# Nowe czujniki mogą pomóc kolejom bronić się przed atakami EM

Virginie Deniau, koordynatorka projektu SECRET, omawia urządzenia opracowane przez swój zespół do wykrywania na bieżąco ataków elektromagnetycznych (EM), aby operatorzy mogli przełączać się na bezpieczny tryb kolejowy.

Jedenaście lat temu seria ataków bombowych na pociągi w Madrycie wyraźnie pokazała, jak bardzo bezpieczeństwo europejskich kolei wciąż wymaga poprawy. Teraz kiedy na kolei – podobnie jak w innych sektorach – intensyfikuje się normalizacja i łączność urządzeń, kolejny, bardziej podstępny rodzaj napaści staje się możliwy: ataki elektromagnetyczne (EM). Partnerzy z dofinansowanego ze środków UE projektu opracowali technologie wykrywania, które mogą wesprzeć sektor w stawieniu czoła temu nowemu zagrożeniu.

Czy wiedzieliście, że już niedługo na Ziemi będzie tyle połączonych urządzeń, co ludzi? Obecnie użytkowanych jest pięć miliardów takich urządzeń, a do roku 2020 ich liczba ma osiągnąć 25 miliardów. Z pewnością każdy nowy typ połączonego urządzenia przybliża nas do nadejścia inteligentnych miast i wszystkich innych przewidywanych korzyści. Jednak z drugiej strony, jak pokazały ostatnie doniesienia, rosnące zagrożenie dla bezpieczeństwa stwarzają hakerzy i inni entuzjaści techniki o niecnych zamiarach.

W przypadku europejskich kolei na przykład ujednolicenie technologii sieciowych i korzystanie w coraz szerszym zakresie z komunikacji bezprzewodowej zdecydowanie zwiększyło prawdopodobieństwo scenariusza ataku EM. Zagłuszacze komunikacji są proste w użyciu i każdy może je kupić w Internecie, co oznacza, że komunikacja może zostać zakłócona, powodując opóźnienia, blokady, a nawet przekierowanie pociągów.

Aby przygotować sektor do stawienia czoła temu nowemu zagrożeniu, partnerzy projektu SECRET (SECurity of Railways against Electromagnetic aTtacks) opracowali komplet czujników do wykrywania, które potrafią na bieżąco wychwytywać ataki EM, dzięki czemu operatorzy mogą przełączyć sieć na „tryb bezpieczny”, odporny na określony typ zastosowanego ataku EM.

Virginie Deniau, koordynatorka SECRET, omawia prawdopodobieństwo scenariusza ataku EM, urządzenia opracowane przez jej zespół i sposób, w jaki sektor będzie zmuszony już niedługo dostosować się do tej nowej rzeczywistości.

Na ile prawdopodobny jest pani zdaniem scenariusz ataku EM?

Definicja ataku EM ewoluuje wraz z mnogością aplikacji opartych na technologiach komunikacji bezprzewodowej. Dotychczas ataki EM opierały się na wytwarzaniu zamierzonych interferencji wysokoenergetycznych (impulsów elektromagnetycznych lub wysokoenergetycznych wiązek mikrofal) zdolnych do zakłócenia pracy urządzeń elektronicznych lub ich uszkodzenia. Obecnie urządzenia te można uruchomić za pomocą sygnału sterującego lub informacji przekazanej łączami bezprzewodowymi, co oznacza, że znacznie łatwiej jest teraz zakłócić przesyłane informacje i uszkodzić urządzenia. Do przeprowadzenia tego typu ataku potrzebny jest słabszy sygnał, który można wytworzyć za pomocą mobilnych lub innych dyskretnych urządzeń. Zatem z technologicznego punktu widzenia, prawdopodobieństwo ataku wzrasta wraz z podatnością infrastruktur. Jednak trudno jest jednoznacznie ustalić prawdopodobieństwo, gdyż nie ma na dzień dzisiejszy możliwości rozróżnienia między usterką techniczną a atakiem EM. Ataki EM oparte na stosunkowo słabym sygnale mocy powodują bowiem zakłócenia bez doprowadzania do trwałych uszkodzeń.

Wspomniała pani o urządzeniach mobilnych. Czy to oznacza, że w zasadzie każdy ma możliwość przeprowadzenia takiego ataku?

Wiedza na temat celu ma zasadnicze znaczenie dla zdefiniowania środków niezbędnych do przeprowadzenia ataku EM. Zagłuszacze komunikacji publicznej są teraz łatwo dostępne na rynku, ale ich moc i działanie są ograniczone.
Jeżeli weźmiemy pod uwagę profesjonalne albo bezpieczne usługi komunikacji, to zazwyczaj potrzebne są specyficzne urządzenia. Ich dostępność jest raczej ograniczona do rynku profesjonalnego albo trzeba je opracować od zera. Choć możliwe, wymaga to pewnego poziomu umiejętności i wiedzy.
Jednak jeżeli te profesjonalne aplikacje są obsługiwane przez publiczne serwisy bezprzewodowe, ich funkcjonowanie może zostać zakłócone przez zwykłe zagłuszacze. Powstaje zatem realny problem, a bezpieczeństwo i newralgiczne znaczenie usług bezprzewodowych wymagają poważnego rozważenia.

SECRET koncentruje się na bezpieczeństwie kolei. Jakimi konsekwencjami skutkowałby ataki EM na ten sektor?

