XLI Konferencja Naukowo - Techniczna

GDAŃSKIE DNI ELEKTRYKI' 2016

Stowarzyszenie Elektryków Polskich, Oddział Gdańsk
Gdańsk, 28 października 2016

KONCEPCJA PLATFORMY WYMIANY INFORMACJI O INCYDENTACH CYBERBEZPIECZEŃSTWA DLA KRAJOWEGO SYSTEMU ELEKTROENERGETYCZNEGO

Rafał LESZCZYNA[1], Robert MAŁKOWSKI[2], Andrzej AUGUSIAK[2]

1) Politechnika Gdańska, Wydział Zarządzania i Ekonomii
e-mail: rafal.leszczyna@pg.gda.pl
2) Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
e-mail: robert.malkowski@pg.gda.pl, andrzej.augusiak@pg.gda.pl

Streszczenie: Artykuł opisuje wybrane zagadnienia związane z cyberbezpieczeństwem w sektorze elektroenergetyki. Jednym z elementów zapewniania bezpieczeństwa sieci elektroenergetycznej jest efektywna wymiana informacji o incydentach bezpieczeństwa. W jej ramach wszystkie zaangażowane podmioty systemu elektroenergetycznego, tj.: elektrownie, operatorzy systemów przesyłowych, operatorzy systemów dystrybucyjnych, dostawcy rozwiązań bezpieczeństwa, organizacje standaryzujące, a także centra badawcze i środowiska akademickie, powinni móc dzielić się między sobą informacjami dotyczącymi incydentów bezpieczeństwa w systemie elektroenergetycznym. W referacie opisano ideę zastosowania do tego celu systemów wieloagentowych. Ponieważ sytuacja formalno-prawna podmiotów związanych z systemem elektroenergetycznym jest bardzo złożona, prowadzenie prac badawczo-rozwojowych w zakresie cyberbezpieczeństwa są znacznie ograniczone, a niekiedy niemożliwe. W referacie przedstawiono możliwości badawcze jakie w tym zakresie oferuje laboratorium LINTE^2.

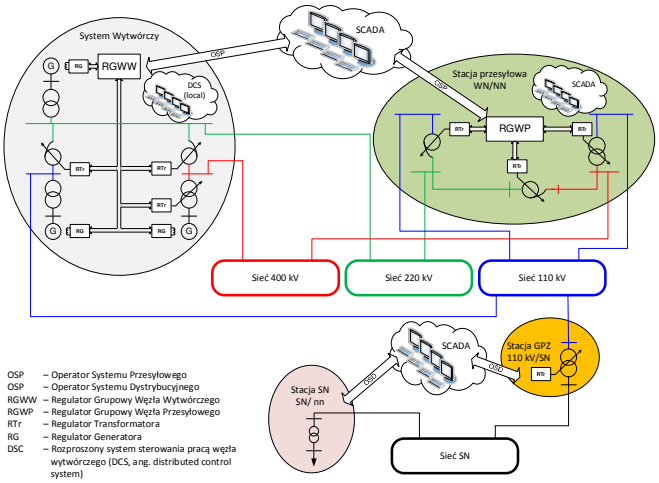
Słowa kluczowe: sieć elektroenergetyczna, bezpieczeństwo cybernetyczne, wymiana informacji, systemy wieloagentowe laboratorium systemów elektroenergetycznych

1. WPROWADZENIE

Cyberbezpieczeństwo jest definiowane jako zdolność do ochrony cyberprzestrzeni przed cyberatakami [8] i jest nierozerwalnie związane z bezpieczeństwem informacji tj. takim stanem informacji, w którym zachowana jest jej poufność, integralność i dostępność [8], [9].

Jedną z najbardziej krytycznych infrastruktur jest system elektroenergetyczny. Istnieje bowiem silna zależności pomiędzy ciągłością zasilania a poprawnym funkcjonowaniem pozostałych infrastruktur. Tym samym, system elektroenergetyczny wraz z całą towarzyszącą mu infrastrukturą teletransmisyjną oraz systemami sterowania i wymiany danych (SCADA, DCS) należy uznać za najbardziej zagrożone sabotażem i atakami cybernetycznymi.

Oprócz działań związanych z nieupoważnionym dostępem do poufnych danych, w tym do informacji o transakcji finansowych prowadzonych na wolnym rynku energii, danych osobowych i finansowych klientów spółek dystrybucyjnych, będą to przede wszystkim działania wykorzystujące funkcje systemów komputerowych. Funkcje takie spełniają komputerowe systemy sterowania stosowane w elektrowniach, stacjach elektroenergetycznych oraz w centrach dyspozycji mocy oraz centrach nadzoru eksploatacyjnego. Uproszczony schemat powiązań funkcjonalnych pomiędzy elementami systemu elektroenergetycznego z wykorzystaniem systemów teleinformatycznych oraz IT rys.1.



