Autoreferat[1]

1. **Imię i Nazwisko:** Marek Klonowski

2. **Posiadane dyplomy, stopnie naukowe/artystyczne z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej.**

   Stopnie naukowe doktora:

   - Doktor nauk matematycznych w zakresie informatyki (dyscyplina **informatyka**); Wydział Matematyki i Informatyki, Uniwersytet Adama Mickiewicza w Poznaniu; obrona 13 grudnia 2005; tytuł rozprawy *Algorytmy zapewniające anonimową komunikację i ich analiza*.
   - Doktor nauk matematycznych (dyscyplina **matematyka**); Instytut Matematyki i Informatyki, Politechnika Wrocławska; obrona 21 maja 2009; tytuł rozprawy *Algorytmy zapewniające anonimową komunikację i ich **matematyczna** analiza*.

   Ponadto uzyskałem dwa **tytuły zawodowe magistra:**

   - Magister inżynier (**matematyka**, specjalność informatyka matematyczna); Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska; obrona 7 lipca 2003 r.
   - Magister inżynier (**informatyka**, specjalność: inżynieria oprogramowania); Wydział Informatyki i Zarządzania, Politechnika Wrocławska; obrona 7 lutego 2007 r.

3. **Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych/artystycznych.**

   Politechnika Wrocławska, Instytut Matematyki i Informatyki. Od lutego 2006 jako asystent. Od października 2006 jako adiunkt.

4. **Wskazanie osiągnięcia* wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. nr 65, poz. 595 ze zm.):**

   Osiągnięcie zatytułowane

   Bezpieczeństwo i efektywna komunikacja w rozproszonych systemach o ograniczonych zasobach

   stanowi jednotematyczny cykl publikacji.

   a) (autor/autorzy, tytuł/tytuły publikacji, rok wydania, nazwa wydawnictwa),

[1] Format dokumentu na podstawie wzoru umieszczonego na stronach CK oraz § 4 i 5 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 1 września 2011 (Dz. Ustaw 196 poz. 1165).

A1 [2] Marek Klonowski, Mirosław Kutyłowski, Jan Zatopiański: *Energy Efficient Alert in Single-Hop Networks of Extremely Weak Devices*, Seria Lecture Notes in Computer Science (Springer Verlag) 5804, str.139-150.

A2 Zbigniew Gołębiewski, Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Leader Election for Multi-Channel Radio Networks –Dependent versus Independent Trials*, IEEE CS (IEEE Computer Society), str. 477-482.

B1 Zbigniew Gołębiewski, Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Towards Fair Leader Election in Wireless Networks*, Seria Lecture Notes in Computer Science (Springer Verlag) 5793 str. 166-179.

B2 Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Repelling Sybil-type Attacks in Wireless Ad Hoc Networks*, Seria Lecture Notes in Computer Science (Springer Verlag) 5793 str. 166-179.

C1 Jacek Cichoń, Marek Klonowski, Mirosław Kutyłowski: *Privacy Protection for RFID's – Hidden Subset Identifiers*, Seria Lecture Notes in Computer Science (Springer Verlag) 5013, str. 298-314.

C2 Przemysław Błaśkiewicz, Zbigniew Gołębiewski, Marek Klonowski, Krzysztof Majcher: *RFID-tags with Allowers*, IEEE CS (IEEE Computer Society), str. 1–6.

D1 Marek Klonowski, Mirosław Kutyłowski, Anna Lauks: *Repelling Detour Attack against Onions with Re-Encryption*, Seria Lecture Notes in Computer Science (Springer Verlag) 5037, str. 296-308.

D2 Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dudka: *Attacking and Repairing the Improved ModOnions Protocol*, Seria Lecture Notes in Computer Science (Springer Verlag) 5984, str. 258 - 273.

D2' (Rozszerzona wersja D1) Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dudka: *Attacking and Repairing the Improved ModOnions Protocol-Tagging Approach*, Rozszerzona wersja pracy D2 wydana w KSII – Transactions on Internet and Information Systems (4(3): 380-399 (2010)) .

Stosowne, szczegółowe oświadczenie dotyczące wkładu autorów jest umieszczone w załączniku do wniosku.

b) omówienie celu naukowego/artystycznego ww. pracy/prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania.

Ze względu na obszerność omówienia znajduje się ono w części I niniejszego dokumentu (str. 5).

5. **Omówienie pozostałych osiągnięć naukowo - badawczych (artystycznych).**

Ze względu na obszerność omówienia znajduje się ono w części II niniejszego dokumentu (str. 61).

[2] Jako załącznik dołączono także rozszerzoną wersję pracy z uwzględnionymi uwagami recenzentów, która została przyjęta do publikacji w TCS.

Spis treści

Część I

Omówienie cyklu prac

Wstęp

Niniejsza część autoreferatu stanowi opis wyników badań autora dotyczących rozproszonych systemów urządzeń o ograniczonych zasobach ze szczególnym uwzględnieniem aspektów efektywności i bezpieczeństwa komunikacji. Choć prace zawierają w dużej części wyniki teoretyczne (w szczególności analizę algorytmów), są one w całości motywowane względami praktycznymi. Urządzenia o ograniczonych zasobach są szeroko stosowane a ich rola stale rośnie. Podkreślić też należy, że wyróżnia się wiele klas urządzeń tego typu. W niniejszej części zajmować będziemy się tylko niektórymi - wymienić tu należy między innymi systemy zdalnej identyfikacji radiowej (tzw. RFID) i sieci sensorów.

Systemy, o których będzie mowa, są typowymi systemami rozproszonymi. W niektórych przypadkach będziemy nawet badać tzw. sieć *ad hoc*. W szczególności węzły (stacje) mogą nie znać struktury sieci, a często nie posiadają nawet informacji, ile jest aktywnych stacji. Drugą cechą wspólną są ograniczone zasoby - w szczególności mała pamięć, małe moce obliczeniowe i silne ograniczenia energetyczne. Powoduje to, że stacje nie mogą wykonywać zaawansowanych obliczeń kryptograficznych, przechowywać dużej ilości danych a z powodu małych zasobów energetycznych muszą ograniczyć ilość komunikacji.

Mamy zatem systemy rozproszone urządzeń o ograniczonych zasobach. Jednocześnie żąda się, aby ich działanie było efektywne w sensie czasu wykonywania procedur oraz poziomu wykorzystania innych zasobów. Największym jednak wyzwaniem jawi się obecnie zapewnienie **dowodliwego** bezpieczeństwa przetwarzanych danych (w sensie poufności, integralności, dostępności danych czy anonimowości uczestników rozproszonego protokołu).

Oczywiście zapewnienie tego samego poziomu bezpieczeństwa czy efektywności przy ograniczonych zasobach **jest zadaniem trudniejszym a w niektórych przypadkach w ogóle nieosiągalnym**. Co więcej, często analiza skonstruowanych protokołów wymaga wykorzystania nieco innych technik matematycznych. Wynika to między innymi z faktu, że standardowe podejście daje w wielu przypadkach jedynie oszacowanie asymptotyczne, podczas gdy w interesujących nas przypadkach potrzebna jest informacja o własnościach algorytmu już dla małych instancji danego problemu (np. rozmiaru pamięci rzędu kilkudziesięciu bitów). Dlatego na przykład redukcja do problemu NP-zupełnego nie jest wystarczającym argumentem świadczącym o bezpieczeństwie konkretnego rozwiązania. Stąd w niektórych z opisanych niżej prac stosuje się różne techniki - od rozwiązań probabilistycznych, algebraicznych aż po wykorzystywanie pewnych struktur kombinatorycznych i argumentację typową dla teorii gier.

Struktura pracy

Niniejsza część zawiera opis cyklu opublikowanych prac, które zostały oznaczone symbolami A1 (A1'),A2,B1,B2,C1,C2,D1,D2 oraz D2'. Choć wszystkie mówią o komunikacji i bezpieczeństwie systemów ograniczonych urządzeń, dotyczą nieco innych ich klas i dlatego pogrupowane zostały w czterech rozdziałach. Każdy rozdział składa się z dwóch części. Pierwsza stanowi wprowadzenie w specyfikę danej dziedziny i ogólnie omawia obecny stan wiedzy w zakresie potrzebnym do przedstawienia nowych wyników. Drugi zaś stanowi podsumowanie zawartości omawianych prac.

Niniejsza część autoreferatu zawiera następujące rozdziały:

Efektywna komunikacja w sieciach sensorów Rozdział ten opisuje następujące prace:

A1 Marek Klonowski, Mirosław Kutyłowski, Jan Zatopiański: *Energy Efficient Alert in Single-Hop Networks of Extremely Weak Devices*, Seria Lecture Notes in Computer Science (Springer Verlag) 5804, str.139-150.

Praca prezentowana na ALGOSENSORS 2009.

A1' Czasopismowa, rozszerzona wersja pracy A1, przyjęta do druku w *Theoretical Computer Science*[3].

A2 Zbigniew Gołębiewski, Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Leader Election for Multi-Channel Radio Networks –Dependent versus Independent Trials*, IEEE CS (IEEE Computer Society), str. 477-482.

Praca prezentowana na First Asian Conference on Intelligent Information and Database Systems (ACIIDS 2009).

Praca A1 (A1') przedstawia algorytm typu Las Vegas rozgłaszania alarmu w sieci sensorów w modelu bez detekcji kolizji i stacjach o bardzo ograniczonych (nawet jak na tego typu urządzenia) mocach - zarówno obliczeniowych jak i energetycznych. Zaproponowany schemat zapewnia **subloga-rytmiczne zużycie energii przy polilogarytmicznym czasie trwania protokołu**. Poza analizą zaproponowanego algorytmu pokazano także **dolne ograniczenie na czas działania** schematów tego typu. Praca A2 analizuje strategie wyboru lidera dla sieci, w której stacje mogą komunikować się jednocześnie na kilku kanałach komunikacyjnych.

Protokoły dla sieci sensorów odporne na *Sybil-attack* Właściwym wkładem zaprezentowanym tym rozdziale są dwie publikacje:

[3]Praca w wersji czasopismowej ma poprawione drobne błędy rachunkowe i zawiera dowody, które zostały pominięte w publikacji A1. Ponadto uwzględnia uwagi recenzentów z *Theoretical Computer Science*.

B1 Zbigniew Gołębiewski, Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Towards Fair Leader Election in Wireless Networks*, Seria Lecture Notes in Computer Science (Springer Verlag) 5793 str. 166-179.

Praca prezentowana na ADHOC-NOW 2009.

B2 Marek Klonowski, Michał Koza, Mirosław Kutyłowski: *Repelling Sybil-type Attacks in Wireless Ad Hoc Networks*, Seria Lecture Notes in Computer Science (Springer Verlag) 5793 str. 166-179.

Praca prezentowana na ACISP 2010.

Obie prace pokazują **ataki na podstawowe protokoły dla radiowych sieci ad hoc** urządzeń o ograniczonych zasobach polegające na tym, że adwersarz, kontrolując niewielką liczbę stacji, może z wysokim prawdopodobieństwem wpłynąć na rezultat rozproszonego protokołu w sieci radiowej. Wykazano między innymi, że klasyczne protokoły wyboru lidera są bardzo podatne na ataki tego typu a adwersarz posiadając kontrolę nawet nad jedną stacją jest w stanie spowodować, że to ona zostanie liderem z prawdopodobieństwem bliskim 1. Co więcej pokazano, że atak tego typu **w praktyce nie może zostać wykryty**. W pracach B1 oraz B2 zaprezentowano szereg protokołów, które są do pewnego stopnia **odporne na ataki** tego rodzaju. Główna idea metod ochrony, zaproponowana w omawianych publikacjach, opiera się o naturalne (fizyczne) ograniczenia komunikacji radiowej. W szczególności na tym, że kilka stacji nie może skutecznie nadawać w tym samym czasie.

