Cooperative Communications with Confidential Messages

Wyniki w skrócie

Bezpieczna wymiana danych w sieciach ad hoc

Współpraca między węzłami sieci może zwiększać podatność sieci bezprzewodowych na ataki. Naukowcy korzystający z dofinansowania UE przyjrzeli się tego typu problemom z bezpieczeństwem w odniesieniu do sieci ad hoc.

GOSPODARKA CYFROWA

© Thinkstock

Oczekuje się, że w niedalekiej przyszłości konwencjonalne sieci bezprzewodowe będą zastępowane przez sieci zdecentralizowane, a mobilne urządzenia końcowe będą na bieżąco dołączać do takich sieci i je opuszczać. Kluczową kwestią podczas projektowania takich systemów jest zapewnienie bezpiecznej wymiany poufnych danych między zaufanymi węzłami sieci.

Za cel projektu "Cooperative communications with confidential messages" (CCCM) przyjęto zwiększenie bezpieczeństwa sieci ad hoc, w których nie jest możliwe zapewnienie bezwzględnej poufności podczas wymiany kluczy kryptograficznych między heterogenicznymi węzłami. Chodziło o zaprojektowanie sieci, w której transmisja danych z węzła źródłowego do węzła docelowego odbywałaby się z użyciem minimalnej mocy. Pozwoliłoby to w znacznej mierze zapobiec odbieraniu przez węzły potencjalnie niebezpieczne danych przeznaczonych dla innych węzłów.

Współpraca innych, przyjaznych użytkowników z nadawcą mogłaby pozwolić na zwiększenie przepustowości. Dążono do maksymalizacji niezawodności i przepustowości sieci bezprzewodowych ad hoc przy ustalonej mocy i jednoczesnym zapewnieniu poufności komunikacji.

Stwierdzono, że węzły współpracujące zwiększają ogólne bezpieczeństwo sieci, funkcjonując albo jako przekaźniki, albo jako zagłuszacze wysyłające zakłócenia do węzłów podsłuchujących. Z wyjątkiem urządzeń mobilnych węzły tego typu mogłyby być zainstalowane na stałe, umożliwiając sieciom z infrastrukturą zarządzaną zwiększanie bezpieczeństwa transmisji. W przypadku sieci ad hoc zamodelowanej w układzie siatki kwadratowej stwierdzono w szczególności zwiększenie przepustowości komunikacji poufnej.

Naukowcy stwierdzili też, że możliwe jest utrzymywanie danych w tajemnicy przed węzłami pośredniczącymi. Pozwoliło to dokonywać bezpiecznej transmisji za pośrednictwem niezaufanych węzłów współpracujących. W tym przypadku wykorzystywanie ich jako zagłuszaczy okazało się skuteczniejsze niż w przypadku węzłów przekazujących.

Inny aspekt projektu dotyczył połączenia konwencjonalnych, kryptograficznych mechanizmów zapewniania poufności z metodami opartymi na teorii informacji. Umożliwia to wymianę kluczy tajnych między pożądanymi uczestnikami komunikacji z użyciem idealnie bezpiecznych łączy wykorzystujących węzły pośrednie, co przekłada się na większą przepustowość komunikacji poufnej.

Wyniki projektu otwierają nowe kierunki rozwoju komunikacji kooperatywnej. Szczególnie mechanizmy poufności oparte na teorii informacji mogą znaleźć zastosowanie w wielu dziedzinach poza mobilnymi sieciami ad hoc. Można tu wymienić łączność zbliżeniową, sieci z identyfikacją radiową, sieciowe systemy kodujące, bezpieczeństwo sieci społecznościowych i prywatność w inteligentnych sieciach energetycznych.

Słowa kluczowe

Bezpieczeństwo danych | wymiana danych | sieć ad hoc | sieci bezprzewodowe | dane poufne | węzły sieci | komunikacja kooperatywna | kryptograficzne | węzeł współpracujący | zagłuszacze | bezpieczna transmisja | przepustowość komunikacji poufnej | teoria informacji

Informacje na temat projektu

CCCM

Identyfikator umowy o grant: 237669

Projekt został zamknięty

Data rozpoczęcia
1 Grudnia 2009

Data zakończenia
31 Maja 2013

Finansowanie w ramach
Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Koszt całkowity
€ 251 049,26

Wkład UE
€ 251 049,26

Koordynowany przez
ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE
Switzerland

Ostatnia aktualizacja: 22 Stycznia 2015

Permalink: https://cordis.europa.eu/article/id/151935-secure-data-exchange-in-adhoc-networks/pl