Rys.1. Uproszczony schemat powiązań funkcjonalnych pomiędzy elementami systemu elektroenergetycznego z wykorzystaniem systemów teleinformatycznych [34]

Przejęcie kontroli nad systemami sterowania może stanowić bezpośrednie zagrożenie dla życia lub zdrowia obsługi. Wzrasta również ryzyko: skażenia środowiska, uszkodzenia urządzeń i układów systemu elektroenergetycznego, czy też przerw w dostawie energii elektrycznej.

2. ZASTOSOWANIE SYSTEMÓW WIELOAGENTOWYCH W ELEKTROENERGETYCE

Ewolucja systemów elektroenergetycznych w kierunku struktur silnie zdecentralizowanych wymaga nowych metod ich nadzoru i kontroli dopasowanych do rozproszonego charakteru tworzących je podsystemów i obiektów. Metody te powinny posiadać zdolność pracy po podziale systemu na wyspy oraz wymiany informacji przy ograniczonym paśmie komunikacyjnym. Muszą być one również odporne m.in. na

brak ciągłości zasilania w energię. Odpowiedź na te wymagania przynoszą tzw. systemy wieloagentowe (ang. *multi-agent systems*) [1].

Agenty to programy komputerowe, reprezentujące użytkownika w rzeczywistości wirtualnej i wykonujące wyznaczone przez niego zadania [2], [3]. Agenty potrafią działać samodzielnie, bez kontroli użytkownika, w czym pomagają im wbudowane mechanizmy wnioskowania oraz możliwość komunikacji z innymi agentami [2], [3]. Specjalnym rodzajem agentów są agenty migrujące (ang. *mobile agents*), posiadające oprócz wymienionych wyżej cech także zdolność przemieszczania się z jednego komputera na drugi [4], [5]. Środowiska złożone z wielu agentów to systemy wieloagentowe [1].

Agentów najczęściej opisuje się poprzez ich *stan* i *zachowanie*. Stan odnosi się do danych (zmiennych i wartości statycznych) opisujących agenta oraz przenoszone przez niego dane. Natomiast zachowanie jest zbiorem czynności wykonywanych przez agenta w celu osiągnięcia *celu* zadanego mu przez użytkownika. Zachowanie reprezentuje zadanie wykonywane przez agenta [6].

Aby osiągnąć zadany cel, agenty migrują z jednej lokalizacji sieciowej (tzw. *kontenera*) do kolejnej, począwszy od tzw. *stacji bazowej*. Sekwencja kontenerów pokonywana podczas "wycieczki" nazywana jest *marszrutą* (ang. *route*).

Systemy wieloagentowe cechują się mniejszymi opóźnieniami i krótszym czasem przetwarzania oraz umożliwiają komunikację asynchroniczną. Jednocześnie zapewniają równomierne rozłożenie obciążenia związanego z przetwarzaniem i są bardzo elastyczne, ponieważ pojedyncza architektura może służyć do różnych zastosowań. Systemy te cechują się również łatwością w instalacji oraz wysoką dostępnością [7]–[9].

Charakterystyki te doskonale odpowiadają wymaganiom stawianym przez współczesne rozproszone systemy elektroenergetyczne. Technologia agentowa spotkała się z dużym zainteresowaniem w dziedzinie elektroenergetyki, a oparte o nie rozwiązania próbuje się zastosować w różnych jej obszarach.

Dla przykładu Ren i in. zaproponowali system wieloagentowy do efektywnego zarządzania infrastrukturami elektroenergetycznymi oraz przywracania stanu sprzed awarii [10]. W działaniu systemu wykorzystano mechanizm dynamicznego formowania zespołu z adaptacyjną strukturą koordynacyjną, która dynamicznie zarządza agentami.

Manickam i in. zaprezentowali samo-rozwijającą się architekturę wieloagentową do monitorowania i ochrony systemów elektroenergetycznych [11]. Architektura ta wykorzystuje systemy głosujące do zwiększenia odporności na awarie. Inną propozycją dotyczącą bezpieczeństwa sieci elektroenergetycznej jest *specjalny system ochrony* (ang. *special protection system – SPS*) autorstwa Rossa i in. [12]. System ten, w przeciwieństwie do tradycyjnych specjalnych systemów ochrony jest zdecentralizowany, aby umożliwić lepsze rozpoznawanie i odpowiadanie na incydenty.

