STRESZCZENIE:
Przeciwdziałanie Atakom Typu Sybil w Bezprzewodowych Systemach Ad Hoc.

Autor: **Michał Koza**
Promotor: **prof. Mirosław Kutyłowski**

Wstęp. Celem rozprawy jest opracowanie algorytmów **wyboru lidera** odpornych na działania adwersarza. W rozprawie rozważana jest bezprzewodowa sieć ad hoc, w której każda para urządzeń ma możliwość bezpośredniej komunikacji. Zakłada się, że urządzenia mają do dyspozycji jeden współdzielony kanał komunikacyjny. W rezultacie, w każdej chwili tylko jedno urządzenie może nadawać. Jednoczesna transmisja dwóch lub więcej urządzeń skutkuje kolizją i wszystkie transmisje są nieczytelne.

Wybór lidera to procedura mająca na celu wskazanie jednego uczestnika jako lidera, tak, żeby wszyscy inni uczestnicy znali jego tożsamość. Lider nie musi być liderem w sensie dosłownym. Może on być wybrany do wykonania jakiegoś zadania lub, aby zdobyć prawo do używania kanału komunikacyjnego. Wybór lidera jest jednym z najbardziej fundamentalnych algorytmów w sieciach ad hoc. W normalnych warunkach każdy uczestnik powinien mieć takie same szanse zostania liderem. Celem adwersarza jest zwiększenie swoich szans.

Adwersarz jest definiowany jako gracz, który przejął lub sklonował jedno lub wiele urządzeń z sieci. Następnie przez nieuczciwe wykonywanie protokołu próbuje przejąć jak największą kontrolę nad siecią, aby wykorzystywać ją do własnych celów. Ponieważ urządzenia pod kontrolą adwersarza są prawowitymi uczestnikami sieci, przyjęte jest założenie, że adwersarz zna protokół i może bez problemu uczestniczyć w każdym zadaniu realizowanym przez sieć.

Warto podkreślić fakt, że blokowanie sieci nie jest celem adwersarza, oraz, że gdy adwersarz zachowuje się zgodnie z protokołem, jego wykrycie jest z założenia niemożliwe. Zatem, przez algorytm odporny na adwersarza, autor rozumie algorytm, który utrzymuje prawdopodobieństwo zwycięstwa adwersarza na poziomie równym frakcji urządzeń pod jego kontrolą w sieci.

Możliwości wykrywania adwersarza. W tym rozdziale przedstawiony jest prosty algorytm wyboru lidera. Jeżeli wszyscy uczestnicy postępują uczciwie – z tym samym "priorytetem" – algorytm daje każdemu równe szanse. Jest on również bardzo szybki – oczekiwana liczba rund potrzebnych do wyłonienia lidera jest bliska e.

Pokazane jest, jak łatwo i efektywnie można zaatakować ten algorytm. Adwersarz atakuje przez bardziej agresywne uczestnictwo – nadawanie z większym priorytetem. Wykazane jest, że w zależności od pewnych założeń, atak jest bardzo trudny, bądź zupełnie niemożliwy do wykrycia. Jest to spowodowane faktem, że atak nie wpływa na żadne obserwowalne parametry wykonania algorytmu, lub wpływa na nie jedynie nieznacznie.

Modele sieci i ataki typu Sybil. Począwszy od tego rozdziału rozważany jest atak typu Sybil. Atak typu Sybil to atak, w którym N urządzeń pod kontrolą adwersarza, symuluje $M > N$ tożsamości.

Najpierw zaproponowane są dwa algorytmy wyboru lidera. Algorytmy zapewniają uczciwy wybór lidera jeżeli atak typu Sybil nie jest możliwy.

Następnie, wykazane jest, że atak typu Sybil stanowi poważne zagrożenie dla protokołu wyboru lidera, oraz, że atak taki trudno jest wykryć.

W końcu, zaproponowany jest zarys algorytmu wyboru lidera, który jest odporny na atak typu Sybil przeprowadzany przez pojedyncze urządzenie adwersarza. Algorytm może być stosowany w sieciach, w których urządzenia nie mogą nadawać i słuchać w tym samym czasie. Wykorzystuje on fakt, że gdy urządzenie adwersarza nadaje jako jedna z symulowanych tożsamości, wówczas wszystkie tożsamości tracą informację o stanie kanału. Nie wiedzą czy transmisja została zagłuszona, czy nie. Algorytm wymaga stworzenia listy wszystkich tożsamości kandydujących o miano lidera. Najpierw wyłaniany jest kandydat na lidera. Następnie wszystkie pozostałe tożsamości są weryfikowane – czy nie są kontrolowane przez to samo urządzenie, co kandydat na lidera. Wykazane jest, że wszystkie inne tożsamości kandydata kontrolowanego przez adwersarza zostają wykryte z dużym prawdopodobieństwem. Problemem jest fakt, że sam kandydat nie jest zweryfikowany. Nie może on zostać usunięty, nawet gdy wydaje się podejrzany. Jest tak dlatego, że adwersarz może łatwo rzucić nieprawdziwe podejrzenie na uczciwego kandydata na lidera. Jednak modyfikacja protokołu, pozwalająca na tymczasowe zawieszenie podejrzanego kandydata na lidera rozwiązuje ten problem. W jej rezultacie adwersarz, decydując się na atak typu Sybil, ponosi ryzyko większe niż potencjalne zyski. Ostatecznie z punktu widzenia adwersarza optymalnie jest postępować zgodnie z protokołem.

Algorytm listowania. W tym rozdziale zaproponowany jest algorytm listowania odporny na ataki typu Sybil. Algorytm bazuje na algorytmie z poprzedniego rozdziału. Jest efektywny nawet przeciwko kilku współpracującym urządzeniom adwersarza. Algorytm ten dokonuje weryfikacji wszystkich tożsamości. Zatem, oprócz wyboru lidera umożliwia również uczciwy listing. W przypadku agresywnego ataku, złożoność algorytmu może bardzo rosnąć. Jednak znów, dzięki konstrukcji algorytmu, optymalnym zachowaniem dla adwersarza jest postępowanie zgodnie z protokołem, co zniechęca go do ataku i pozwala oczekiwać niskiej złożoności protokołu.

Podejście Proof of Work do ataków typu Sybil. W ostatnim rozdziale zaproponowane są dwa algorytmy wyboru lidera. Algorytmy bazują na koncepcji Proof of Work, czyli dowodu wykonanej pracy. Ideą algorytmów jest to, że każde urządzenie musi spędzić dużo czasu (poświęcić znaczną ilość pewnego zasobu), aby autoryzować swoją tożsamość. W rezultacie, każde urządzenie jest zdolne do autoryzowania tylko jednej tożsamości.

Algorytmy różnią się głównie złożonością. Pierwszy – bardziej czasochłonny jest również minimalnie bardziej bezpieczny. Wymaga on stworzenia listy wszystkich uczestników, ale gwarantuje, że wszystkie uczciwe urządzenia wezmą udział w kluczowych procedurach algorytmu. Drugi algorytm nie wymaga tworzenia listy wszystkich uczestników, ale pozwala by z pewnym prawdopodobieństwem, jedynie urządzenia adwersarza brały udział w kluczowych procedurach algorytmu.