Bezpieczeństwo w systemach RFID Rozdział opisuje tematykę związaną z dwoma pracami:

C1 Jacek Cichoń, Marek Klonowski, Mirosław Kutyłowski: *Privacy Protection for RFID's – Hidden Subset Identifiers*, Seria Lecture Notes in Computer Science (Springer Verlag) 5013, str. 298-314.

Praca zaprezentowana na PERVASIVE 2008.

C2 Przemysław Błaśkiewicz, Zbigniew Gołębiewski, Marek Klonowski, Krzysztof Majcher: *RFID-tags with Allowers*, IEEE CS (IEEE Computer Society), str. 1–6.

Praca prezentowana na IEEE PerSec 2009 (Galveston, TX, USA).

Praca C1 prezentuje schemat **uwierzytelniania dla urządzeń typu RFID o minimalnych mocach obliczeniowych, który zapewnia ochronę prywatności użytkowników**. Praca także przedstawia dowód, że schemat z wysokim prawdopodobieństwem zapewnia teorioinformacyjne bezpieczeństwo, pod warunkiem że adwersarz nie jest w stanie przechwycić więcej niż liniowej (względem rozmiaru pamięci taga) liczby transmisji (odpowiedzi) pochodzących z pojedynczego urządzenia. Druga praca pokazuje **schemat analogiczny do *Blockera*** z pracy Juelsa, Rivesta i Szydlo ([71]), w którym RFID-tag może być odczytany tylko gdy w jego zasięgu jest obecne inne urządzenie,

zwane *Allowerem*. W pracy wykazano, że nowe podejście zapewnia wyższy poziom bezpieczeństwa niż oryginalne rozwiązanie i może być wykorzystane do zaoferowania pożądanych z praktycznego punktu widzenia funkcjonalności użytkownikom systemów RFID.

Protokoły anonimowej komunikacji w systemach rozproszonych o ograniczonej pamięci W tej części skoncentrowano się na pracach:

D1 Marek Klonowski, Mirosław Kutyłowski, Anna Lauks: *Repelling Detour Attack against Onions with Re-Encryption*, Seria Lecture Notes in Computer Science (Springer Verlag) 5037, str. 296-308.

Praca prezentowana na ACNS 2008.

D2 Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dudka: *Attacking and Repairing the Improved ModOnions Protocol*, Seria Lecture Notes in Computer Science (Springer Verlag) 5984, str. 258 - 273.

Prezentowana na ICISC 2009.

D2' Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dudka: *Attacking and Repairing the Improved ModOnions Protocol-Tagging Approach*, Rozszerzona wersja pracy D2 wydana w KSII – Transactions on Internet and Information Systems (4(3): 380-399 (2010)) .

Prace przedstawiają metody anonimowej komunikacji odporne na tzw. *ataki powtórzeniowe*. Podobnie jak wcześniejsze rozwiązania ochrony przed atakami tego typu, zaproponowane protokoły oparte są na reszyfrowaniu uniwersalnym. Poprzednie protokoły, mimo zalet, podatne były na różne klasy innych zagrożeń. Prace D1 i D2 prezentują **zmodyfikowane wersje wcześniejszych protokołów o znacznie wyższym poziomie bezpieczeństwa**. Zaprezentowane rozwiązania mogą też być stosowane w innych protokołach komunikacyjnych w celu efektywnej weryfikacji poprawności działania ich uczestników oraz uodpornienia na szeroką klasę zagrożeń integralności danych.

Rozdział 1

Efektywna komunikacja w sieciach sensorów

Niniejszy Rozdział poświęcony jest sieciom ad hoc urządzeń o ograniczonych zasobach, które komunikują się drogą radiową.

1.1 Model i algorytmika radiowej sieci ad hoc

Zarówno w tym Rozdziale, jak też w Rozdziale 2 badana sieć składa się urządzeń nazywanych *stacjami* – ze względu na zastosowania można myśleć o sensorach, które mierzą pewne własności środowiska i komunikują się drogą radiową. Urządzenia takie mają zazwyczaj bardzo ograniczone moce obliczeniowe. W badanym modelu czas jest dyskretny – wszelkie akcje wykonywane są w kolejnych *rundach*[1]. W każdej rundzie stacja może wykonywać dwa podstawowe typy akcji - *nadawać* komunikaty lub (albo) *nasłuchiwać* na kanale komunikacyjnym. W każdej rundzie dodatkowo może wykonywać obliczenie lokalne. Słuchająca stacja odbierze wiadomość wtedy, gdy dokładnie jedna stacja nadaje. Jeżeli więcej niż jedna stacja nadaje, występuje *kolizja*. W zależności od założeń może ona być odróżnialna od stanu, w którym żadna stacja nie nadaje (model z detekcją kolizji). Jeśli natomiast stan kanału komunikacyjnego w rundzie, gdzie żadna stacja nie nadaje, jest nierozróżnialny od tego jaki się da zaobserwować w przypadku nadawania kilku stacji, mówimy o *modelu bez detekcji kolizji*[2]. Wszystkie stacje są w zasięgu swojego nadawania – mówimy zatem o modelu sieci *single hop*. Stacje są zsynchronizowane, tak jakby miały dostęp do globalnego zegara.
Zakładamy, że stacje posiadają stochastycznie niezależne, idealne generatory bitów losowych. Sieć działa w trybie *ad hoc* – przed rozpoczęciem protokołu nie jest znana jej dokładnia struktura. W szczególności nie jest znana liczba urządzeń obecnych w sieci. W przypadku modelu z adwersarzem nie jest zaś znany podzbiór stacji kontrolowanych przez adwersarza. Model taki jest po-

[1] Funkcjonuje też termin *sloty*.
[2] noCD model

wszechnie rozważany w literaturze (np. [101, 102]) i uważa się go za stosunkowo realistyczne przybliżenie niektórych typów rzeczywistych sieci. Warto podkreślić, że w przypadku wielu problemów komunikacyjnych model taki jest niemal tożsamy z modelami kanału wielodostępowego (MAC, *Multiple Access Channel*) co widać między innymi w pracach [10, 28, 119].

Typowe procedury dla radiowych sieci ad hoc

Radiowa sieć ad hoc, aby mogła wykonywać określone zadania, musi przeprowadzić działania samoorganizujące, co najczęściej sprowadza się do wykonania jednej lub kilku następujących procedur.

Wybór lidera Problem wyboru lidera (*leader election*) polega na tym, że po wykonaniu protokołu

- dokładnie jedna stacja otrzymuje status *lider* a pozostałe stacje otrzymują status *nie-lider*;
- każda stacja zna swój status.

Protokoły wyboru lidera badane były między innymi w [12, 101, 102, 119].

Inicjalizacja Problem inicjalizacji (*initialization*) polega na tym, że po wykonaniu protokołu dla sieci n stacji

- każda stacja otrzymuje unikalny w skali sieci identyfikator – liczbę naturalną ze zbioru $\{1, \ldots, n\}$;
- każda stacja zna swój identyfikator.

Protokoły inicjalizacji prezentowane były między innymi w [62, 89].

Szacowanie rozmiaru Problem szacowania rozmiaru (*size approximation*) polega na tym, że po wykonaniu protokołu dla sieci n stacji wszystkie stacje znają pewną liczbę n^*, taką że $1/c \cdot n \leq n^* \leq c \cdot n$ dla pewnego ustalonego $c \geq 1$. Zazwyczaj rozpatrywane są zrandomizowane analogi tego problemu a n^* stanowi nieobciążony estymator o możliwie małej wariancji. Protokoły szacowania rozmiaru sieci opisane zostały między innymi w pracach [26, 74].

Należy też wspomnieć o niektórych innych protokołach będących obiektem intensywnych badań - przykładem może być problem **k-selekcji** ([85]).

Kryteria oceny algorytmów W przypadku algorytmów dla sieci ad hoc przy ich ocenie bierze się pod uwagę klasyczne wskaźniki takie jak **złożoność czasowa** czy **złożoność pamięciowa** ([107]). Dodatkowym rozważanym parametrem jest **złożoność energetyczna** blisko związana ze **złożonością komunikacyjną**. Złożoność energetyczna jest badana ze względu na fakt, że stacje są zazwyczaj zasilane bateryjnie i rozlokowane na bardzo rozległym, nierzadko trudno dostępnym, terenie. Przez to nie ma możliwości zwiększenia ich zasobów energetycznych. Właśnie konieczność ograniczania energii powoduje, że konstrukcje algorytmów dla radiowych sieci ad hoc istotnie różnią się od innych algorytmów rozproszonych. W przypadku algorytmów dyskretnych, przez *wydatek energetyczny stacji* rozumie się liczbę rund, w których stacja nadaje komunikat bądź nasłuchuje na kanale komunikacyjnym. Przez *złożoność energetyczną* algorytmu rozumie się maksymalny wydatek energetyczny wszystkich stacji biorących udział w protokole.

Warto nadmienić, że w niektórych pracach przyjmuje się jako złożoność energetyczną średnią z wydatku energetycznego wszystkich stacji. Podejście takie wydaje się niewłaściwe w przypadku systemów gdzie zakłada się, że aby system mógł funkcjonować, **wszystkie** urządzenia muszą być sprawne.

W części prac (np. [23, 24]) przyjmuje się, że wydatek energetyczny to liczba rund, w których stacja nadaje a nie są uwzględniane rundy, w których stacje nasłuchują. Wynika to ze spostrzeżenia, że w przypadku niektórych urządzeń nadawanie jest znacznie bardziej energochłonne niż nasłuchiwanie.

1.2 Nowe wyniki - Algorytm alarmu (Praca A1)

W tym podrozdziale zaprezentowane zostaną wyniki z publikacji stanowiącej pracę A1 (A1')[3].

1.2.1 Algorytmy alarmu

W A1 rozważany jest następujący problem alarmu (*alert problem*)- w sieci jest n stacji ponumerowanych kolejnymi liczbami naturalnymi. Zakłada się, że pewne $0 \leq n_0 \leq n$ spośród wszystkich stacji jest *wzbudzonych*. Problem alarmu jest poprawnie rozwiązany, jeżeli po wykonaniu algorytmu wszystkie stacje mają informację czy choć jedna stacja jest wzbudzona (tzn. czy $n_0 > 0$). Problem taki ma naturalną interpretację – można tu myśleć o sieci zaimplementowanej w celu wykrycia pewnego zdarzenia - na przykład pożaru albo powodzi. Jeśli choć jedna ze stacji - detektorów wykryje dane zdarzenie, powinna możliwie szybko poinformować o tym wszystkie inne stacje.

Model W badanym modelu przyjmuje się sieć single hop bez detekcji kolizji (noCD-model), zatem sytuacja w której więcej niż jedna stacja nadaje jest nierozróżnialna od tej, w której żadna stacja nie nadaje.

[3]Szanownemu Czytelnikowi uprzejmie sugeruje się skorzystanie z rozszerzonej i poprawionej wersji pracy oznaczonej jako A1', uwzględniającej dodatkowo uwagi recenzentów z *Theoretical Computer Science*.

Stacje działają w trybie *half duplex* - to znaczy, że stacja może w pojedynczej rundzie nadawać wiadomość lub nasłuchiwać. Nie może jednak wykonywać obu tych akcji jednocześnie (w tej samej rundzie). W szczególności stacja nie wie czy udało się jej poprawnie nadać wiadomość.