Pozostałe zastosowania agentów w systemie elektroenergetycznym dotyczą kontroli napięcia (np. system czasu rzeczywistego kontroli stacji bazowych [13]), czy modelowania środowiska sieci elektroenergetycznej [14]. Szerokie badania poświęcono również działaniu i kontroli mikrosieci [15]–[18] oraz bezprzewodowym sieciom sensorów [19]. W tym ostatnim agenty wykorzystywane są do wysokopoziomowego wnioskowania i nadzoru. Ciekawą odpowiedzią na niektóre wyzwania w sieciach elektroenergetycznych są rozwiązania biologicznie inspirowane, wykorzystujące podobieństwo agentów do organizmów żywych [20].

Architektura anonimowości przedstawiona w artykule jest nową propozycją odnoszącą się do dopiero rozwijanej dziedziny zastosowań w systemach elektroenergetycznych, tj. wymiany informacji dotyczących bezpieczeństwa. Oryginalną koncepcją rozwiązania jest również zastosowanie agentów do zagadnień anonimowości związanych z tego rodzaju komunikacją.

3. ANONIMOWA WYMIANA INFORMACJI W SYSTEMACH ELEKTROENERGETYCZNYCH

W zapewnianiu bezpieczeństwa sieci elektroenergetycznej niezbędna jest efektywna i nieskrępowana wymiana informacji o incydentach bezpieczeństwa. W jej ramach wszyscy zaangażowani interesariusze tzn. elektrownie, operatorzy systemów przesyłowych, operatorzy systemów dystrybucyjnych, dostawcy rozwiązań bezpieczeństwa, organizacje standaryzujące a także centra badawcze i środowiska akademickie dzielą się między sobą informacjami dotyczącym bezpieczeństwa w systemie elektroenergetycznym. Informacje te to m.in. alarmy o nowych zagrożeniach, wykryte słabości systemów, środki bezpieczeństwa itd.

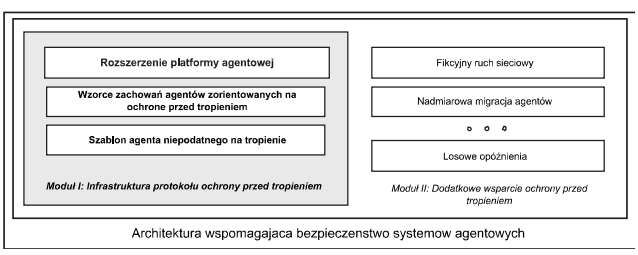
W wielu sytuacjach są to dane wrażliwe, których udostępnianie nie leży w interesie danego interesariusza. Przykładowo, trudnością dla zarządu elektrowni będzie podzielenie się informacjami o przebiegu i efektach cyberataku, którego celem stał się zarządzany przez niego obiekt. Stanie się to jeszcze trudniejsze, gdy odbiorcami wiadomości są konkurencyjni wytwórcy energii elektrycznej. Z tego po powodu niezwykle ważne jest zapewnienie anonimowości nadawców wrażliwych informacji [9].

W kolejnych sekcjach artykułu zaprezentowano agentową architekturę anonimowości, która szczególnie odpowiada rozproszonej i zdecentralizowanej strukturze współczesnego systemu elektroenergetycznego i zapewnia wybrany poziom bezpieczeństwa.

4. ARCHITEKTURA ANONIMOWOŚCI

Architektura składa się z dwóch modułów (rys. 2):

- Moduł I: Infrastruktura protokołu ochrony przed tropieniem – służący do ukrycie adresu stacji bazowej agentów,
- Moduł II: Dodatkowe wsparcie ochrony przed tropieniem – chroniący agenty przed analizą ruchu sieciowego.



Rys.2. Dwumodułowa architektura wspomagająca bezpieczeństwo (anonimowość) systemów agentowych

Moduł I zapewnia funkcjonalność protokołu ochrony przed tropieniem, z tą zaletą, że nie wprowadza ograniczeń wobec agentów samodzielnie ustalających trasę własnej

wędrówki [21]. Moduł I stanowi rdzeń architektury, który z założenia ma być otoczony opcjonalnymi elementami Modułu II. Reprezentuje on infrastrukturę implementującą protokół ochrony przed tropieniem

Moduł II odnosi się do złożonego zagadnienia rozszerzonej ochrony przed tropieniem. Adresuje mniej prawdopodobne ataki analizy ruchu sieciowego oraz śledzenie agentów na podstawie interpretowania przenoszonych przez nich danych. Ponieważ jego całościowe wdrożenie może wymagać znaczących nakładów na narzuty obliczeniowe i komunikacyjne, powinno się go raczej implementować w zakresie wynikającym z analizy zysków do nakładów [22].

