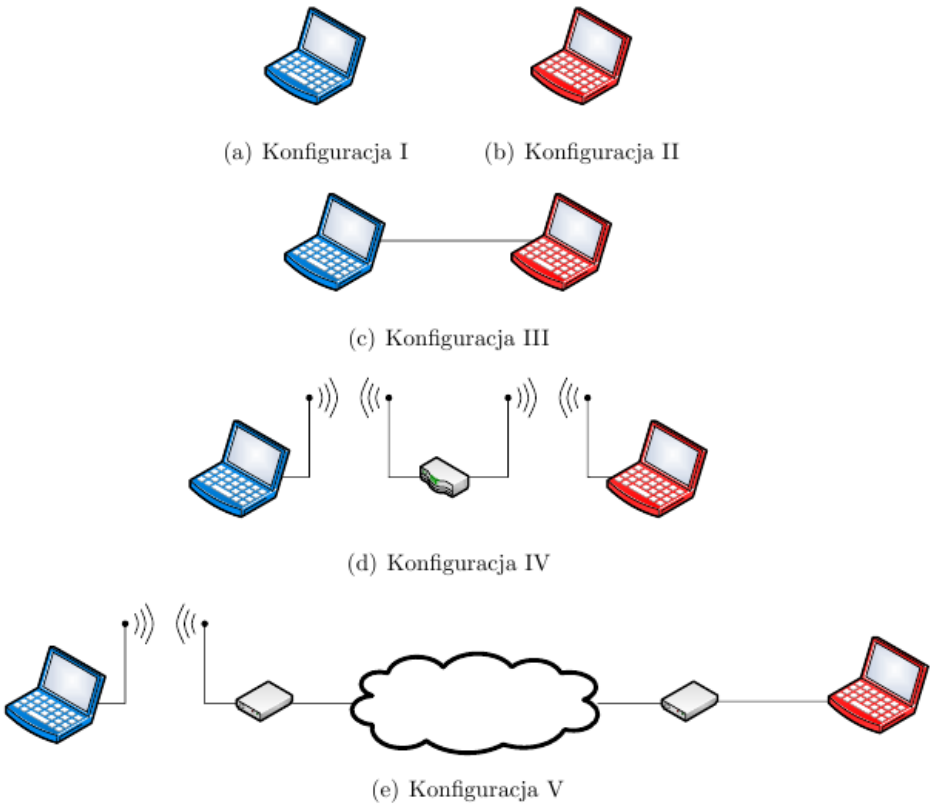
Rys. 1. Zaproponowany przebieg bezpiecznej komunikacji z zastosowanym protokołem negocjacji poziomu zabezpieczeń

Fig. 1. Proposed course of the secure communication with interaction protocol for the security level negotiations applied

4. Ocena rozwiązania

Możliwość szyfrowania i podpisywania wiadomości zdecydowanie zwiększa bezpieczeństwo w systemie wieloagentowym. Wprowadzenie takich modyfikacji niesie jednak ze sobą znaczące konsekwencje. W poniższym rozdziale zaprezentowane zostały testy zaimplementowanego rozwiązania. Duży nacisk położony został na zbadanie wpływu dodanych funkcjonalności na czas przesyłania komunikatów oraz ich wielkości. Dane te zostały porównane z wynikami testów przeprowadzonych na systemie bez zabezpieczeń. Dodatkowo przeprowadzone zostały testy lokalne, które przedstawiały uwierzytelnianie zakończone sukcesem, uwierzytelnianie zakończone niepowodzeniem, prawidłowe wykorzystanie uprawnień z kon-

troli dostępu, nadużycie uprawnień z kontroli dostępu oraz zbadano średni czas szyfrowania wiadomości w zależności od jej wielkości i wykorzystywanego algorytmu. Dokładne wyniki testów można znaleźć w pracy [13].



Rys. 2. Konfiguracje środowisk testowych
Fig. 2. Configurations of the test environments

4.1. Środowisko testowe

Aplikacja, w której testowano nakłady czasowe związane z zapewnieniem wymaganego poziomu bezpieczeństwa, to wieloagentowa platforma handlu wielotowarowego, opisana w pracach [5,10]. Jest to o tyle istotne, że systemy handlowe są predysponowane do zapewnienia wysokiego poziomu bezpieczeństwa wymienianych informacji. Jednak pewne procesy wymiany handlowej powinny zachodzić szybko. Przykładowo, procesy handlu w segmencie czasu rzeczywistego RCR na rynku bilansującym energii elektrycznej, gdzie czas wymagany na przesłanie wiadomości o ofertach, przetworzenie danych przez jednostkę centralną (uwzględniające rozwiązanie złożonych zadań optymalizacyjnych) oraz odesłanie danych o alokacji ofert do każdego podmiotu, powinien trwać kilka minut. Innym przykładem jest zastosowanie metodyki wieloagentowej do bilansowania niedoborów i nadmiarów energii w mikrosieciach, gdzie czas przesyłania danych jest krytyczny, ze względu na czas zbilansowania energii [7]. Tak więc czas, wymagany na dodatkowe operacje związane z zapewnieniem bezpieczeństwa, powinien być możliwie krótki.