Model taki rodzi następujący problem – jeśli wzbudzone stacje nadają w kolejnych rundach z ustalonym, małym prawdopodobieństwem (na przykład rzędu $\Theta(1/n)$) w przypadku gdy $n_0 > 0$ ale $n_0 = o(n)$ czas oczekiwania na nadawanie pojedynczej wzbudzonej stacji jest długi. Z kolei zastosowanie wysokiego np. stałego prawdopodobieństwa spowoduje, że z wysokim prawdopodobieństwem w kolejnych rundach następować będą nadawania więcej niż jednej stacji jednocześnie (kolizje), co także prowadzić będzie do długiego czasu wykonania protokołu. Można pokazać, że zastosowanie bardziej wyrafinowanych, klasycznych strategii jak na przykład algorytmu wzorowanego na *podwójnie wykładniczym algorytmie Willarda* ([119]) wymaga długiego czasu wykonania protokołu lub prowadzi do wysokiej złożoności energetycznej protokołu.

Stacje podzielone są na *strażników* (*guardians*) oraz *detektory* (*detectors*). W protokole zakłada się *explicite*, że strażnicy są ponumerowani kolejnymi liczbami naturalnymi. Numeracja ta może zostać jednak wykonana **jednorazowo** przy implementacji sieci dla małej (rzędu $O((\log n)^3)$) liczby urządzeń względem liczby wszystkich stacji (parametr n). W pracy A1' pokazano jak te założenia można istotnie osłabić.

1.2.2 Algorytm EEAA

W pracy A1 (A1') pokazany jest algorytm EEAA[4] rozwiązujący wyżej zdefiniowany problem alarmu w opisanym modelu. Procedura składa się z czterech faz.

Faza 1 - jest zrandomizowana i trwa $O(\log^3(n))$ rund. W tej fazie każda wzbudzona stacja nadaje w l rundach wybranych z rozkładem jednostajnym spośród wszystkich rund tej fazy. Dla każdej rundy tej fazy wyznaczona jest stacja - strażnik do nasłuchiwania komunikatów.

Faza 2 - jest zrandomizowana i trwa $O(\log^3(n))$ rund. W tej fazie każda wzbudzona stacja nadaje w dokładnie jednej, losowo wybranej rundzie. Prawdopodobieństwa nadania w kolejnych rundach nie są jednak takie same. W każdej rundzie tej fazy wyznaczona jest stacja - strażnik do nasłuchiwania komunikatów.

Faza 3 - jest deterministyczna i trwa $O(\log^3(n))$ rund. Kolejni strażnicy przekazują sobie sygnał alarmu, o ile sami go usłyszą we wcześniejszych fazach.

Faza 4 - jest deterministyczna i trwa stałą liczbę rund. Wybrany strażnik rozgłasza alarm wszystkim stacjom.

Wartość l jest parametrem protokołu. Dla uzyskania optymalnych wartości przyjęto $l = \frac{\log(n)}{\log\log(n)}$. Można w uproszczeniu stwierdzić, że Faza 1 algorytmu służy „przechwyceniu" sygnału alarmowego jeśli liczba wzbudzonych stacji jest mała w stosunku do n. Faza 2 służy wykryciu alarmu dla przypadku gdy $n_0 = \Omega(n^\alpha)$, dla pewnego $\alpha > 0$.

[4]Nazwa–akronim pochodzi od Energy Effective Alert Algorithm.

Główny rezultat W pracy A1 (A1') udowodniono następujące twierdzenie

Twierdzenie 1.3 (Theorem 1 z A1')**.** *Algorytm EEAA*

1. *wykonywany jest w czasie* $O(\log^3(n))$*;*
2. *ma złożoność energetyczną* $O\left(\frac{\log(n)}{\log\log(n)}\right)$*;*
3. *wykonywany jest poprawnie z prawdopodobieństwem nie mniejszym niż* $1-\frac{3}{n}$ *dla dowolnego podzbioru wzbudzonych stacji.*

Dowód powyższego twierdzenia sprowadzony zostaje do analizy modelu kul i urn. Wymaga się oszacowania prawdopodobieństwa, że pojawi się pewna urna z dokładnie jedną kulą. W stosunku do klasycznego modelu z [3] bada się jednak przypadek, w którym kule nie są umieszczane w urnach wybieranych z rozkładem jednostajnym. W dowodzie wykorzystuje się między innymi martyngałową nierówność Azumy - Hoeffdinga.

Modyfikacje, rozszerzenia i uwagi

Nieadaptatywność - w algorytmie większość stacji (poza strażnikami) wykonuje algorytm nieadaptatywny[5] i poza Fazą 4 w ogóle nie musi nasłuchiwać.

Numerowanie stacji - w pracy A1 (A1') zakłada się, że stacje są ponumerowane. Założenie to może być znacząco osłabione poprzez niewielką modyfikację algorytmu. Podkreślmy, że nawet w zaprezentowanej formie potrzeba jedynie ponumerowania małego podzbioru strażników.

Znana liczba stacji - w pracy zakłada się też, że liczba wszystkich stacji (parametr n) jest znana. W praktyce jednak wystarczy nawet mało precyzyjne oszacowanie tej wartości.

Szczegółową dyskusję na temat rozwinięć algorytmu EEAA znaleźć można w rozdziale 3.2 pracy A1'.

1.3.1 Ograniczenie dolne

W pracy A1 (A1') pokazano także następujące ograniczenie dolne dla algorytmów typu Monte Carlo dla problemu alarmu w określonym wyżej modelu.

Twierdzenie 1.4 (Theorem 9 z A1')**.** *Nie istnieje zrandomizowany algorytm alarmu, który daje poprawną odpowiedź dla dowolnego podzbioru wzbudzonych stacji z prawdopodobieństwem nie mniejszym niż* $1-1/n$*, czasem wykonania* $t<n$ *i złożonością energetyczną* $l<\frac{\log(n/2)}{\log(t)}$*.*

Kombinatoryczny dowód tego twierdzenia jest niekonstrukcyjny. Wnioskiem z niego jest asymptotyczna optymalność algorytmu EEAA.

[5] ang. *oblivious*

1.4.1 Prace powiązane

Istnieje wiele publikacji, w których rozważane są problemy podobne do alarmu. Wskazać należy przede wszystkim prace [23, 24, 49, 73], gdzie badany jest *wake-up problem*. Celem prezentowanych w tych pracach algorytmów jest to, aby pojedyncza stacja „obudziła" wszystkie inne stacje przesyłając im sygnał. Główna różnica polega na tym, że w zacytowanych publikacjach przyjmuje się założenie o tym, że stacje zużywają swoją energię jedynie gdy nadają. To prowadzi do zupełnie innej konstrukcji algorytmów.

Inną pracą związaną z A1 jest [98], w której autorzy rozważają podobny do alarmu problem dla ogólnych sieci o topologii UDG (*Unit Disc Graph*). Zaproponowany algorytm jest jednak mniej efektywny dla sieci typu single-hop rozważanej w A1. Autorzy zakładają, że nasłuchiwanie także zużywa energię. Mimo to, w pracy [98] przyjęta została inna miara złożoności energetycznej algorytmu niż w A1.

Kolejna praca, w której dyskutowany jest protokół alarmu to [25]. Obiektem badań jest jednak sieć multi-hop w innym modelu energetycznym i komunikacyjnym. Do pewnego stopnia problem alarmu podobny jest do szczególnych przypadków k-selekcji (np. [85]), niemniej dotychczas problem ten nie był rozważany z punktu widzenia złożoności energetycznej.

Bezpośrednią kontynuacją badań z pracy A1 jest przyjęta do publikacji praca [95], gdzie zaprezentowany jest protokół k-alert, w którym sygnał alarmu ma być rozprzestrzeniany, gdy $n_0 > k$. Innymi słowy, alarm jest ogłaszany, gdy liczba wzbudzonych stacji przekroczy k.

1.5 Nowe wyniki - wybór lidera w systemie wielokanałowym (Praca A2)

Przedmiotem badań, których wyniki przedstawione zostały w pracy A2 jest uogólnienie problemu wyboru lidera na system wielokanałowy – stacje w każdej rundzie mogą nadawać na k kanałach. Gdy dwie stacje w jednej rundzie nadają na różnych kanałach, nie powoduje to kolizji. Celem protokołu jest doprowadzenie do tego, aby wyłoniony został lider, czyli stacja która jako jedyna nada sygnał na pewnym kanale przy małym zużyciu energii oraz w możliwie krótkim czasie (w sensie wartości oczekiwanej). Zauważmy, że problem ten może być wyrażony w sposób ekwiwalentny w języku procesów, które chcą jako jedyne uzyskać dostęp do jednego z k kanałów wielodostępowych (analogicznie do klasycznego *Multiple Access Channel*, [10, 28]). Główne rezultaty dotyczą porównania algorytmów, w których każda stacja niezależnie nadaje w każdej rundzie sygnał, stosując jedną z dwóch strategii:

Strategia ITA Stacja z ustalonym prawdopodobieństwem p decyduje czy nadawać. Jeżeli decyzja jest pozytywna, stacja na każdym spośród k kanałów nadaje niezależnie z prawdopodobieństwem q.

Strategia STA Stacja z ustalonym prawdopodobieństwem p decyduje czy nadawać. Jeżeli decyzja jest pozytywna, stacja nadaje na **dokładnie jednym** kanale, który jest wybrany spośród k ka-

nałów z rozkładem jednostajnym – każdy z kanałów jest wybierany z prawdopodobieństwem $1/k$.

W pracy A2 analizowano powyższe strategie. Podkreślmy, że mimo formalnego modelu prace w niektórych miejscach nie zawierają formalnych dowodów - postawiono jedynie hipotezy poparte jednak dużą liczbą wiarygodnych wyników numerycznych. Z rozważań wynikają następujące fakty:

Fakt 1.

- *Strategia ITA jest optymalna dla $p = 1$ oraz $q = 1/n$. (A2, Rozdział 2.1)*
- *Strategia STA jest optymalna dla $p = k/n$. (A2, Rozdział 2.2)*
- *Strategia ITA dla optymalnych parametrów jest szybsza, oraz wymaga mniejszej energii w sensie wartości oczekiwanej. (A2, Rozdział 3)*
- *Strategia STA jest bardziej stabilna - wariancja próbkowa jest istotnie mniejsza. (A2, Rozdział 3)*

Uwagi Praca A2 zawiera także dyskusję na temat omówionych strategii w modelu, w którym znane jest jedynie oszacowanie na liczbę stacji n.

Zaprezentowane algorytmy mogą być stosowane nie tylko w systemach urządzeń, które nadają na fizycznych, różnych częstotliwościach, ale także w sytuacji gdy następuje nadawanie na pojedynczym kanale przy użyciu kodów ortogonalnych albo pewnych kodów korygujących błędy.

Zaprezentowane wyniki, obliczenia oraz eksperymenty numeryczne omówione w pracy A2 miały na celu jedynie wykazanie istnienia znaczących różnic i pewnych niespodziewanych zjawisk w naturalnym modelu dla praktycznych (niewielkich) rozmiarów instancji rozważanego problemu. Asymptotyczne rachunki z tej pracy mogą być przeprowadzone ze znacznie większą dokładnością – na przykład przy zastosowaniu metod analizy kombinatorycznej, w szczególności stosując techniki z książki [112] (Rozdziały II oraz VI). Dalej wzór (1) z A2 jest przykładem sumy dwumianowej, które są omówione na przykład w [45]. Podanie dokładnej asymptotyki jest ciekawym zadaniem teoretycznym, ale wydaje się mieć niewielkie znaczenie praktyczne.

Rozdział 2

Protokoły dla sieci sensorów odporne na Sybil-attack

W niniejszym rozdziale dyskutowane będą zagadnienia związane z bezpieczeństwem radiowej sieci ad hoc, której model opisany został w Rozdziale 1. Zasadniczą cześć rozdziału stanowi opis wyników publikacji B1 i B2, gdzie rozpatruje się zagrożenie tzw. *Sybil attack* [1] dla tego typu sieci.

