Prof. dr hab. inż. Franciszek Seredyński
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Wydział Matematyczno – Przyrodniczy
Szkoła Nauk Ścisłych
ul. Wóycickiego 1/3, 01-938 Warszawa

Warszawa, 5.08.2013

R E C E N Z J A

rozprawy doktorskiej mgr inż. Michała Kozy pt.
„Repelling Sybil Attacks in wireless ad hoc systems”

1. Problematyka naukowa oraz przedmiot rozprawy

Sieci mobilne i bezprzewodowe to jeden z dynamicznie rozwijających się kierunków współczesnej informatyki i telekomunikacji. Najbardziej znany dzisiaj segment tych sieci to sieci komórkowe, których wszyscy jesteśmy użytkownikami. Innym nowym i perspektywicznym segmentem sieci mobilnych i bezprzewodowych to sieci ad hoc, nazywane również sieciami doraźnymi bądź spontanicznymi, które w odróżnieniu od sieci komórkowych nie wymagają budowy infrastruktury, a urządzenia mobilne, takie jak np. laptopy czy komórki przemieszczając się „widzą” siebie wzajemnie w odległości kilkuset metrów. Kolejnym segmentem sieci bezprzewodowych to sieci sensorowe, w których sensory, tzn. zminiaturyzowane procesory o bardzo małej mocy obliczeniowej, wyposażone w czujniki oraz na ogół jednorazowe baterie, umieszczone są na stale na jakimś obszarze, który monitorują i mogą komunikować się na odległość kilku metrów i przekazywać sobie informację. Recenzowana rozprawa doktorska dotyczy tych dwóch ostatnich segmentu sieci bezprzewodowych.

Pojawienie się koncepcji sieci ad hoc oraz sieci sensorowych, opracowanie oraz implementacja konkretnych technologii tych sieci, jak też doświadczenia zdobyte w trakcie ich eksploatacji skutkowało pojawieniem się szeregu nowych problemów teoretycznych, których rozwiązanie jest konieczne z punktu dalszego rozwoju tych technologii. Sieci te to z punktu widzenia informatyki, przede wszystkim systemy rozproszone, w których brak centralnego zarządzania, a więc proponowane algorytmy muszą mieć charakter algorytmów rozproszonych, a jednym z centralnych zagadnień w kontekście tych algorytmów jest problem wyboru lidera. O ile problem wyboru lidera w kontekście algorytmów i systemów rozproszonych jest znany od dawna to jakościowo zupełnie nowym elementem jest problem bezpieczeństwa tych sieci, a w szczególności duża ich wrażliwość na różnego rodzaju ataki i związana z tym możliwość przechwycenia zasobów tych sieci. Ta wrażliwość na ataki jest spowodowana wieloma czynnikami: tym, że liczba uczestników sieci zmienia się dynamicznie w czasie (sieci ad hoc), pojemność baterii urządzeń jest silnie ograniczona (sieci ad hoc, sieci sensorowe), moc obliczeniowa procesorów jest niska (sieci sensorowe), a komunikacja między urządzeniami ma charakter komunikacji radiowej, mało odpornej na, np. podsłuchiwanie czy zewnętrzne celowe zakłócenia (sieci ad hoc, sieci sensorowe).

Recenzowana rozprawa doktorska poświęcona jest opracowaniu algorytmów przeciwdziałania pewnej klasie ataków w sieciach bezprzewodowych, określanych jako atak typu Sybil, który polega na tym, że N urządzeń związanych z prawowitymi uczestnikami sieci jest przechwyconych przez atakującego (adwersarza) i urządzenia te symulują (podszywają się) pod M > N uczestników sieci.

Doktorant w swojej rozprawie opracował szereg oryginalnych algorytmów wyboru lidera w sieci bezprzewodowej, odpornych na działanie adwersarza, w tym adwersarza wykonującego ataki typu Sybil. Postawiony w rozprawie cel został ściśle określony oraz w pełni osiągnięty. Rozważane w rozprawie zagadnienia są aktualne i w istotny sposób wpisują się w obszar informatyki. Rozprawa może zatem być przedstawiona jako monografia doktorska w dziedzinie informatyki.

2. Analiza treści rozprawy oraz uzyskanych wyników

Rozprawa została przygotowana w języku angielskim i składa się z 5 rozdziałów, podsumowania oraz bibliografii obejmującej 30 pozycji literaturowych. Całość pracy obejmuje 100 stron i ma ona charakter teoretyczny. Wyniki własne doktoranta przedstawione są w rozdziałach 2,3,4 i 5.