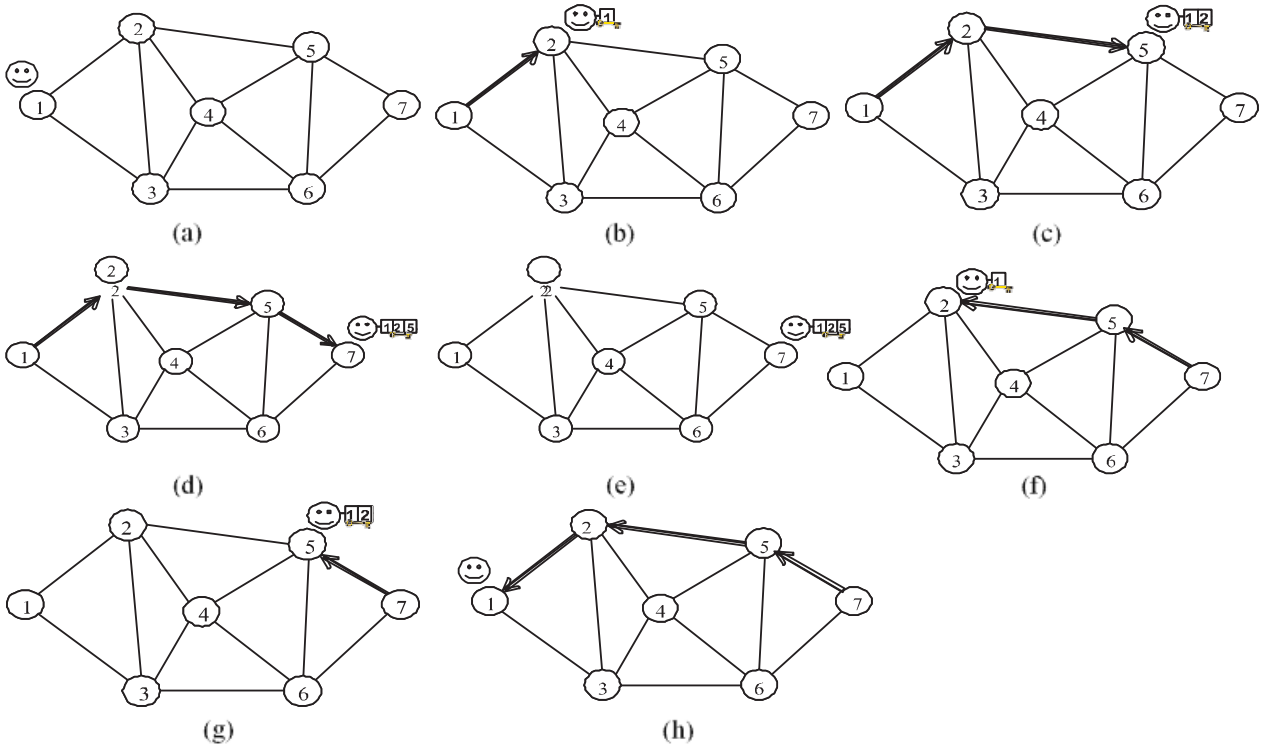
4.1 Założenia

Architektura powinna zapewnić standardowy poziom ochrony przed tropieniem (poziom ustanowiony przez większość protokołów ochrony przed tropieniem), gwarantując jednocześnie brak ograniczeń samodzielności agentów. *Cel* stawiany architekturze został sformułowany następująco: *Architektura powinna umożliwić właścicielom agentów ukrycie (uczynienie nieczytelnym dla osób niepowołanych) adresu stacji bazowej agenta. Operacja ta nie powinna ograniczać samodzielności agenta w planowaniu i realizowaniu migracji. Mimo ukrycia adresu agent powinien być zdolny do powrotu do stacji bazowej*.