Testy zaimplementowanego rozwiązania polegały na wygenerowaniu losowej wiadomości o odpowiedniej długości oraz przesłaniu jej do odbiorcy. W każdym przypadku przesyłanych było 1000 takich wiadomości. Czasy były mierzone z dokładnością do milisekund, co jest bardzo ważne z perspektywy uzyskanych wyników. Wszystkie testy zostały zrealizowane w pięciu konfiguracjach (patrz rys. 2).

Poszczególne maszyny były skonfigurowane w następujący sposób. Komputer A: procesor: Intel(R) Core(TM) 2 Duo CPU T6600 @ 2.20GHZ 2,20 GHz; zainstalowana pamięć (RAM): 4,00 GB; system operacyjny: Windows 7 Professional, 64-bitowy system operacyjny. Komputer B: procesor: Intel(R) Pentium(R) M 1,60 GHz; zainstalowana pamięć (RAM): 1,50 GB; system operacyjny: Debian 6.0.2.1 (Kernel Linux 2.6.32-5-686).

4.2. Wyniki testów

Na podstawie przeprowadzonych testów można stwierdzić, że czasy przesyłania wiadomości w znacznym stopniu zależą od konfiguracji, w jakiej znajdują się komputery. W przypadku testów realizowanych lokalnie, czasy te były krótkie i zależały jedynie od zasobów komputera. W przypadku testów sieciowych dochodziły dodatkowe czynniki, wynikające z przepustowości sieci i ilości routerów na trasie z komputera źródłowego do docelowego. W konfiguracji V okazało się, że pomiędzy maszynami A i B znajduje się 7 routerów. Na podstawie zebranych danych można również zauważyć, że w konfiguracji III, w której komputery A i B były połączone za pomocą złącza RJ45, uzyskano bardzo zbliżone wyniki, jak w konfiguracji II, gdzie symulacja była przeprowadzana lokalnie na komputerze B. Świadczy to o tym, że przepustowość kabla była zbliżona do możliwości słabszego z dostępnych komputerów. Oczywiście, zgodnie z oczekiwaniami, wyniki były gorsze w przypadku wykorzystania sieci opartej na WiFi i zdecydowanie gorsze w sieci rozległej w konfiguracji V. W tabeli 1 przedstawiono szczegółowe wyniki testów przesyłania wiadomości o różnym rozmiarze, szyfrowanych algorytmem RSA. Dla wzrostu rozmiaru komunikatu czas jego przesyłania rośnie. Znaczący wzrost czasu przesyłania wiadomości zaszyfrowanej i niezaszyfrowanej można zauważyć dla większych rozmiarów komunikatu. Uśredniony dla dwóch ostatnich kolumn nakład na szyfrowanie wiadomości wyniósł około 32%. Zakładając, że będziemy się zazwyczaj spotykać z takim właśnie rozmiarem wiadomości, należy stwierdzić, że narzut 32% na czas przesyłanych komunikatów jest akceptowalny, zważając na potencjalne niebezpieczeństwo, jakim obciążone jest przesyłanie niezaszyfrowanych komunikatów.

Wyniki testów wydajnościowych przedstawiono w tabeli 1. W poszczególnych kolumnach znajdują się wyniki dotyczące wielkości zawartości przesyłanego komunikatu (w znakach). Dane zawierają czas komunikacji bez szyfrowania/z szyfrowaniem. Wyniki zastały podane w milisekundach.

Tabela 1

Wyniki testów wydajnościowych dotyczących czasu trwania przesyłania wiadomości

	10	100	1 000	10 000	100 000
Konf. I	0,94/1,10	0,90/0,91	0,90/1,10	1,26/1,21	4,06/5,71
Konf. II	1,09/1,21	0,82/1,04	0,87/1,09	1,46/1,86	6,41/9,85
Konf. III	1,25/1,86	1,16/1,65	1,25/1,73	1,81/2,51	6,86/9,73
Konf. IV	5,41/5,54	6,83/6,04	5,26/10,33	18,57/25,22	173,8/213,2
Konf. V	19,11/30,76	17,72/26,05	20,25/32,35	67,75/91,30	475,6/623,9