2.1 Sybil attack w sieciach sensorów

Sybil attack (SA) polega na tym, że uczestnik wielostronnego protokołu stara się zdobyć wpływ na system, niewspółmierny do posiadanych zasobów, poprzez tworzenie nadmiarowych tożsamości. Celem adwersarza może być uzyskanie dostępu do zwiększonej ilości zasobów. Atak ten obecny był w różnych postaciach wcześniej w literaturze, atoli zdefiniowany został dopiero w [38].

Implementacja tego ataku może znacząco się różnić w przypadku różnych systemów. Był on szeroko dyskutowany w systemach P2P (gdzie celem adwersarza jest uzyskanie dostępu do większej ilości zasobów – na przykład danych czy przepustowości kanału komunikacyjnego) lub systemach kont pocztowych (tu w naturalnym celem jest rozsyłanie SPAMu). Dla każdego typu systemów zaproponowano inne metody ochrony (np. [15, 30]).

Podobnie SA może być realizowany w radiowej sieci ad hoc - adwersarz kontrolując pewną liczbę stacji symuluje dodatkowe, *nadmiarowe* stacje, aby zdobyć większą kontrolę nad systemem. Ochrona przed SA w radiowych sieciach ad hoc jest bardzo trudna z kilku powodów. Wymienić tu należy:

- brak ustalonej, wiarygodnej infrastruktury - w wielu przypadkach nie da się stwierdzić jaka jest topologia sieci, w szczególności, ile działa w niej fizycznych stacji;

[1] W języku polskim brak jest tłumaczenia tego pojęcia. Sam termin pochodzi od cierpiącej na zaburzenie dysocjacyjne tożsamości (rozdwojenie jaźni, *multiple personality*) bohaterki książki Flory Schreiber *Sybil*.

- nie ma możliwości stosowania zaawansowanych metod kryptografii asymetrycznej ze względu na ograniczone moce obliczeniowe i małą pamięć;
- w realistycznych modelach nie ma możliwości uniknięcia przejęcia i fizycznej penetracji przez adwersarza części urządzeń wraz z zawartym w ich pamięci materiałem kryptograficznym;
- metody oparte o ustanawianie wspólnych sekretów[2], schematy predystrybucji są trudne w realizacji;

Ponadto, wskazać też trzeba na wszystkie inne problemy typowe dla dużych systemów rozproszonych – w szczególności brak centralnej jednostki mającej pełną wiedzę lub pełniącą rolę arbitra.

Wcześniejsze rezultaty Należy podkreślić, że ataki przeciw systemom ad hoc są problemem stosunkowo nowym i trudno wskazać ogólne, zaakceptowane w badaniach teoretycznych i w rzeczywistych implementacjach rozwiązania. Dzieje się też tak dlatego, że metody ochrony pozostają w silnej zależności z przyjętym modelem. W kontekście sieci ad hoc niewiele jest rezultatów dotyczących SA. Nieliczne prace, na przykład [27, 51, 103, 108], dotyczą mobilnych urządzeń w sieci multi-hop lub sieci z predystrybuowanym kluczem. Modele te istotnie różnią się od tego zakładanego w pracach B1 i B2.

2.2 Nowe Wyniki - Algorytm wyboru lidera a Sybil attack (praca B1)

W pracy B1 rozpatrywane są algorytmy wyboru lidera w radiowej sieci ad hoc. (Opis samego problemu znajduje się w Rozdziale 1). Można zauważyć, że we wszystkich klasycznych algorytmach wyboru lidera dla radiowej sieci (np. [12, 102, 101, 96, 119]), każda stacja obecna w systemie jest wybierana liderem z takim samym prawdopodobieństwem.

Model adwersarza W modelu przyjęto następujące założenia. Adwersarz kontroluje m stacji, które mają takie same możliwości jak n pozostałych, *uczciwych* stacji. Stacje adwersarza mają jednak nieograniczone zasoby energetyczne. Celem adwersarza jest przyjęcie takiej strategii, aby status lidera otrzymała jedna z m kontrolowanych przez niego stacji z możliwie wysokim prawdopodobieństwem. Oczywiście, przejęcie roli lidera przez stację kontrolowaną przez adwersarza może stanowić punkt wyjścia do innych ataków. Dodatkowo, atak taki powinien być możliwie trudny do wykrycia – to znaczy, wykonanie algorytmu z udziałem adwersarza powinno być bliskie, jako proces losowy, wykonaniu bez obecności adwersarza. W ujęciu formalnym może oznaczać to zbieżność według prawdopodobieństwa wraz z parametrem n odpowiednich rozkładów. W

[2]Na przykład protokoły typu *key predistribution* ([108]).

pracy B1 są to rozkłady nad ciągami możliwych stanów kanału komunikacyjnego a jako sposób porównywania rozkładów przyjęto Definicję 2.2.1.

Model ataku odpowiada sytuacji, w której adwersarz przejmuje część stacji. Ze względu na nieograniczone zasoby energetyczne w dalszej analizie nie bierzemy pod uwagę ataków typu DoS, możliwych do przeprowadzenia w oczywisty sposób poprzez stałe blokowanie kanału komunikacyjnego. Zauważmy jednak, że tego typu atak zostanie szybko zauważony, dlatego przyjęte założenie jest realistyczne.

2.2.1 Negatywne wyniki - niewykrywalność Sybil attack w klasycznych schematach

W Rozdziale 2 pracy B1 pokazano, że atak adwersarza, mającego na celu uzyskanie statusu lidera, jest w praktyce niewykrywalne w przypadku klasycznych protokołów. Ponadto atak taki wymaga od adwersarza relatywnie małego wydatku energetycznego, dlatego może on być przeprowadzany wielokrotnie. Atak przeanalizowano w pracy B1 na przykładzie protokołu `Ethernet Trial`[3] ([96]). Obserwacje z pracy B1 jednak da się rozszerzyć w prosty sposób na wszystkie klasyczne protokoły wyboru lidera, w szczególności te z prac [12, 101, 102, 119].

Algorithm 1 Metoda `Ethernet Trial` dla pojedynczej stacji

```
1: loop
2:   if decyduje nadawać z prawdopodobieństwem p then
3:     wysyła(ID);
4:   end if
5:   if jedyna stacja nadaje then
6:     return LEADER = przesłana ID;
7:   end if
8: end loop
```

Można zauważyć, że w przyjętym modelu wykonanie protokołu `Ethernet Trial` jest zmienną losową o wartościach w zbiorze ciągów nad zbiorem trzyelementowym (cisza, pojedyncze nadawanie oraz kolizja[4]). Zbiór ten reprezentuje możliwe stany kanału komunikacyjnego. Do porównywania wykonania protokołów w naturalny sposób można wykorzystać definicję nierozróżnialności (*indistningushability*).

Definicja 2.2.1. *Dyskretne zmienne losowe X, Y są (α, δ)-nierozróżnialne, jeśli istnieje zbiór A, taki że:* $\Pr[X \in A] \geq 1 - \delta, \Pr[Y \in A] \geq 1 - \delta$ *i dla każdego $a \in A$ zachodzi*

$$\frac{1}{\alpha} \leq \frac{\Pr[X = a]}{\Pr[Y = a]} \leq \alpha.$$

[3] W oryginalnej pracy nazwa protokołu jest inna. Nazwa `Ethernet Trial` używana jest w kontekście sieci ad hoc.

[4] Tylko w modelu z detekcją kolizji

Definicja ta jest powszechnie stosowana w literaturze dotyczącej bezpieczeństwa komputerowego (np. [18, 40, 41]), szczególnie w kontekście tzw. *differential privacy*. Wdaje się ona być bardziej użyteczna (choć zazwyczaj trudniejsza w analizie) do porównywania rozkładów w kontekście detekcji działania adwersarza niż na przykład *separation distance* lub oparty o normę L_1 *total variation distance*, które są powszechnie używane przy badaniach nad anonimowością.

Dla `Ethernet Trial` w Rozdziale 2 pracy B1, pokazano między innymi następujące fakty:

Fakt 2 (Lemat 1 w B1)**.** *Jeśli stacje adwersarza nadają z prawdopodobieństwem p_z, a pozostałe stacje z prawdopodobieństwem $p \leq p_z$, wtedy stacja adwersarza zostaje liderem z prawdopodobieństwem*

$$\frac{mp_z(1-p)}{mp_z(1-p) + np(1-p_z)}.$$

Fakt 3 (Lemat 2 w B1)**.** *Rozkład czasu trwania protokołu potrzebnego do wybrania lidera jest taki sam gdy **dokładnie jedna** stacja w sieci zostanie przejęta przez adwersarza, który nadaje z **dowolnym** prawdopodobieństwem, jak w przypadku gdy adwersarz nie jest obecny w sieci (wszystkie stacje postępują zgodnie z protokołem).*

Fakt 4 (Lemat 3 w B1)**.** *Istnieje strategia adwersarza, która zapewnia, że jedyna stacja kontrolowana przez adwersarza może nadawać z prawdopodobieństwem $p_z \leq 1/2$ a wykonanie protokołu jest $(3, 0.3)$- nierozróżnialne od wykonania protokołu bez obecności adwersarza.*

Wszystkie powyższe rezultaty dotyczą zarówno modelu z detekcją kolizji (rozróżniane są sytuacje, gdy żadna stacja nie nadaje od sytuacji gdy więcej niż jedna stacja nadaje) jak też bez detekcji kolizji. Z praktycznego punktu widzenia najistotniejsza jest trzecia obserwacja. Jej konsekwencją jest to, że wykonanie protokołu, nawet z relatywnie agresywnym adwersarzem, ma rozkład bliski temu bez obecności adwersarza. Oznacza to, że nie można zbudować strategii wykrywającej adwersarza zapewniającej jednocześnie akceptowalny poziom błędów I i II rodzaju. Niektóre wyniki pracy B1 zostały rozszerzone w pracy [79]. W szczególności pokazano, że dla sieci bez detekcji kolizji, Fakt 4 może zostać znacząco doprecyzowany (Twierdzenie 2.3). Z drugiej strony nie ma możliwości asymptotycznego poprawienia wyniku dla modelu z detekcją kolizji (Twierdzenie 2.4). Modele te zatem pod względem teoretycznym są istotnie różne. Dokładniej, niech zmienne losowe X oraz $X^*(p)$ oznaczają wykonanie protokołu odpowiednio bez udziału adwersarza oraz z adwersarzem, którego jedyna stacja nadaje z prawdopodobieństwem p w każdej rundzie zanim lider zostanie wybrany.

Twierdzenie 2.3. *Dla modelu bez detekcji kolizji zmienne losowe X oraz $X^*(p)$ są (ε, δ)-nierozróżnialne*

dla

$$\varepsilon \geq 1 \textit{ oraz } \delta = 1 - O\left(\left(\frac{3}{4}\right)^{\frac{n}{p}}\right),$$
$$\frac{4}{5}\frac{p}{n} < \varepsilon < 1 \textit{ oraz } \delta = 1 - O\left(\left(\frac{3}{4}\right)^{\frac{n}{2p}\varepsilon}\right).$$

Twierdzenie 2.4. *Rozważmy model z detekcją kolizji. Jeśli X oraz $X^*(p)$ są (ε, δ) -nierozróżnialne, wtedy $\delta = \Omega(1)$ (względem n).*

Inne algorytmy odporne Algorytm wyboru lidera odporny na działanie adwersarza analizowany był w [88] – zaprezentowany tam protokół działał jednak przy założeniu **adwersarza zewnętrznego**, co w praktyce oznaczało że stacje posiadają ustalony, nieznany adwersarzowi sekret. Ponadto adwersarz miał ograniczone zasoby energetyczne. Powstało także kilka prac badających działanie adwersarza chcącego uniemożliwić wykonanie protokołu. Wskazać tu należy szczególnie prace [36, 51]. Nieco szersze omówienie zagadnienia odpornych algorytmów można znaleźć w Rozdziale 1.1 pracy B1 tudzież Rozdziale 1 pracy B2.