Rozdział 1 stanowi wprowadzenie do problematyki rozprawy. Doktorant przedstawia ogólny model bezprzewodowej sieci, w której urządzenia komunikują się radiowo przez jeden współdzielony kanał, charakteryzuje adwersarza, który przez nieuczciwe zachowanie może przejąć kontrolę nad siecią, definiuje atak typu Sybil oraz formułuje cel pracy

W Rozdziale 2 doktorant definiuje problem wyboru lidera w środowisku sieci bezprzewodowej i przedstawia prosty znany z literatury algorytm wyboru lidera w takim środowisku. Następnie wykazuje słabości tego algorytmu z punktu widzenia jego bezpieczeństwa, wynikające ze stosunkowo łatwej możliwości wykonania ataku na ten algorytm i przechwycenia zasobów komunikacyjnych sieci jak też bardzo dużą trudność wykrycia takiego ataku. Dokonana w tym rozdziale analiza własności algorytmu wyboru lidera z punktu widzenia jego słabości jest punktem wyjściowym w kierunku opracowania bezpiecznych algorytmów wyboru lidera w kontekście specyficznego ataku typu Sybil wykonywanego w środowisku sieci bezprzewodowej.

Następny rozdział, Rozdział 3 poświęcony jest zagadnieniom ataków typu Sybil w sieciach bezprzewodowych. Intencją doktoranta było rozpatrzenie sytuacji, w których istnieją ograniczenia stacji transmitujących na możliwości monitorowania stanu kanału w sensie jednoczesnej transmisji oraz nasłuchiwania jak też możliwości wielokrotnego symulowania fałszywych tożsamości. Doktorant rozpatruje kilka modeli sieci opartych na powyższych założeniach i analizuje je pod katem możliwości wykonania ataku typu Sybil. Następnie proponuje dwa algorytmy wyboru lidera, które zapewniają uczciwy wybór lidera w sytuacji gdy atak typu Sybil nie jest możliwy do wykonania. W dalszej kolejności doktorant wykazuje jakim dużym zagrożeniem dla protokołu wyboru lidera jest atak typu Sybil i jak trudno jest go wykryć. W kolejnej części rozdziału doktorant przedstawia algorytm wyboru lidera odporny na atak typu Sybil przeprowadzony przez pojedyncze urządzenie będące w posiadaniu adwersarza, które nie ma pełnej informacji o kanale i wykazuje, że przy tym algorytmie wyboru lidera wykonanie ataku jest dla adwersarza nieopłacalne.

W Rozdziale 4 doktorant bazując na algorytmie z poprzedniego rozdziału i proponuje algorytm listowania odporny na ataki typu Sybil. Doktorant pokazuje, że ten algorytm jest efektywny również w sytuacji gdy adwersarz posługuje się kilkoma urządzeniami. Złożoność tego algorytmu może potencjalnie rosnąć w przypadku agresywnego ataku, ale dzięki konstrukcji algorytmu takie zachowanie adwersarza nie jest dla niego opłacalne i wg. autora powinno zniechęcać do wykonania ataku.

W ostatnim numerowanym rozdziale rozprawy, Rozdziale 5 doktorant proponuje dwa algorytmy wyboru lidera bazujące na koncepcji tzw. dowodu wykonania pracy związanej z autoryzowaniem tożsamości. Algorytmy różnią się głównie złożonością i w minimalnym stopniu bezpieczeństwem. Rozprawa kończy się krótkim podsumowaniem wyników osiągniętych w rozprawie.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Rozprawa doktorska mgra inż. Michała Kozy zawiera nowe, oryginalne wyniki dotyczące metod przeciwdziałania atakom typu Sybil w systemach bezprzewodowych. Do najistotniejszych osiągnięć rozprawy zaliczyć należy:

- opracowanie dwóch algorytmów wyboru lidera zapewniających uczciwy wybór lidera w sytuacji gdy atak typu Sybil nie jest możliwy i wykazanie, że tego typu atak stanowi poważne zagrożenie dla protokołu wyboru lidera, w tym trudną jego wykrywalność
- opracowanie koncepcji algorytmu wyboru lidera odpornego na atak typu Sybil przeprowadzony przez pojedyncze urządzenie adwersarza
- opracowanie algorytmu listowania odpornego na ataki typu Sybil przeprowadzane jednocześnie przez kilku adwersarzy
- opracowanie dwóch wariantów wyboru lidera bazujących na koncepcji tzw. Proof of Work czyli dowodu wykonanej pracy.