Głównym i bezpośrednim zagrożeniem jest zakłócenie ruchu w sieci kolejowej. Możliwe jest powstrzymanie wyjazdu i wymuszenie zatrzymania pociągów, doprowadzenie do poważnych strat finansowych oraz niewyobrażalnych sytuacji. Niemniej trudno jest dokładnie ocenić kaskadowe następstwa, gdyż są one uzależnione od charakterystyki danej sieci kolejowej (eksploatacja, infrastruktura, aplikacje itp.).

Czy może nam pani powiedzieć więcej na temat opracowanych narzędzi?

Wizja SECRET opiera się na założeniu, że dysponując zdolnością do niezawodnego wykrywania ataku EM, możemy zakładać przełączanie na bezpieczny – doskonale przystosowany do sytuacji – tryb kolejowy, który pozwoli operatorom odzyskać kontrolę. Zadanie polega zatem na opracowaniu szybkich i niezawodnych rozwiązań w zakresie wykrywania. Mając to na względzie przeanalizowaliśmy w ramach SECRET kilka rozwiązań. Niektóre z nich można by wdrożyć bezpośrednio w terminalach komunikacyjnych, podczas gdy inne wymagałyby specjalnych urządzeń, ale mających tę zaletę, że potrafią monitorować wiele łączy komunikacyjnych.
Aby osiągnąć odporność, nasze czujniki wykrywania zostały sprzężone z decyzyjnym terminalem gromadzenia danych, którego zadanie polegało na analizie danych pochodzących z tych czujników i sterowaniu rekonfigurowalną platformą telekomunikacyjną. Na podstawie danych otrzymywanych z czujników, terminal decyzyjny kieruje przekazywanie komunikatów do łącza komunikacyjnego, które jest najbardziej odporne na atak EM. Takie podejście wymaga, co oczywiste, wdrożenia kilku sieci komunikacyjnych.

Kiedy spodziewa się pani, że technologia SECRET trafi na rynek?

Ze względu na mobilność i szerokie spektrum elektromagnetycznych środowisk kolejowych, trudno jest zademonstrować odporność i całkowity brak wadliwości rozwiązań w zakresie wykrywania na pokładzie pociągu. Niemniej, kiedy pociąg stoi, technologie SECRET są naprawdę skuteczne. Możemy zatem przewidywać stosunkowo szybkie wejście na rynek tych technologii w celu ochrony stacji kolejowych lub innej infrastruktury krytycznej.
Równolegle technologie SECRET mogą przyczynić się do ewolucji standardów telekomunikacyjnych wykorzystywanych w infrastrukturze krytycznej. Zamiast zwiększania szybkości transmisji danych, standardy mogą ewoluować w kierunku dostarczania w czasie rzeczywistym informacji na temat jakości usług czy obecności sygnałów zagłuszających (celowych lub niezamierzonych). Wówczas mogłyby zapewnić odpowiednią diagnostykę i uruchomić adekwatny proces interwencji.

Europejskie koleje już znajdują się pod wysoką presją związaną z rentownością i

bezpieczeństwem. Czy pani zdaniem sektor jest w stanie udźwignąć dodatkowe koszty związane z wdrożeniem rozwiązań SECRET?

Sądzę, że zważywszy na rosnące zagrożenie, koniecznością będzie zagwarantowanie odporności sieci kolejowej na takie ataki. Systemy komunikacji bezprzewodowej zazwyczaj stanowią jedynie niewielki odsetek budżetu projektu kolejowego. Niemniej mają zasadnicze znaczenie dla planów dotyczących eksploatacji i bezpieczeństwa. Ataki EM mogą mieć dramatyczne następstwa pod względem kosztów, a jeżeli będą łatwe do przeprowadzenia, to mogą przekształcić się w częste, złośliwe działania. Rozwiązanie chroniące przed atakami EM należy zatem rozważać w świetle zagrożeń, skutków i nakładów inwestycyjnych.

Jakie macie plany teraz, kiedy prace nad projektem dobiegają końca?

Chlelibyśmy przetestować naszą analizę ataków EM na innych rodzajach ataków, takich jak fizyczne czy innego typu cyberataki. Tak naprawdę ataki zagłuszające mogą być łatwo wykorzystane do wsparcia innych złośliwych działań, aby uniknąć transmisji wideo lub sygnału alarmowego. W konsekwencji analizy ryzyka muszą brać pod uwagę potencjalnie połączone ataki fizyczne i zagłuszające. Sądzimy także, że architektura wykrywania ataków EM zaproponowana w ramach SECRET powinna zostać sprzężona z innymi narzędziami monitorującymi infrastrukturę, aby zyskać lepszy wgląd w to, co dzieje się w sieci w czasie rzeczywistym.

Więcej informacji:

SECRET
http://www.secret-project.eu/

## Kraje

Francja

## Powiązane projekty

ARCHIVED

## SECurity of Railways against Electromagnetic aTtacks

SECRET

12 Września 2016

PROJEKT

## Ten artykuł pojawia się w...

MAGAZYN RESEARCH*EU

**Nauka w parze z bezpieczeństwem**

## Powiązane artykuły

WIADOMOŚCI

NOWE PRODUKTY I TECHNOLOGIE

### Nowe narzędzia i metody ochrony infrastruktury krytycznej w Europie

19 Maja 2016

**Ostatnia aktualizacja:** 14 Lipca 2015

**Permalink:** https://cordis.europa.eu/article/id/117444-new-detection-sensors-can-help-railways-cope-with-em-attacks/pl