Opisany poziom bezpieczeństwa powinien zostać zagwarantowany przy *modelu atakującego*, który uwzględnia wszystkie znane rodzaje atakujących, a w tym [23]:

- Atakujących *wewnętrznych* / *zewnętrznych*, posiadających kontrolę nad kontenerem, bądź tylko medium komunikacyjnym łączącym kontenery [24].
- Atakujących *wszechobecnych* / *k-podsłuchujących*, mogących uzyskać dostęp do wszystkich kontenerów lub do ich k-podzbioru. W szczególności *pojedynczy* atakujący to taki, który opanował tylko jeden kontener [25].
- Atakujących *aktywnych* / *pasywnych*, potrafiących modyfikować obliczenia i dane (dodając i usuwając), lub jedynie czytać („podsłuchiwać") dane [24].
- Atakujących *adaptacyjnych* / *statycznych*, mogących lub nie – zmieniać kontrolowane zasoby podczas działania protokołu bezpieczeństwa [24], [26]. Adaptacyjni atakujący mogą na przykład „podążać" za agentami [24].
- Atakujących *hybrydowych*, łączących cechy wybranych pozostałych typów atakujących, lub będących *sojuszami* atakujących, współpracujących ze sobą, aby osiągnąć wspólny cel. Przykładami są *zewnętrzni-aktywni* atakujący, czy *współpracujący zewnętrzny i wewnętrzny* atakujący. Syverson i inni [25], rozróżniają między *wielokrotnym atakującym* i *wędrownym atakującym*, czyli: k-podsłuchującym statycznym i k-podsłuchującym adaptacyjnym atakującym.

Zdefiniowano również model środowiska, dla którego architektura jest dedykowana i w którym powinna realizować wymagany cel. Zgodnie z tym modelem architektura powinna być rozszerzeniem dowolnej platformy agentowej zgodnej ze specyfikacją FIPA (ang. the Foundation for Intelligent Physical Agents) [27]. FIPA jest organizacją standaryzującą należącą do IEEE Computer Society. Od roku 1997 FIPA opublikowała dwadzieścia trzy standardy opisujące różne aspekty technologii agentowej takie jak komunikacja między agentami, zarządzanie agentami, czy agentowa architektura abstrakcyjna.



Rys.3. Protokół ochrony przed tropieniem (a) – (d) podczas migracji agenta, na każdym kolejnym kontenerze odwiedzanym przez agenta, szyfrowany jest identyfikator poprzednio odwiedzonego kontenera i umieszczany na stosie; (e) – (h) następnie identyfikatory zdejmowane kolejno ze stosu i odszyfrowywane, pozwolą wrócić agentowi do stacji bazowej.

Dodatkowo sformułowano założenia, które muszą być spełnione do prawidłowego działania architektury. Założenia te dotyczą dystrybucji kluczy kryptograficznych, właściwości funkcji kryptograficznych oraz izolacji kontenerów i udostępniania informacji o poprzednim kontenerze [23].

4.2 Protokół ochrony przed tropieniem

Funkcjonalność protokołu ochrony przed tropieniem zaadaptowana do środowisk agentowych implementowana jest w Module I architektury anonimowości. W ramach specyfikacji architektury, przedstawiono formalną definicję protokołu w postaci pseudokodu.

W uproszczeniu, działanie protokołu opiera się na zasadzie, że podczas wędrówki agenta, na każdym kolejnym, nowym kontenerze szyfrowany jest identyfikator poprzednio odwiedzonego kontenera. Szyfrowanie to wykonywane jest przez kontener, a symetrycznie zaszyfrowany identyfikator umieszczany jest w kolejce LIFO znajdującej się w danych agenta. Podczas drogi powrotnej agenta, kontener będzie mógł go znowu rozszyfrowywać, odkrywając, do którego kontenera agent powinien udać się w następnej kolejności. W ten sposób po osiągnięciu ostatniego kontenera na ścieżce agenta, powrót agenta do stacji bazowej odbywa się poprzez sukcesywne odszyfrowywanie identyfikatorów z kolejki LIFO, przez kontenery w odwrotnej kolejności do ścieżki agenta. Uproszczony schemat działania protokołu przedstawiono na Rysunku 3.

Przed rozpoczęciem migracji kolejka LIFO wypełniana jest wartościami losowymi (wartości te pozostają w kolejce, a zaszyfrowane identyfikatory dodawane są po nich), aby uniemożliwić atakującemu rozpoznanie, która część kolejki zawiera zaszyfrowany identyfikator stacji bazowej.

Aby umożliwiać wykrycie ewentualnych modyfikacji danych w kolejce (przez osoby niepowołane), zastosowano metodę polegającą na obliczaniu przez każdy kontener funkcji skrótu. Funkcja obliczana jest dla binarnej konkatenacji (złączenia) identyfikatorów trzech kontenerów: poprzedniego, bieżącego i następnego. Wynik dołączany jest do szyfrowanego identyfikatora jeszcze przed jego zaszyfrowaniem. Metoda ta została zaproponowana wcześniej przez Karjoth'a i znana jest pod nazwą *hash chaining* [28]. Jej celem jest ochrona przed atakami polegającymi na usuwaniu identyfikatorów kontenerów pośrednich.