5. Podsumowanie

Problemy poufności, autentyczności i niezaprzeczalności w systemach wieloagentowych są tematem bardzo rozległym. Zbudowanie w pełni bezpiecznego systemu jest zadaniem trudnym. Wykorzystanie wszystkich przedstawionych w niniejszej pracy metod zabezpieczenia daje jednak solidne podstawy do stworzenia takiej aplikacji. Wpływ zaimplementowanego rozwiązania na szybkość i wielkość przesyłanych danych jest do zaakceptowania, dzięki czemu, to po stronie użytkownika leży podjęcie decyzji, co jest dla niego ważniejsze – szybkość komunikacji czy jej bezpieczeństwo. Jednak biorąc pod uwagę średnie wydłużenie czasu komunikacji o 32%, zapewnienie bezpieczeństwa przesyłanych komunikatów nie jest obciążone dużymi narzutami czasowymi. Agenty są w stanie prowadzić swobodną komunikację oraz przeprowadzać negocjacje poziomu bezpieczeństwa. Przeprowadzone testy udowodniły, że zbudowane rozszerzenie rozwiązuje podstawowe problemy poufności, autentyczności i niezaprzeczalności. Przez wykorzystanie plików polityk realizujących kontrolę dostępu, mechanizmów uwierzytelniania, podpisywania i szyfrowania wiadomości, stworzony został system, który posiada niezbędne cechy bezpiecznego systemu wieloagentowego. Zaproponowany protokół negocjacji poziomu zabezpieczeń dostarcza autonomicznym agentom nowej funkcjonalności, pozwalając im na swobodny dobór algorytmów szyfrowania.

BIBLIOGRAFIA

1. Foundation for Intelligent Physical Agents, http://fipa.org/.
2. FIPA MAS Security white paper, 2002.
3. International Standard ISO 7498-2, 1989.
4. JADE Board. JADE Security Guide, 2005.

5. Kaleta M., Pałka P., Toczyłowski E., Traczyk T.: Electronic Trading on Electricity Markets within a Multi-Agent Framework. Lecture Notes in Artificial Intelligence, Vol. 5796, 2009, s. 788÷799.
6. Kaleta M., Pałka P., Toczyłowski E., Traczyk T.: Wykorzystanie modelu M3 w implementacji wieloagentowej platformy wymiany wielotowarowej w środowisku AIMMS, Studia Informatica, Vol. 31, No. 2B (90), Wydawnictwo Politechniki Śląskiej, Gliwice 2010, s. 181÷192.
7. Nahorski Z., Pałka P., Stańczak J., Radziszewska W.: Wieloagentowa metodyka zarządzania niedoborami i nadmiarami energii w sieciach dystrybucyjnych. Rynek Energii, Vol. 1(92), 2011, s. 22÷27.
8. McArthur S., Davidson E., Catterson V., Dimeas A., Hatziagyriou N., Ponci F., Funabashi T.: Multi-Agent Systems for Power Engineering Applications – Part I: Concepts, Approaches and technical Challenges. IEEE Transactions on Power Systems, Vol. 22(4), 2007, s. 1743÷1752.
9. McArthur S., Davidson E., Catterson V., Dimeas A., Hatziagyriou N., Ponci F., Funabashi T.: Multi-Agent Systems for Power Engineering Applications – Part II: Technologies, Standards and Tools for Building Multi-agent Systems. IEEE Transactions on Power Systems, Vol. 22(4), 2007, s. 1753÷1759.
10. Pałka P.: Multilateral negotiations in distributed, multi-agent environment. Lecture Notes in Computer Science, Vol. 6923, 2011, s. 80÷89.
11. Pałka P., Traczyk T., Wilk R.: Scentralizowane negocjacje multilateralne w handlu wielotowarowym z wykorzystaniem standardów M3 i ebXML. Studia Informatica, Vol. 32, Wydawnictwo Politechniki Śląskiej, Gliwice 2011, s. 455÷466.
12. Pfleeger C. P., Pfleeger S. L.: Security in computing. Prentice Hall Professional, 2003.
13. Strzałek M.: Problemy poufności, niezaprzeczalności oraz autentyczności w systemach wieloagentowych. Praca inżynierska, Politechnika Warszawska, Warszawa 2011.
14. Woolridge M.: Introduction to multiagent systems. John Wiley & Sons, 2001.

Wpłynęło do Redakcji 10 stycznia 2012 r.

Abstract

Multi-agent systems are increasingly used in various areas of our lives. They are implemented, as simulation, diagnostic, monitoring, and control systems. Wide range of potential applications is also the trading systems that operate either in a centralized configuration (auc-

tion systems) and distributed systems (negotiating). Multi-agent system architecture, which uses the Internet as the main channel of communication, is a potentially weak point of the whole system security. Unauthorized access and interference with the specialized resources of the system can cause enormous losses not limited to financial. It is therefore necessary to ensure an adequate level of security of transactions taking place in multi-agent system. Widely accepted standard in computer security is ISO 7498-2, which defines basic security services: authentication, access control, data confidentiality, integrity, non-repudiation, and availability. Work describes the method to provide with appropriate levels of confidentiality, non-repudiation of sending messages and their authentication. Moreover, the possibility of negotiating an appropriate level of security and encryption algorithm is considered.

Adresy

Marcin STRZAŁEK: Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej, ul. Nowowiejska 15/19, 00-665 Warszawa, Polska, Marcin.Strzalek@gmail.com.
Piotr PAŁKA: Politechnika Warszawska, Instytut Automatyki i Informatyki Stosowanej, ul. Nowowiejska 15/19, 00-665 Warszawa, Polska, P.Palka@ia.pw.edu.pl.