2.4.1 Algorytm wyboru lidera odporny na Sybli attack

Kolejny rezultat pracy B1 (Rozdział 3) to konstrukcja i analiza algorytmów wyboru lidera, która zapewnia odporność na SA. W zaproponowanych rozwiązaniach adwersarz może uniemożliwić wyłonienie lidera (atak typu DoS) ale nie może zmienić rozkładu wybieranych stacji – przy optymalnej dla adwersarza strategii, lider jest wybierany z jednostajnym rozkładem spośród wszystkich stacji w sieci.

Algorytm dla sieci z pełną wiedzą o kanale i ograniczonym adwersarzem

W podrozdziale 3.2 pracy B1 pokazano algorytm dla sieci, w której adwersarz nie może symulować dodatkowych stacji ale stacje posiadają pełną wiedzę na temat stanu kanału komunikacyjnego - mogą nasłuchiwać i nadawać jednocześnie.

Zaproponowany algorytm działa w średnim czasie $O(n \log n)$, jeżeli adwersarz nie podejmuje działań mających na celu wydłużanie działania algorytmu (tj. ataków typu DoS). Główną procedurą wykorzystywaną w opisanym protokole jest *weryfikowalna gra dla dwóch stacji* [5], dzięki której można losowo wybrać w weryfikowalny sposób jedną z dwóch stacji. Ponadto wykorzystane zostały typowe mechanizmy stosowane dla sieci ad hoc zmodyfikowane w taki sposób, aby wykryć odstępstwa od protokołu.

[5] W pracy B1 określona jako *Verifiable parity game in ad hoc network*. Stanowi analogon typowej *Parity game* wykorzystywany w algorytmicznej teorii gier ([105]), który został dostosowany do modelu radiowych sieci ad hoc.

Algorytm dla modelu z niepełną wiedzą o sieci i nieograniczonym adwersarzem

Podrozdział 3.3 przedstawia algorytm dla modelu, w którym stacje nie mają pełnej wiedzy o kanale komunikacyjnym co wynika z faktu, że nie mogą jednocześnie nadawać i odbierać komunikatów (model taki jest bliski niektórym ze standardów IEEE 802.11). Adwersarz może jednak symulować dowolną liczbę stacji - jak przy typowym założeniu dotyczącym SA. Dodatkowo zakłada się, że stacje posiadają możliwość obliczania wartości jednokierunkowej funkcji haszującej. Stacje nie mają jednak żadnego ustalonego sekretu przed wykonaniem protokołu (Jak na przykład zakładano w [108]). Protokół wykorzystuje kilka procedur pomocniczych i składa się z trzech faz.

Tworzenie listy wszystkich identyfikatorów (stacji) - w pierwszej fazie tworzona jest lista wszystkich deklarowanych identyfikatorów. Lista ta **może** zawierać większą liczbę identyfikatorów niż jest fizycznych urządzeń obecnych w sieci.

Wybór kandydata na lidera - stacje w rozproszony sposób permutują listę identyfikatorów. Pierwszy identyfikator zostaje *kandydatem na lidera*.

Testowanie kandydata na lidera - stacje w rozproszony sposób testują kandydata. Sprawdza się, czy kandydat na lidera jest zgłoszony przez stację inną niż stacje, które brały udział w zgłaszaniu pozostałych identyfikatorów na listę.

Główny pomysł algorytmiczny opiera się na tym, że stacje są zmuszane do nadawania w rundach wskazanych w pseudolosowy sposób. Z założeń wynika, że w tych rundach stacja nie zna stanu kanału - nie wie zatem czy komunikat został prawidłowo nadany. Pozostałe stacje mogą jednak obserwować stan kanału. Algorytm działa w czasie $O(n \log n + t)$, gdzie t jest parametrem bezpieczeństwa.

Ponadto uzasadniono w podrozdziale 3.1 następujący fakt:

Fakt 5. *Załóżmy, że adwersarz może symulować dowolną liczbę stacji oraz może nasłuchiwać stan kanału komunikacyjnego i nadawać jednocześnie. W takim modelu może on zastosować strategię taką, aby prawdopodobieństwo zostania liderem przez kontrolowaną przez niego stację było dowolnie bliskie* 1.

2.5 Generyczne metody ochrony radiowej sieci przed Sybil attack (praca B2)

W pracy B2 zaproponowano ogólną metodę ochrony przed SA. Algorytm można traktować jako specyficzny protokół inicjalizacji (opis w Rozdziale 1) odporny na SA. Dokładniej, żądamy żeby po wykonaniu algorytmu stworzona została znana wszystkim stacjom lista unikalnych identyfikatorów, taka że

- każda uczciwa stacja posiada dokładnie jeden identyfikator;
- liczba identyfikatorów nie przekracza liczby stacji.

Model i założenia Rozważa się typowy model sieci radiowej ad hoc z detekcją kolizji jak w opisie Rozdziału 1. Stacja nie może jednocześnie słuchać i nadawać. Stacje posiadają dostęp do niezależnych źródeł bitów pseudolosowych. Stacje adwersarza mogą mieć pewien ustalony sekret nieznany uczciwym stacjom. Nie mogą jednak porozumiewać się innym kanałem komunikacyjnym podczas wykonywania protokołu. Ponadto wymaga się spełnienia dwóch niestandardowych, choć łatwych do realizacji w praktyce, założeń:

1. Adwersarz kontroluje m stacji a ponadto jest w sieci n stacji wolnych od wpływu adwersarza. Zakłada się, że $N_{min} \leq n$ oraz $n+m \leq N_{max}$ dla pewnych ustalonych N_{min}, N_{max} będących parametrami protokołu.

2. Stacje mogą obliczać wartości funkcji haszującej H, która ma następującą własność:

   Niech $y = H(x)$ dla pewnego ciągu k-bitowego $x = x_1 x_2 \ldots x_k$. Załóżmy, że adwersarz zna y i może ustalić pewne bity ciągu x. Istnieje jednak podciąg $x_{i_1} x_{i_2} \ldots x_{i_a}$, taki że z punktu widzenia adwersarza obserwującego protokół

   $$(1/2)^{\frac{N_{max}}{N_{min}}} \leq \Pr[x_{i_j} = 1 | x_1 = b_1, \ldots, x_{i_j-1} = b_{i_j-1}, x_{i_j+1} = b_{i_j+1}, \ldots, x_k = b_k] \leq (1/2)^{\frac{N_{min}}{N_{max}}}$$

   dla dowolnych bitów $b_1, \ldots, b_{i_j-1}, b_{i_j+1}, \ldots, b_k$ i dowolnego $1 \leq j \leq a$. Wtedy adwersarz nie jest w stanie z prawdopodobieństwem większym niż $1/n^2$ znaleźć x', takie że $H(x') = y$.

   Wartość a jest parametrem protokołu. Mniej formalnie można drugi warunek wyrazić w następujący sposób - jeżeli adwersarz zna pewne bity ciągu x, jednak a spośród nich jest losowa (choć być może w ograniczony sposób obciążona), adwersarz nie może znaleźć żadnego elementu przeciwobrazu $H(x)$.

Zauważmy, że założenia dotyczące adwersarza są inne niż w przypadku protokołu z pracy B1, gdzie adwersarz może w praktyce kontrolować tylko jedną stację.

2.5.1 Opis nowego algorytmu

Szczegółowy opis znajduje się Rozdziale 2 pracy B2.

Algorithm 2 Ogólna struktura algorytmu

Rejestracja identyfikatorów – tworzenie listy;
repeat
  Zobowiązanie do wartości inicjalnych PRNG;
  Weryfikacja identyfikatorów z listy;
  Ujawnianie wartości inicjalnych PRNG i usuwanie nieprawidłowych identyfikatorów;
until (Brak nieprawidłowych identyfikatorów na liście).

Protokół składa się z kilku faz. W pierwszej deklarowane są identyfikatory. Liczba identyfikatorów może znacznie przekraczać liczbę stacji. W kolejnych krokach wykonywana jest pętla mająca na celu wyeliminować sytuację, w której jedna stacja bierze udział w symulowaniu więcej niż jednego identyfikatora. Testowanie to opiera się przede wszystkim na tym, że stacja nie może nadawać i słuchać w tej samej rundzie. Stacje deklarujące identyfikatory są zmuszane do nadawania w rundach określonych za pomocą funkcji pseudolosowej dla argumentu obliczonego przez wszystkie stacje, tak by jedynie wszystkie stacje działając wspólnie mogły zdeterminować jej wynik.

Krok weryfikacji stacji umożliwia wykrycie z wysokim prawdopodobieństwem pary identyfikatorów symulowanych przez tę samą stację. Należy podkreślić, że procedura wykrywa z wysokim prawdopodobieństwem dowolne strategie adwersarza niezgodne z protokołem – nawet takie, w których l stacji adwersarza symuluje kooperatywnie l' identyfikatorów (dla $l' > l$). Ponadto algorytm jest odporny na dynamiczne (adaptatywne) działanie adwersarza - to znaczy, gdy w kolejnych przebiegach pętli inne identyfikatory są symulowane przez inne stacje. Szczegółowy opis algorytmu znajduje się Rozdziale 2 pracy B2.

2.5.2 Analiza algorytmu

Rozdział 3 pracy B2 poświęcony jest analizie protokołu. Głównym twierdzeniem pracy B2 jest

Twierdzenie 2.6 (B2, Theorem 1)**.** *Jeśli na liście identyfikatorów jest więcej identyfikatorów niż fizycznych stacji, podczas pojedynczego wykonania pętli*

1. *przynajmniej jeden identyfikator zgłoszony przez stację działającą niezgodnie z protokołem zostanie usunięty z prawdopodobieństwem nie mniejszym niż* $1 - \frac{1}{n^2}$ *;*
2. *żaden z identyfikatorów deklarowanych przez stację deklarującą dokładnie jeden identyfikator nie zostanie usunięty z listy.*

Główna trudność w konstrukcji dowodu polegała na uwzględnieniu **wszystkich możliwych strategii**, w których adwersarza symuluje l' identyfikatorów za pomocą l stacji dla $l > l'$. W szczególności trzeba wziąć pod uwagę, że pojedynczy identyfikator może być symulowany przez kilka stacji adwersarza. Odpowiednia konstrukcja sprawia jednak, że przynajmniej jedna ze stacji adwersarza będzie musiała nadawać w a rundach, w których nie pozna czy nadawanie było skuteczne.

Jednocześnie w tych rundach będzie następowała kolizja z prawdopodobieństwem bliskim $1/2$. W dowodzie wykorzystuje się między innymi wariant nierówności Chernoffa dla rozkładu dwumianowego.

W Rozdziale 3.2 pokazane zostało także

Twierdzenie 2.7 (B2, Theorem 2)**.** *Niech X będzie liczbą identyfikatorów zarejestrowaną przez stacje adwersarza po wykonaniu całego protokołu. Jeśli jakakolwiek stacja adwersarza symuluje jednocześnie więcej niż jedną stację, wtedy*

$$E[X] < m - 1 + 1/n \, .$$

Ponieważ adwersarz postępując zgodnie z protokołem otrzymuje $X = m$, optymalną strategią[6] jest postępowanie zgodne z protokołem.

Ponadto zachodzi następujący fakt dotyczący czasu wykonania protokołu

Fakt 6. *Czas wykonania protokołu wynosi $O((n+m)^2 ma)$.*

2.7.1 Inne wyniki i dalsze kierunki badań

Pewne ogólne rozwiązanie problemu SA dla radiowej sieci ad hoc zaprezentowane zostało w pracy [31]. Wymaga ono jednak, aby stacje na podstawie komunikacji były w stanie z bardzo dużą dokładnością oceniać swoją odległość względem innych stacji. Założenie takie jest w praktyce trudne do zrealizowania w większości realistycznych modeli badanych dotychczas. Ponadto większość zaproponowanych mechanizmów nie będzie dawała odporności, jeśli adwersarz będzie mógł używać nawet prostych anten kierunkowych.