Także jeszcze przed zaszyfrowaniem identyfikatora (a właściwie już pewnej porcji danych go zawierającej), dołączana jest także wartość losowa (w terminologii bezpieczeństwa informacji operacja samego dołączenia danych losowych określana jest jako *solenie*, ang. *salting*), aby zaszyfrowane dane miały unikalną wartość. Operacja ta określana jest jako *pieczętowanie* danych (ang. *sealing*) [29]. W rezultacie zaszyfrowaniu podlega następująca porcja danych: funkcja skrótu, identyfikator i wartość losowa.

Protokół został tak zaprojektowany, aby zużywać jak najmniej zasobów. Szyfrowanie wykorzystywane jest wyłącznie, gdy to konieczne i wyłącznie w odniesieniu do kluczowych danych [30]. Analiza wydajności protokołu wykazała ponadto, że to migracja agenta, a nie szyfrowanie, ma zasadniczy wpływ na jego złożoność czasową [31], [32].

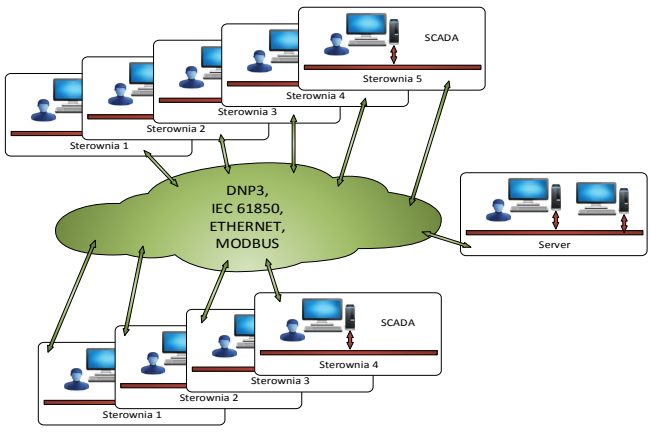
4.3 Instalacja architektury w laboratorim LINTE^2

W celu umożliwienia anonimowej wymiany informacji w Krajowym Systemie Elektroenergetycznym konieczna jest instalacja środowiska agentowego w infrastrukturze informatycznej. W tym celu zalecane jest zastosowanie platformy zgodnej ze specyfikacjami FIPA.

Najbardziej dojrzałym środowiskiem agentowym zgodnym z FIPA jest JADE (ang. *Java Agent DEvelopment Framework*) – platforma agentowa udostępniana w ramach licencji otwartej, wspierana przez liczną społeczność użytkowników oraz programistów, którzy gwarantują jej ciągłą poprawę i rozwój. Środowisko JADE zostało napisane w Java, co powoduje, że jest ono niezależne od systemu operacyjnego i architektury sprzętowej. Cecha ta jest szczególnie ważna dla instalacji w systemie elektro-energetycznym, gdzie różne rodzaje systemów informatycznych są wzajemnie połączone.

Ze względu na krytyczny charakter systemów elektroenergetycznych niezbędne jest przetestowanie działania technologii wieloagentowej w środowisku laboratoryjnym, o strukturze jak najbardziej zbliżonej do środowiska przemysłowego.

Takie możliwości daje m.in. infrastruktura badawcza Laboratorium LINTE^2 Wydziału Elektrotechniki i Automatyki, w którym stworzono unikalne warunki badań dotyczących inteligentnych sieci elektroenergetycznych (Smart Grids), inteligentnych wysp energetycznych z własnymi zasobami wytwórczymi, nowych usług sieciowych (zarządzanie zapotrzebowaniem na energię elektryczną, lokalna generacja energii itp.), nowych konstrukcji przekształtników energoelektronicznych i ich zastosowań w systemie elektroenergetycznym (układy FACTS, filtry aktywne, przekształtniki sprzęgające itp.) [33]. Dodatkowym atutem wykorzystania Laboratorium LINTE^2 jest jego rozproszony system sterowania oparty na sieci komunikacyjnej Ethernet obejmujący lokalne sterowniki jednostek funkcjonalnych, cyfrowe przekaźniki zabezpieczeniowe i 9 sterowni ze stanowiskami operatorsko-inżynierskimi (rys.4), w których planowana jest instalacja kontenerów architektury wielagentowej.



