UNIWERSYTET WARSZAWSKI

Wydział Matematyki, Informatyki i Mechaniki

Warszawa, 22 października 2013

dr hab. Stefan Dziembowski
Instytut Informatyki
Uniwersytet Warszawski
ul. Banacha 2, 02-097 Warszawa
e-mail: S.Dziembowski@crypto.edu.pl
telefon: +48 22 55 44 154

RECENZJA ROZPRAWY DOKTORSKIEJ MGRA MICHAŁA KOZY
PT. „REPELLING SYBIL ATTACKS IN WIRELESS AD HOC SYSTEMS"
(„PRZEWCIWDZIAŁANIE ATAKOM TYPU SYBIL W BEZPRZEWODOWYCH SYSTEMACH AD HOC")

Omówienie zawartości pracy wraz z jej oceną

Rozprawa mgra Kozy dotyczy problemu bezpieczeństwa sieci bezprzewodowych typu *ad-hoc*. Jest to ciekawa i ważna dziedzina informatyki. W skrócie: bezprzewodowe sieci typu ad-hoc różnią się od zwykłych sieci przewodowych tym, że tworzone są w sposób spontaniczny przez równorzędne urządzenia. Ponieważ w związku z tym sieć taka nie posiada wyróżnionego ośrodka sprawującego nad nią kontrolę, to naturalnym problemem jaki pojawia się w praktyce jest zadanie wyłonienia przez te urządzenia spośród siebie jednego które przejęłoby funkcje kontrolne, lub uzyskało dostęp do jakiegoś ograniczonego zasobu. Cel ten osiąga się za pomocą tzw. *algorytmu wyboru lidera*. Wynikiem działania takiego algorytmu jest wskazanie jednego z urządzeń jako lidera, przy czym wymaga się, by wśród urządzeń panował konsensus co do tego kto jest tym liderem, oraz by lider był dokładnie jeden. W pracy przyjęto założenie, że każda para urządzeń ma możliwość bezpośredniej komunikacji, czyli, inaczej mówią, graf sieci jest kliką.

Zadanie wybrania lidera jest szczególnie trudne w sytuacji w której sieć jest poddana atakowi ze strony złośliwego przeciwnika, którego celem jest zwiększenie własnej szansy na uzyskanie statusu lidera. Tego właśnie problemu dotyczy praca mgra Kozy. Uważam ten problem za dobrze umotywowany zastosowaniami praktycznymi, gdyż w wielu przypadkach złośliwe ataki są łatwe do przeprowadzenia ze względu na to, że komunikacja w sieci jest bezprzewodowa, oraz na to, że sieć tworzona jest spontanicznie przez nieznających się uczestników.

Część merytoryczna pracy została umieszczona w rozdziałach 2-5. W rozdziale 2 autor analizuje bezpieczeństwo prostego algorytmu, który działa w następujący sposób: czas jego działania podzielony jest na rundy; w każdej z nich, każdy z uczestników rozgłasza do wszystkich pozostałych swój identyfikator, przy czym czyni to z prawdopodobieństwem p. Jeśli w danej rundzie więcej niż jeden z uczestników rozgłosił swój identyfikator, to mówimy, że zaszła kolizja. Działanie algorytmu kończy się w pierwszej rundzie w której rozgłoszony zostanie dokładnie jeden identyfikator. Łatwo pokazać, że wyborem parametru p, który minimalizuje czas działania algorytmu jest $p = 1/e$, gdzie e jest podstawą logarytmu naturalnego. Złośliwe działanie przeciwnika, które rozważa autor, polega na agresywnym rozgłaszaniu przez nieuczciwego uczestnika swojego identyfikatora z prawdopodobieństwem większym niż p. Autor pokazuje, że taki przeciwnik może z łatwością zaatakować ten algorytm. Co więcej, atak ten jest niemożliwy do wykrycia przy założeniu, że uczciwi uczestnicy nie mogą odróżnić kolizji w kanale rozgłaszającym od ciszy. Jest nieco łatwiejszy (choć ciągle trudny) do wykrycia jeśli uczestnicy są w stanie odróżnić te dwie sytuacje. Analiza zaprezentowana w pracy oparta jest na standardowych metodach matematyki dyskretnej i nie wydaj się zbyt trudna do przeprowadzenia. Tym niemniej uważam, że jej wykonanie jest cennym wkładem autora w zrozumienie bezpieczeństwa algorytmów wyboru lidera.