Inną ścieżką dalszych badań jest konstrukcja i analiza algorytmów odpornych na działanie adwersarza dla konkretnych typów zadań. Wynika to z faktu, że pewne problemy mogą być rozwiązane w sposób bardziej efektywny przy zastosowaniu algorytmów dostosowanych do konkretnego modelu i problemu, jaki ma być rozwiązany, niż przez stosowanie metod generycznych, polegających na stworzeniu listy rzeczywistych stacji a następnie przeprowadzeniu właściwego algorytmu dla identyfikatorów z wygenerowanej listy. W szczególności objęte badaniami są odporne algorytmy dla problemu *size approximation*, czyli oszacowania rozmiaru sieci. Częściowe rezultaty uzyskane zostały już w pracy [84].

Wyzwaniem wydaje się też konstrukcja algorytmów ochrony przed SA oparta o badanie innych zasobów. Jedną z takich prac jest [79], w której zaprezentowany został algorytm inicjalizacji, którego odporność opiera się na badaniu mocy obliczeniowych stacji (podobnie jak w [42]) .

Problemem otwartym jest konstrukcja analogicznych rezultatów dla innych topologii sieci. Pewne techniki, mogące stanowić punkt wyjścia do badań tego rodzaju znaleźć można w [31]. Prowadzone są też poszukiwania analogicznych protokołów, w których adwersarz dysponuje urządzeniami, których zasoby są większe niż w pozostałych stacjach.

[6] W sensie maksymalizacji wartości oczekiwanej

Rozdział 3

Bezpieczeństwo w systemach RFID

W niniejszym rozdziale omówione zostaną rezultaty dotyczące systemów RFID. Pierwsze dwa podrozdziały stanowią wprowadzenie w tematykę oraz przegląd poprzednich rezultatów. Kolejne dwa opisują pokrótce wyniki zawarte w pracach C1 oraz C2.

3.1 Systemy RFID

RFID to systemy identyfikacji radiowej. Akronim ten pochodzi od *Radio Frequency IDentification*. System taki składa się z trzech podstawowych komponentów - tagów, czytników oraz systemu bazodanowego.

Tagi – zwane też *transponderami (transponders)* albo *znacznikami* to małe układy elektroniczne (nierzadko o powierzchni poniżej 0.2 mm^2) o bardzo ograniczonych mocach obliczeniowych. Zazwyczaj nie są one w stanie samodzielnie inicjować komunikacji a energia do funkcjonowania generowana jest indukcyjnie podczas komunikacji z czytnikami. Komunikacja z nimi odbywa się zdalnie.

Czytnik - (*transceiver*) urządzenie, które może nawiązywać komunikację z tagami poprzez kanał radiowy. Czytniki mają stosunkowo duże możliwości obliczeniowo-pamięciowe oraz energetyczne, porównywalne ze standardowym komputerem osobistym. Czytniki mogą stanowić części innych urządzeń - na przykład telefonów komórkowych. Komunikacja między znacznikiem a czytnikiem, w zależności od specyfiki systemu, może się odbywać na odległość od kilku milimetrów do kilkunastu metrów.

System bazodanowy - system w którym zgromadzone są dane powiązane z informacjami z tagów. Zazwyczaj zakłada się, że czytnik podczas komunikacji z RFID-tagiem ma dostęp do systemu bazodanowego.

RFID-tagi, stosowane od lat 70. XX wieku, są obecnie bardzo rozpowszechnione. Ze względu na liczne standardy i producentów trudno wskazać dokładną liczbę wyprodukowanych tagów. Wia-

domo jednak, że przekroczyła ona dziesięć miliardów ([48]). Duża ich część to proste tagi zawierające kody zgodne ze standardem EPC (Electronic Product Codes), który stanowi następcę Universal Product Code (UCP), czyli popularnych kodów kreskowych.

Z teoretycznego punktu widzenia zdecydowana większość RFID-tagów stanowi urządzenia o ekstremalnie ograniczonych, właściwie pod każdym względem, zasobach. Mogą one być traktowane jako niewielkie nośniki pamięci, które są zdalnie odczytywane. Te bardziej zaawansowane dodatkowo zdolne są do wykonywania prostych obliczeń. Natura tych systemów wynika z trzech przyczyn:

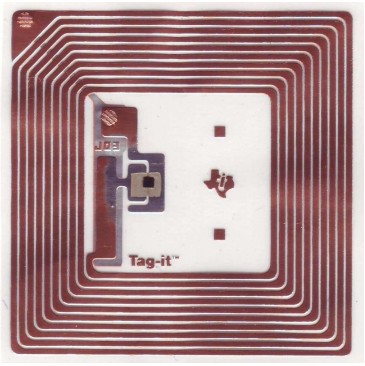
- redukcji kosztów - małe urządzenia muszą być znacznie tańsze niż przedmioty do których są przyłączane w celu identyfikacji, zatem koszt pojedynczego znacznika nie może przekroczyć kilku centów;
- konieczności miniaturyzacji – niektóre tagi są wtapiane w papier;
- brak możliwości utylizacji – w szczególności, nie ma możliwości uwzględniania w cyklu życia znacznika usunięcia baterii po zakończeniu jego używania.

Z tych przyczyn w pracach dotyczących systemów RFID badane są najczęściej urządzenia, które umożliwiają wykonanie tylko najprostszych operacji (np. dodawanie, zapis i odczyt bitów). Ich możliwości są znacznie niższe niż w przypadku typowych stacji-sensorów opisanych w Rozdziałach 1 i 2. W szczególności nie mogą obliczać wartości funkcji haszujących standardowo wykorzystywanych w protokołach kryptograficznych. Urządzenia tego typu mają pamięć, która nie przekracza kilkuset bitów. Nie mają także baterii a zasilanie odbywa się podczas komunikacji z czytnikiem na drodze indukcyjnej. W niektórych pracach przyjmuje się, że tagi mają wewnętrzne źródło bitów losowych, które wykorzystuje prosty fizyczny generator ([109]).

RFID-tagi są bardzo zróżnicowane pod względem możliwości i ceny [1]. W zdecydowanej większości nawet bardziej zaawansowane RFID-tagi mogą przeznaczyć na implementację mechanizmów bezpieczeństwa układ składający się z najwyżej 2000 bramek logicznych. Natomiast najefektywniejsza (w sensie złożoności układu logicznego) implementacja algorytmu AES wymaga 5000 bramek logicznych ([44]).

Zastosowania Systemy RFID zostały na początku wprowadzone, aby zastąpić kody UPC (Universal Product Codes), znane także jako *kody kreskowe*. Ich zastosowanie umożliwiało zidentyfikowanie obiektu bez konieczności fizycznego i optycznego kontaktu z nim. W szczególności można stworzyć listę obiektów które znajdują się w opakowaniu bez konieczności ich wypakowywania. Obecnie jednak zakres zastosowań jest znacznie szerszy - systemów tego typu używa się między

[1] Na przykład tagi wytworzone według standardu Unique czy TIRIS umożliwiają jedynie odczyt raz zapisanych danych. Tagi typu Q5 mają wbudowany mechanizm sprawdzania hasła. Stosunkowo drogie urządzenia typu MiFare, stosowane w niektórych kartach kryptograficznych oferują zaawansowane mechanizmy kryptograficzne – przy użyciu specjalnego koprocesora mogą nawet wykonać obliczenie funkcji 3DES.



Rysunek 3.1: Zdjęcie prostego RFID-taga. Mała czarna kropka w części wewnętrznej to miniaturowy obwód logiczny. Charakterystyczna prostokątna spirala to antena. Na zdjęciu widoczny jest też mały kondensator. Zdjęcie z [1].

innymi jako dodatkowe zabezpieczenie w kartach płatniczych, w systemach fizycznego i logicznego dostępu, w transporcie jako bilety, do zabezpieczania dokumentów, czy w szeroko rozumianej kontroli ruchu. Inne, także potencjalne, przykłady zastosowań można znaleźć w [59, 97].

3.1.1 Systemy RFID a bezpieczeństwo

Zauważmy, że w systemach tego typu nie jest możliwe użycie typowych mechanizmów bezpieczeństwa – nawet funkcji haszujących takich jak SHA-256. Uważa się, że dalszy rozwój systemów RFID w wielu obszarach zależy od opracowania efektywnych i tanich metod zapewniania bezpieczeństwa. Z tego względu metody zabezpieczania systemów RFID są badane już od lat 90. XX w. a wyniki tych badań zamieszczone są w setkach publikacji. Należy podkreślić, że produkowane są coraz mniejsze RFID-tagi (np. μ-TAG firmy Hitachi) i nadal istnieje potrzeba dalszej miniaturyzacji. Z tego względu w najbliższej przyszłości wyzwanie konstrukcji ultralekkich mechanizmów bezpieczeństwa wymagających minimalnych zasobów będzie stale aktualne.

Do podstawowych zagrożeń systemów RFID należą:

- nieautoryzowanym odczycie tagów, co może powodować między innymi zagrożenie szpiegostwem przemysłowym;
- zagrożenie prywatności - odczytując dane z tagów można zbierać informacje o przedmiotach posiadanych przez daną osobę a także ją śledzić;
- klonowanie tagów - tworzenie kopii RFID-taga. W zależności od zasobów nieuprawniona strona może uzyskać dostęp do pewnych zasobów albo tworzyć w nieautoryzowany sposób „podróbki” pewnych przedmiotów i dołączyć do nich klonowane tagi.

Zagrożenie prywatności W badaniach wskazywano bardzo wiele zagrożeń systemów RFID - między innymi ataki typu DoS, możliwość klonowania tagów czy zagrożenie ułatwionym szpiegostwem przemysłowym. Najczęściej jednak dyskutowano na temat zagrożenia prywatności. Osoba posiadająca przedmiot z RFID-tagiem może być łatwo śledzona. Co więcej wraz pewnymi dodatkowymi informacjami (np. numery kart kredytowych, fizyczne położenie) obecność RFID-taga może zdradzać bardzo dużo wrażliwych danych. Warto zauważyć, że dodatkowym aspektem zagrożenia prywatności jest to, że osoby często pozostają nieświadome tego, że są użytkownikami systemu RFID. Mamy zatem do czynienia z istotną różnicą jakościową – nie tylko korzystanie z systemu może narazić użytkownika na nieznane zagrożenia, ale także samo korzystanie z systemu może być nieświadome [2].

Cele bezpieczeństwa systemów RFID istotnie się różnią między sobą, podobnie jak ich formalne definicje. Niemniej podstawową pożądaną własnością jest *niepowiązywalność* (*unlinkability*) - formalnie wyrażona w Definicji 1 pracy C2 (Rozdział 4) jako gra z adwersarzem. Własność ta oznacza w praktyce, że strona nieuprawniona nie może ustalić, czy dwie odpowiedzi zostały wygenerowane przez tego samego RFID-taga.