Rys.4. Ogólna struktura komunikacyjna Laboratorium LINTE^2

Kontenery architektury agentowej zostaną zainstalowane w poszczególnych sterowniach. W każdym z kontenerów zostanie włączona specjalna wtyczka do JADE służąca do zapewniania anonimowości (ang. *anonymity add-on*) oraz zarejestrowana usługa ochrony przed tropieniem. Sam proces aktywacji agentów niepodatnych na tropienie wymaga wykorzystania dedykowanych klas Java oraz wzorców zachowania związanych z migracją agentów. W tak skonfigurowanym środowisku, anonimizowane informacje o incydentach będą przenoszone przez specjalne agenty migrujące.

5. PODSUMOWANIE

Sytuacja formalno-prawna podmiotów związanych z systemem elektroenergetycznym jest bardzo złożona. Elektrownie oraz stacje elektroenergetyczne należą obecnie do różnych właścicieli. W obecnej sytuacji przekazywanie danych i informacji na temat potencjalnych zagrożeń i zaistniałych cyberatakach jest utrudnione, a wręcz ze względów konkurencji na rynku energii niemożliwe.

Zabezpieczanie tak rozległej i złożonej sieci wymaga połączenia standardowych i zaawansowanych technologii bezpieczeństwa informacji. Tradycyjne rozwiązania, takie jak zapory ogniowe, systemy wykrywania włamań /prewencji (IDS / IPS) lub anty-malware nie stanowią wystarczającej ochrony. W celu przeciwdziałania rozwojowi wyrafinowanych zagrożeń, takich jak APT lub DDoS, wymagane jest stosowanie technologii najwyższej klasy, łącznie z systemami zarządzania bezpieczeństwem i zdarzeniami (SIEM) w tym opisywanej w niniejszym artykule systemu wieloagentowego.

Laboratorium LINTE^2 stanowi znakomitą platformę testową dla przetestowania różnych wariantów ataków jak również nowych metod ich nadzoru i kontroli.

6. BIBLIOGRAFIA

[1] R. Roche, B. Blunier, A. Miraoui, V. Hilaire, and A. Koukam, "Multi-agent systems for grid energy management: A short review," in IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society, 2010, pp. 3341–3346.

[2] S. Franklin and A. Graesser, "Is It an Agent, or Just a Program?: A Taxonomy for Autonomous Agents," in Intelligent Agents III. Agent Theories, Architectures and Languages (ATAL'96), 1996, vol. 1193.

[3] R. Murch and T. Johnson, Intelligent software agents. Prentice Hall PTR, 1999.

[4] D. Chess, B. Grosof, C. Harrison, D. Levine, C. Parris, and G. Tsudik, "Itinerant Agents for Mobile Computing," IEEE Pers. Commun., vol. 2, no. 5, pp. 34–49, 1995.

[5] J. Odell, "Introduction to Agents." 2000.

[6] F. Bellifemine, G. Caire, T. Trucco, and G. Rimassa, "Jade Programmer's Guide." Tilab, 2003.

[7] M. Luck, P. McBurney, O. Shehory, S. Willmott, and the AgentLink Community, Agent Technology Roadmap: A Roadmap for Agent Based Computing. AgentLink III, 2005.

[8] W. M. Farmer, J. D. Guttman, and V. Swarup, "Security for Mobile Agents: Issues and Requirements." 1996.

[9] R. S. Gray, D. Kotz, G. Cybenko, and D. Rus, "Mobile Agents: Motivations and State-of-the-Art Systems," Hanover, NH, 2000.

[10] F. Ren, M. Zhang, D. Soetanto, and X. Su, "Conceptual Design of A Multi-Agent System for Interconnected Power Systems Restoration," IEEE Trans. Power Syst., vol. 27, no. 2, pp. 732–740, May 2012.

[11] A. Manickam, G. D. Swann, S. Kamalasadan, D. Edwards, and S. Simmons, "A novel self-evolving multi-agent architecture for power system monitoring and protection against attacks of malicious intent," in IEEE PES General Meeting, 2010, pp. 1–8.

[12] K. J. Ross, K. M. Hopkinson, and M. Pachter, "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security," IEEE Trans. Smart Grid, vol. 4, pp. 1216–1224, 2013.

[13] M. Nasri, H. Farhangi, A. Palizban, and M. Moallem, "Multi-agent control system for real-time adaptive VVO/CVR in Smart Substation," in 2012 IEEE Electrical Power and Energy Conference, 2012, pp. 1–7.