4. Uwagi merytoryczne

W trakcie czytania rozprawy doktorskiej nasuwają się pewne uwagi o charakterze dyskusyjnym. Są to:

- Widzę pewną niekonsekwencję w następującym łańcuchu pojęć: w tytule pracy doktorant używa nazwę „sieci ad hoc" zakładającą zarówno bezprzewodowość jak też mobilność, Wstęp Rozdziału 1 oraz definicja ataku Sybil (Definicja 1.4) sugerują, że doktorant będzie zajmował się sieciami sensorowymi zakładającymi bezprzewodowość, brak mobilności i bardzo ograniczoną energię jednorazowej baterii, a w rzeczywistości doktorant zajmuje się w swojej rozprawie modelem sieci odpowiadającym bezprzewodowemu Ethernetowi

- Problematyka sieci mobilnych i bezprzewodowych jest rozwijana bardzo intensywnie na przestrzeni ostatnich 20 lat, zarówno na poziomie teoretycznym jak też na poziomie technologii, z których masowo korzystamy; w pracy brakuje pogłębionego przeglądu literaturowego, który wskazywałby na relacje między przyjętym modelem sieci i aktualnie stosowanymi rozwiązaniami; lista pozycji literaturowych zamieszczonych w bibliografii jest zbyt mała i odpowiada artykułowi publikowanym w czasopiśmie

- Czy doktorant rozważał celowość eksperymentalnej weryfikacji praktycznej złożoności proponowanych rozwiązań, np. algorytmów bazujących na koncepcji Proof of Work ? Jak ta złożoność zależy od liczby stacji N i jaka wartość N byłaby akceptowalna praktycznie ?

- Jak złożoność proponowanych algorytmów ma się do ograniczonych zwykle pojemności baterii stacji i mocy obliczeniowej urzadzeń ?

- Czy doktorant widzi możliwość zastosowania zaproponowanych rozwiązań w ramach aktualnie stosowanych technologii bezprzewodowych ?

5. Uwagi redakcyjne i edytorskie

Rozprawa napisana jest precyzyjnym językiem i starannie zredagowana. Doktorant dobrze radzi sobie z konstrukcjami języka angielskiego. Odnajduję w niej kilka następujących niedociągnięć edytorskich bądź językowych:

- W spisie treści na str. 6 brakuje ostatniego wiersza dotyczącego „Bibliography"
- Brakuje przecinka przed „where' w Definition 1.5 (str. 14), w Theorem 3.10 (str. 49)
- „vales" → „values" (str. 15)
- Brakuje przecinka po „However" (str. 21), (str. 23), str. 96
- Brakuje przecinka po „Finally" (str. 44)
- „ …execution of Algorithm 3 each box represents …" → „ …execution of Algorithm 3. Each box represents …" (str. 48)
- „…is such kind" → „…is such a kind" (str. 49)
- " If is succeeds …" → " If it succeeds …" (str. 51)

6. Podsumowanie

Powyżej przedstawione uwagi merytoryczne oraz redakcyjne nie mają istotnego wpływu na jakość i wagę przedstawionych rozwiązań i w żadnym stopniu nie obniżają wartości pracy. Przedstawione przez autora badane aspekty zostały ujęte wystarczająco szczegółowo i dokładnie. Uzyskane wyniki teoretyczne są dobrą bazą startową do badań w zakresie bezpieczeństwa dla bardziej zaawansowanych modeli systemów ad hoc. Reasumując można stwierdzić, że główne wyniki rozprawy potwierdzają osiągnięcie z powodzeniem założonego w rozprawie celu. Wyniki te były prezentowane na międzynarodowych konferencjach i publikowane w serii *LNCS* wydawnictwa Springer.

Podsumowując, stwierdzam, że przedstawiona do oceny rozprawa doktorska mgr inż. Michała Kozy pt.: „Repelling Sybil Attacks in wireless ad hoc systems" spełnia w stopniu bardzo dobrym wymagania stawiane rozprawom doktorskim przez obowiązującą ustawę o stopniach i tytule naukowym. W konsekwencji, może ona stać się przedmiotem publicznej obrony. Wnoszę zatem o dopuszczenie mgr inż. Michała Kozy do dalszych etapów przewodu doktorskiego.