3.1.2 Podstawowe metody ochrony

Techniki ochrony bezpieczeństwa w systemach RFID mają bardzo różną naturę. Nierzadko łączy się metody algorytmiczne z typowo fizycznymi. Jednym ze sposobów zapewniania bezpieczeństwa danych w systemach RFID jest uniemożliwienie ich odczytu niepowołanej stronie. Do podstawowych technik zaliczyć należy całkowite wyeliminowanie możliwości komunikacji z RFID-tagiem w określonym czasie. Wskazać tu można następujące podejścia:

Klatka Faradaya (Ekranowanie) - Przedmioty zaopatrzone w RFID-tagi umieszcza się w klatce Faradaya przez co komunikacja z nimi nie będzie możliwa. Rozwiązanie tego typu jest w praktyce wykonalne w przypadku bardzo nielicznych zastosowań. Przykładem może być paszport zaopatrzony w RFID-taga, którego okładki stanowią klatkę Faradaya. Zawartość taga może zostać odczytana tylko gdy okładki są otwarte. W produkcji znalazły się także portfele będące klatką Faradaya, dzięki temu uniemożliwiony może być odczyt RFID-tagów znajdujących się w różnego rodzaju kartach elektronicznych czy w banknotach[3].

„Kill command“ - Tagi mogą zostać trwale deaktywowane. Schemat taki jest wykorzystywany często w sklepach, w których po zakupie towarów przy kasie urządzenie jest deaktywowane. Rozwinięciem tego pomysłu jest schemat, w którym przed deaktywacją trzeba podać odpowiednie hasło - indywidualne dla każdego taga. Podejście takie bardzo ogranicza funkcjonalność wielu systemów. Co więcej, pokazano, że w przypadku niektórych tagów

[2] Zagrożenie takie nie ogranicza się jedynie do systemów RFID, ale także dotyczy szerszej kasy tzw. *pervasive systems*.

[3] Planowany była implementacja RFID-tagów w banknotach o wyższych nominałach (między innymi Euro) w celu utrudnienia fałszowania oraz automatyzacji wielu czynności obrotu finansowego. Plany te, budzące wiele kontrowersji, nie zostały dotąd zrealizowane ([70]).

po deaktywacji dalej możliwe jest uzyskanie przez adwersarza pewnych informacji w nich zawartych.

Skracanie anteny - Stosunkowo nową techniką jest, zaproponowana w [99], procedura polegająca na usuwaniu z RFID-taga dużej części anteny. W ten sposób można nawiązać komunikację z RFID-tagiem jedynie z bardzo bliskiej odległości (np. kilku milimetrów) a odczyt przy większym dystansie jest znacząco utrudniony. Dzięki temu, w pewnych przypadkach, możliwy jest odczyt tagów a zdalne śledzenie już nie. Metoda ta jest praktyczna jedynie w niektórych zastosowaniach systemów RFID.

Zagłuszanie - Do zbioru tagów może zostać dołączone dodatkowe urządzenie, które będzie powodować zagłuszanie normalnej komunikacji pomiędzy czytnikiem a tagami. Okazuje się jednak, że metoda taka nie zawsze jest skuteczna, bo właściwy sygnał transmitowany przez tagi w wielu przypadkach może być odfiltrowany. Ponadto stosowanie takich urządzeń może naruszać regulacje prawne i w istotny sposób ograniczać funkcjonalność systemu.

Zauważmy, że opisane metody nie wymagają wykonywania żadnych obliczeń. Z drugiej strony, ich implementacja możliwa jest tylko w niektórych z szerokiego spektrum zastosowań RFID. Bardziej szczegółowe opisy metod tego typu znaleźć można między innymi w [48, 91].

3.1.3 Ultralekkie protokoły uwierzytelniania dla systemów RFID

W badaniach coraz większą rolę odgrywają ultralekkie schematy uwierzytelniania. Mimo licznych propozycji główny nurt badań stanowią obecnie schematy związane z protokołem HB, który został zaproponowany w kontekście protokołów RFID w pracy [72]. Protokół HB oparty jest na schemacie *Human-to-computer authentication protocol* autorstwa Hoppera i Bluma ([64]).

Trudność złamania wspomnianych protokołów redukuje się do problemu LPN (*Linear Parity with Noise*), który jest NP-trudny ([8], [61]). Dla szczególnych przypadków, w pewnych modelach problem LPN badany był w pracach [11, 92, 93] .

Protokół HB+
Parametry publiczne: n, m, ε, N
Tajne, współdzielone klucze: $x \in_R \{0,1\}^n, y \in_R \{0,1\}^m$
Parametr pomocniczy: $L = 0$

Poniższa procedura powtarzana jest N razy:

Czytnik		**Tag**
		$b \in_R \{0,1\}^m$
	$\xleftarrow{b}$	
Wybiera $a \in_R \{0,1\}^n$		
	$\xrightarrow{a}$	
		$v := 1$ z prob. ε, w przeciwnym wypadku $v := 0$
		Oblicza $r :=< x, a > \oplus < y, b > \oplus v$
	$\xleftarrow{r}$	
Jeśli $r =< x, r > \oplus < y, b >$ to $L := L + 1$;		

Odpowiedź jest akceptowana gdy $L \geq (1 - \varepsilon)N$.

Typowe parametry protokołu to $\varepsilon = 1/4$, $N = 1164$. Jednocześnie długości ciągów x i y ustala się odpowiednio na 80 oraz 512.

Analiza bezpieczeństwa tego protokołu prezentowana w [75, 76]. Wykazano tam między innymi, że protokół HB+ nie jest bezpieczny, jeżeli adwersarz może jednocześnie prowadzić komunikację z czytnikiem jak i z tagiem (t.j. stosować podejście typu *Man in the middle*). Inne efektywne ataki pokazano w [53].

Przedstawiono liczne protokoły oparte o schemat HB+. W przypadku większości pokazano już ich poważne luki bezpieczeństwa. Wskazać tu należy między innymi:

HB# ([50]) – skutecznie zaatakowany w [106];

HB-PUF ([60]) – oparty o *Physically Unclonable Function (PUF)*;

Trusted-HB ([17]) – oparty o inny protokół z [87]. Protokół Trusted-HB został zaatakowany w [47];

HB++ ([16]) – zaatakowany w [113];

HB-MP ([100]) – stanowi bezpośrednie rozwinięcie HB+, które zapewnia ochronę przed niektórymi zaprezentowanymi wcześniej atakami.

Najbardziej obecnie zaawansowanym schematem z tej rodziny jest protokół uwierzytelniania z [78], który jest odporny na szerszą klasę ataków aktywnych niż HB+. Co więcej, przedstawiony dowód oparty o redukcję do problemu LPN, daje silniejsze gwarancje bezpieczeństwa. Praca nie podaje jednak praktycznych wartości jakie muszą być użyte dla zabezpieczenia protokołu, stąd trudno ocenić jego efektywność i przydatność w praktyce. Podobny zarzut postawić można wszystkim protokołom z rodziny HB ze względu na bardzo dużą ilość danych, jakie musi nadać tag podczas komunikacji z czytnikiem[4].

[4]W pracach często wielkości te nie są podawane, ale da się zauważyć, że na przykład protokół z [78] wymaga

3.2 Nowe rezultaty – schemat uwierzytelniania CKK (Praca C1)

W pracy C2 został zaprezentowany nowy, ultralekki schemat uwierzytelniania dla systemów RFID-tagów, który odchodzi od paradygmatu wyznaczonego przez protokół HB. Obok schematu bazowego (Rozdział 2 w C2) pokazano także szereg jego rozszerzeń (Rozdział 5 w C2). Analiza protokołu bazowego (Rozdziały 3 oraz 4 pracy C2) wykazuje nie tylko bezpieczeństwo samego procesu uwierzytelniania taga wobec czytnika ale także dowodliwie zachowywanie prywatności. Własności te są jednak pokazane jedynie przy słabym, choć w wielu przypadkach ciągle realistycznym, modelu adwersarza.

3.2.1 Opis podstawowego protokołu uwierzytelniania

Opisywany protokół zależy od dwóch parametrów - n oraz k. Na każdą komunikacją zainicjowaną przez czytnik, (n, k)-tag odpowiada $n + k$ bitowym ciągiem $X||Y$. Pierwsze n bitów (ciąg X), tworzących część *niezależną* jest losowane z rozkładem jednostajnym ze zbioru $\{0, 1\}^n$. Część zależna to ciąg Y o długości k bitów, które stanowią wartości funkcji xor na ustalonych pozycjach części niezależnej. Dokładniej, i-ty bit jest wyznaczany jako xor bitów na pozycjach części niezależnej z ustalonego zbioru $C_i \subset \{1 \ldots n\}$. Same zbiory $C_1, \ldots, C_k$ stanowią **sekret znany tylko czytnikowi i tagowi**.

Niech $Y(i)$ oznacza i-ty bit ciągu X. Protokół komunikacyjny pomiędzy czytnikiem a tagiem T wygląda w następujący sposób:

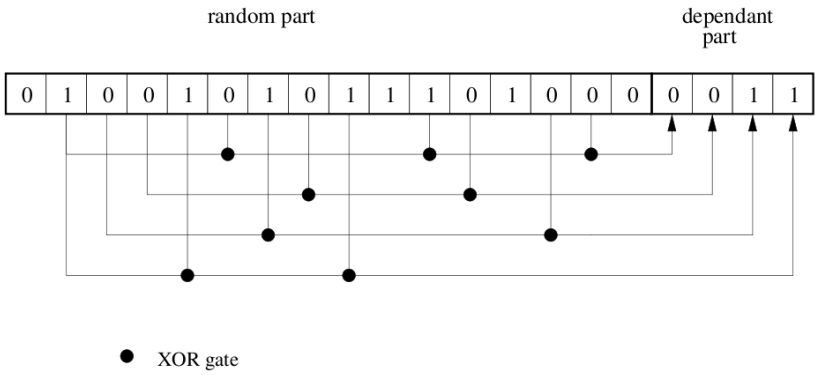
1. Czytnik przesyła do RFID-taga sygnał inicjujący komunikację.
2. Tag T przesyła odpowiedź postaci $X_T||Y_T$, która jest skonstruowana za pomocą następującej procedury:

   procedura Update(T)
   begin
   $X_T \in_R \{0,1\}^n$;
   for $i = 1$ to k
   $Y_T(i) := \bigoplus_{C_T^i} X_T$;
   end;

3. Czytnik sprawdza czy w bazie danych jest **dokładnie jeden** tag o zbiorach ukrytych $C'_1, \ldots, C'_k$, dla których spełniona jest relacja pomiędzy ciągami X i Y. W takim przypadku tag zostaje zidentyfikowany i zaakceptowany. W przeciwnym razie jest odrzucany.

Zauważmy, że RFID-tag nie musi interpretować żadnego komunikatu przesyłanego przez czytnik a pierwsza runda potrzebna jest jedynie po to, aby zainicjować protokół i dostarczyć pasywnemu tagowi energii.

przesłania przez tag nawet 1 Mb danych podczas pojedynczego wykonania.



Rysunek 3.2: Schemat układu realizującego RFID tag. Przykład $(16, 4)$-taga.

Schematy produkcji tagów Fizyczna realizacja taga jest bardzo prosta. Istotnie, poza generatorem liczb losowych, który może być zaimplementowany w standardowy sposób dla systemów małych urządzeń ([21, 63]) – wymaga się jedynie $\sum_{1\leq i\leq k} |C_i|$ bramek xor. Rysunek 3.2 prezentuje układ logiczny implementujący RFID-taga.

Można zauważyć, że efektywność oraz bezpieczeństwo protokołu zależy, poza parametrami n tudzież k, przede wszystkim od odpowiedniego wybrania zbiorów ukrytych $C_1, C_2, \ldots, C_k$. Oczywiste jest, że jeśli, na przykład, we wszystkich RFID-tagach zbiory te będą takie same, tagów nie będzie można rozróżnić. Z drugiej strony bardzo małe lub bardzo duże zbiory ukryte nie zapewnią bezpieczeństwa, bo mogą zostać łatwo odgadnięte.