[14] S. Kahrobaee, R. A. Rajabzadeh, L.-K. Soh, and S. Asgarpoor, "A Multiagent Modeling and Investigation of Smart Homes With Power Generation, Storage, and Trading Features," IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 659–668, Jun. 2013.

[15] H. S. V. S. Kumar Nunna and S. Doolla, "Multiagent-Based Distributed-Energy-Resource Management for Intelligent Microgrids," IEEE Trans. Ind. Electron., vol. 60, no. 4, pp. 1678–1687, Apr. 2013.

[16] H. N. Aung, A. M. Khambadkone, D. Srinivasan, and T. Logenthiran, "Agent-based intelligent control for real-time operation of a microgrid," in 2010 Joint International Conference on Power Electronics, Drives and Energy Systems & 2010 Power India, 2010, pp. 1–6.

[17] A. S. A. Awad and A. Abdr, "Multiagent coordination in microgrids via wireless networks," IEEE Wirel. Commun., vol. 19, no. 3, pp. 14–22, Jun. 2012.

[18] C. M. Colson and M. H. Nehrir, "Comprehensive Real-Time Microgrid Power Management and Control With Distributed Agents," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 617–627, Mar. 2013.

[19] M. Chen and S. Gonzalez, "Applications and design issues for mobile agents in wireless sensor networks," IEEE Wirel. Commun., vol. 14, no. 6, pp. 20–26, Dec. 2007.

[20] A. D. McKinnon, S. R. Thompson, R. A. Doroshchuk, G. A. Fink, and E. W. Fulp, "Bio-inspired cyber security for smart grid deployments," in 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), 2013, pp. 1–6.

[21] R. Leszczyna and J. Górski, "Untraceability of Mobile Agents," in Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS '05), 2005, vol. 3, pp. 1233–1234.

[22] R. Leszczyna and J. Górski, "An Untraceability Protocol for Mobile Agents and Its Enhanced Security Study," in 15th EICAR Annual Conference Proceedings, 2006, pp. 26–37.

[23] R. Leszczyna, "Anonymity Architecture for Mobile Agents," Ispra, Italy, 2006.

[24] J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," in Designing Privacy Enhancing Technologies: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability, 2001, vol. 2009, pp. 10–29.

[25] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr, "Towards an analysis of onion routing security," in Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, 2000, vol. 2009, pp. 96–114.

[26] Y. Lindell, "Foundations of Cryptography 89-856." 2006.

[27] Foundation for Intelligent Physical Agents (FIPA), "FIPA Abstract Architecture Specification." 2002.

[28] G. Karjoth, N. Asokan, and C. Gülcü;, "Protecting the Computation Results of Free-Roaming Agents," in MA '98: Proceedings of the Second International Workshop on Mobile Agents, 1999, pp. 195–207.

[29] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 4, no. 2, 1981.

[30] R. Leszczyna and J. Górski, "Untraceability of Mobile Agents," 2004.

[31] R. Leszczyna and J. Górski, "Performance Analysis of Untraceability Protocols for Mobile Agents Using an Adaptable Framework," in Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS '05), 2006, pp. 1063–1070.

[32] R. Leszczyna and J. Górski, "Performance Analysis of Untraceability Protocols for Mobile Agents," 2005.

[33] J. Nieznański, “Laboratorium LINTE^2 ukończone”. Pismo PG nr 1, Politechnika Gdańska 2016, str. 11-12.
[34] R. Leszczyna, M.R. Wróbel, R. Małkowski, "Security requirements and controls for incident information sharing in the polish power system", Compatibility Power Electronics and Power Engineering (CPE-POWERENG) 2016 10th International Conference on, pp. 94-99, 2016, ISSN 2166-9546.

CONCEPT OF PLATFORM FOR SHARING INFORMATION ABOUT CYBER-SECURITY INCIDENTS IN THE NATIONAL POWER SYSTEM

The article describes selected issues related to cybersecurity in the electric power sector. One of the aspects of providing power grid security is the effective exchange of information on security incidents. Under the framework, all the actors of the power system, ie .: power plants, transmission system operators, distribution system operators, suppliers of security solutions, standardization organizations, as well as research centers and academia, should be able to share information with each other on security incidents in the power system. The paper describes the idea of using multi-agent systems for this purpose. As the formal and legal circumstances of power system entities are very complex, possibilities of conducting research and development in the field of cybersecurity are significantly reduced, and sometimes impossible. The paper presents the research capabilities in this area, offered by the Laboratory LINTE^2.

Keywords: Power grid, cyber security, information sharing, anonymity, Multi-Agent, Power System Laboratory.