W rozdziale 3 autor zajmuje się konstrukcją algorytmów wyboru lidera które są odporne na ataki typu *sybil*. W atakach tych przyjmuje się, że przeciwnik może zasymulować działanie wielu fałszywych uczestników sieci bezprzewodowej np. po to aby zwiększyć prawdopodobieństwo tego, że jedno z kontrolowanych przez niego urządzeń uzyska status lidera. Autor wpierw pokazuje, że jeżeli przeciwnik dysponuje nieograniczoną liczbą urządzeń, to może on złamać bezpieczeństwo dowolnego algorytmu wyboru lidera. Następnie rozważa on sytuację w której przeciwnik dysponuje tylko jednym urządzeniem, które nie może jednocześnie nadawać i odbierać komunikatów. Przy tym założeniu autorowi udaje się skonstruować algorytm wyboru lidera, który działa w następujący sposób: najpierw tworzona jest lista wszystkich tożsamości które pretendują do bycia liderem. Następnie, wszystkie te tożsamości są sprawdzane, czy nie pochodzą od jednego urządzenia (w tym miejscu wykorzystywane jest założenie, że żadne urządzenie nie jest w stanie jednocześnie nadawać i odbierać komunikatów). Następnie, lider wybierany jest spośród tych tożsamości, które pozytywnie przeszły weryfikację. Wybór ten jest funkcją losowego ciągu bitów wygenerowanego bit-po-bicie za pomocą protokołu „gier parzystości" (ang. *parity game*). Założenie, że tylko jedno urządzenie może być pod kontrolą przeciwnika wydaje się dość optymistyczne i trudne do spełnienia w praktyce. Z drugiej strony jego użycie wydaje się uzasadnione, zwłaszcza w świetle wspomnianego wyżej wyniku negatywnego.

Rozdział 4 zawiera opis algorytmu *listowania* bezpiecznego ze względu na ataki typu *sybil*. Algorytm ten służy uzyskaniu listy wszystkich użytkowników sieci. Podobny algorytm był jedną z części składowych algorytmu wyboru lidera zaproponowanego w rozdziale 3. W rozdziale 4 autor ulepsza ten algorytm, dzięki czemu jest on bezpieczny również względem przeciwnika dysponującego większą liczbą urządzeń.

W rozdziale 5 autor przedstawia metodę obrony przed atakami typu *sybil* opartą na tzw. *dowody pracy* (ang. *Proofs of Work)*. Jest to technika w której każdy uczestnik protokołu na poparcie autentyczności swojej tożsamości przedstawia dowód, że wykonał on pewien wysiłek obliczeniowy. Nie jestem pewien na ile pomysł ten jest praktyczny, ponieważ wymaga on założenia, że moc obliczeniowa przeciwnika jest porównywalna z mocą obliczeniową uczciwych użytkowników, podczas gdy standardem w kryptografii jest raczej założenie, że przeciwnik ma znacznie wyższą moc obliczeniową niż inni uczestnicy protokołu.

Pewną wadą zaprezentowanych wyników jest też niski stopień formalizmu, nieco poniżej standardów przyjętych dla prac doktorskich w kryptografii. Np. definicja *zobowiązania* (*ang. commitment)* na stronie 15 jest zdecydowanie zbyt nieformalna. Brak jest również formalnych argumentów dotyczących bezpieczeństwa prezentowanych konstrukcji. Tym niemniej, uważam, że jest to wartościowa praca, zawierająca ciekawy wkład naukowy w ważną dziedzinę informatyki jaką jest bezpieczeństwo sieci bezprzewodowych.

Konkluzja

Uważam, że złożona rozprawa mgra Michała Kozy w pełni spełnia wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora nauk matematycznych w zakresie informatyki.

(-) Stefan Dziembowski