W pracy zaproponowano i przeanalizowano (n, k, p)-*schemat produkcji tagów.* Idea jego jest następująca:

Definicja 3.2.1. *Każdy z indeksów $\{1, \ldots n\}$ jest elementem każdego zbioru $C_1, \ldots C_k$ z prawdopodobieństwem p. Wybory są niezależne dla poszczególnych indeksów, zbiorów oraz tagów.*

Jak wykazała analiza, procedura taka jest bardzo efektywna pod względem poziomu bezpieczeństwa jaki zapewnia.

3.2.2 Analiza protokołu CKK

W pracy C1 pokazano kilka własności opisanego protokołu gdy używany jest (n, k, p)-*schemat produkcji tagów.* Będziemy korzystać z następującego oznaczenia

$$\mathrm{UPD}(n, m, p) = \frac{1}{2^n} \sum_{a=1}^{m} \binom{m}{a} \left(1 + (1-2p)^a\right)^n \ .$$

Okazuje się, że funkcja ta przyjmuje bardzo małe wartości dla dużego zakresu istotnych z praktycznego punktu widzenia argumentów, co zostało omówione w pracy C1.

Rozróżnialność tagów W pracy C1 wykazano między innymi

Fakt 7 (C1,Theorem 1)**.** *Niech T_0 oraz T będą dwoma tagami stworzonymi za pomocą (n, k, p)-schematu produkcji. Prawdopodobieństwo, że odpowiedź T_0 będzie zaakceptowana jako odpowiedź T jest mniejsza niż*

$$\frac{1}{2^k} + UDP(n, k, 2p(1-p)).$$

Fakt 8 (C1, Theorem 2)**.** *Prawdopodobieństwo (błędnego) zidentyfikowania taga, którego **nie ma**[5] w zbiorze L tagów nie przekracza*

$$\frac{L}{2^k} + L \cdot \mathit{UPD}(n, k, 2p(1-p)).$$

Analiza oparta była na badaniu linowej zależności pomiędzy losowymi wektorami binarnymi. Kluczowy w analizie okazały się następujące fakty

Fakt 9 (Theorem 3, C1)**.** *Niech $x_1, x_2, \ldots x_{n-k}$ będzie zbiorem losowych ciągów bitowych długości n, które zostały wybrane z rozkładem jednostajnym. Niech $p_{n,k}$ dla $1 \leq k \leq n$ oznacza prawdopodobieństwo, że zbiór $x_1, x_2, \ldots x_{n-k}$ jest liniowo niezależny nad ciałem $\mathbf{Z}_2$. Wtedy*

$$1 - 2^{-k} < p_{n,k} < 1 - 2^{-(k+1)}.$$

Istotne jest, że powyższe ograniczenie nie zależy od n.

Fakt 10 (Theorem 6, C1)**.** *Niech x_i^j dla $i, j \in \{1, 2, \ldots, n\}$ będzie losowym ciągiem binarnym, takim że $\Pr[x_j^i = 1] = p$ dla pewnego $0 < p < 1$. Niech $x_i = (x_i^1, x_i^2, \ldots, x_i^n)$. Prawdopodobieństwo, że ciąg $(x_1, x_2, \ldots, x_m)$ dla pewnego $0 < m \leq 1$ jest liniowo zależny, jest mniejsze niż $UDP(n, k, 2p(1-p))$.*

Anonimowość

Fakt 11 (C1, Corollary 1,2)**.** *Załóżmy, że adwersarz (pasywny) może zdobyć t odczytów z każdego z L tagów znajdujących się w systemie. Następnie losowany jest z rozkładem jednostajnym jeden z L tagów i zwracany jest adwersarzowi $(t+1)$-szy odczyt z tego taga. Adwersarz nie jest w stanie wskazać taga, z którego pochodzi odczyt z prawdopodobieństwem przekraczającym*

$$\frac{1}{L} + L \cdot \mathit{UPD}(n, t+1, p)\ . \tag{3.1}$$

Zauważmy, że powyższe ograniczenie jest bardzo bliskie optymalnej wartości $1/L$ dla realistycznych wielkości n, L i niedużej liczby odczytów t. Istotnie, można na przykład sprawdzić, że dla $n \in [128, 1024]$ oraz $t \leq n - 40$ zachodzi $\mathrm{UPD}(n, t+1, \frac{30}{n}) < 2.3 \cdot 10^{-10}$.

[5] Popełnienie błędu drugiego rodzaju *(ang. false positive error)*;

3.2.3 Rozszerzenia i modyfikacje

W pracy C2 zaproponowane zostały (bez pełnej analizy) rozszerzenia bazowego schematu (Rozdział 5 pracy C1).

RFID-tag może przesyłać, poza odpowiedzią, unikalny identyfikator. Rozwiązanie takie oczywiście spowoduje, że schemat nie będzie zachowywać nierozróżnialności. Schemat taki może jednak dalej służyć do uwierzytelniania. Zaletą jest jednak znaczne przyspieszenie obliczeń po stronie czytnika. Istotnie, zauważmy że w podstawowej wersji schemat może wymagać od czytnika wykonania obliczeń proporcjonalnych do liczby tagów w całym systemie.

C1, Rozdział 5.1 Poza odpowiedzią opisaną w bazowym schemacie, RFID-tag oblicza dodatkowy, losowy n-bitowy ciąg X'. Jako odpowiedź przesyła z prawdopodobieństwem $1/2$ ciąg $X||X'||Y$ a z prawdopodobieństwem $1/2$ ciąg $X'||X||Y$.

Rozwiązanie to jest wzorowane na idei *Chaffing and Winnowing* Rivesta ([116]). W pracy [86] schemat ten został określony jako CKK^2.

C2, Rozdział 5.2 Odpowiedzi opisane w schemacie bazowym są permutowane za pomocą ustalonej dla każdego taga permutacji σ. Dokładniej, $n + k$ bitów schematu bazowego pojawia się na pozycjach wskazanych przez permutację σ. Permutacja ta stanowi część sekretu dzielonego między czytnik i tag. Kolejnym krokiem jest zastosowanie permutacji σ^t przy t-tym odczycie taga. Zauważmy, że zaproponowana modyfikacja może być zrealizowana bardzo efektywnie nawet na ekstremalnie prostych układach logicznych. W pracy [86] schemat ten został określony jako $CKK^{\sigma,L}$.

Należy zaznaczyć, że mimo opublikowania ataków na niektóre protokoły z rodziny CKK, są one obiektem dalszych badań i modyfikacji [86].

3.2.4 Ataki na schemat CKK

Protokoły typu CKK stały się obiektem ataków oraz analiz. W pracy [53] przedstawiono atak na CKK^2. Był on jednak nieefektywny, gdyż jego czas wykonania wynosił $n^{\Theta(k)}$ oraz wymagał zdobycia liczby odczytów tego samego rzędu. Atak ten został skutecznie przyspieszony w pracy [86], gdzie pokazano metodę ataku wymagającą dla realistycznych wartości n mniej niż minuty obliczeń standardowego komputera i około $2n$ obserwacji. Zauważmy jednak, że w przypadku rzeczywistych systemów i $n = 256$ wymaganie aby adwersarz był w stanie zgromadzić ponad 500 obserwacji w wielu przypadkach wydaje się zadaniem trudnym.

Warto zaznaczyć, że autorzy [86] nie byli w stanie swoimi stosunkowo silnymi metodami zaatakować protokołu $CKK^{\sigma,L}$. Mimo to w pracy [86] postawiona została hipoteza, że istnieje efektywny (praktyczny) algorytm łamania $CKK^{\sigma,L}$.

3.2.5 Porównanie z innymi protokołami ultralekkimi

Złożoność obliczeniowa Zarówno schemat CKK jak i jego rozszerzenia są bardzo łatwe w implementacji sprzętowej. Rozmiar koniecznego układu logicznego jest nieco mniejszy niż w przypadku protokołów z rodziny HB+.

Złożoność komunikacyjna Schemat CKK ma znacznie mniejszą złożoność komunikacyjną niż protokoły z rodziny HB. Dla identyfikacji taga w CKK wystarczą w praktyce $1-3$ rundy komunikacji. Każda z nich wymaga przesłania $n+k$ bitów. W przypadku protokołu HB+ wymaga się przesłania aż $n \cdot N$ bitów, gdzie typowa wartość parametru N może przekraczać 1000 ([78]).

Bezpieczeństwo Przedstawiona w pracy C1 analiza bezpieczeństwa dla schematu CKK jest istotnie różna od zaproponowanych dla rodziny HB/HB+ [64, 72, 78]. W przypadku tych prac analiza redukowała bezpieczeństwo do rozwiązania określonego problemu - w tym przypadku problemu LPN (Linear Problem with Noise). W analizie protokołu CKK w pracy C1 zostało precyzyjnie oszacowane górne ograniczenie na prawdopodobieństwo udanego ataku dla dowolnych, nawet małych rozmiarów tagów. Co więcej, pokazano że póki liczba odczytów jest mała, bezpieczeństwo oferowane przez schemat jest teorioinformacyjne – nie zależy od mocy obliczeniowych adwersarza. Z drugiej strony należy wskazać, że analiza bezpieczeństwa:

- została przeprowadzona jedynie dla podstawowego schematu CKK;
- ogranicza się jedynie do relatywnie słabego adwersarza pasywnego;
- wykazuje bardzo wysoki poziom bezpieczeństwa jedynie dla relatywnie małej, liniowej względem długości taga liczby odczytów.

Co więcej, niektóre wskazane w rozdziale techniki, które miały na celu uodpornienie bazowego schematu na działanie silniejszego adwersarza okazały się możliwe do zaatakowania ([53, 86]).

3.3 Nowe rezultaty – Allowery (Praca C2)

W pracy C2 przedstawiono rodzinę protokołów, które mają zapewnić bezpieczeństwo, w szczególności ochronę prywatności użytkownikom RFID-tagów. Schemat można traktować jako rozwiązanie komplementarne do protokołu *Tag-blocker* ([71]).

Blocker Idea rozwiązania polega na tym, żeby uniemożliwić odczytanie RFID-tagów poprzez dodanie do ich zbioru dodatkowego, **pojedynczego** urządzenia zwanego *blockerem*, które symuluje w pewnym otoczeniu obecność **wszystkich** tagów, o identyfikatorach z pewnej przestrzeni $\{0,1\}^l$. To oczywiście uniemożliwia stwierdzenie, jakie tagi są w zasięgu czytnika, a które są jedynie symulowane. Blocker może działać efektywnie dzięki szczególnemu protokołowi komunikacji

pomiędzy czytnikiem a wieloma tagami nazywanym QT. W protokole tym czytnik transmituje ciągi bitowe zaczynając od ciągu pustego. Tag odbierając x, jeśli jego identyfikator ma prefiks postaci $x||b$ gdzie $b \in \{0,1\}$, odpowiada bitem b. Na tej podstawie czytnik jest w stanie ustalić czy są w jego zasięgu RFID-tagi z identyfikatorami o prefiksach $x||0$ lub $x||1$ i wywołuje rekurencyjnie kolejne zapytania aż do ciągów długości $l-1$, co umożliwia zapytanie o konkretny identyfikator. Skrótowy opis protokołu QT znaleźć można w Rozdziale 2 pracy C1, szczegółowy zaś w [71].

Blocker działa w następujący sposób - na każde zapytanie czytnika, przesyła zarówno 1 jak i 0. Prowadzi to w oczywisty sposób do symulacji obecności tagów o wszystkich możliwych identyfikatorach ze zbioru $\{0,1\}^n$. Rozwiązanie to, mimo prostoty i dużej efektywności w pewnych przypadkach, ma szereg wad:

- Może ono działać jedynie w systemie, w którym tagi używają protokołu QT.
- Przynajmniej w niektórych przypadkach, możliwe jest odfiltrowanie sygnału nadawanego przez tagi od tych nadawanych przez blockera. Dokładniej, można pokazać, że adwersarz wnioskując po sile sygnału o liczbie urządzeń, które odpowiadają na zadane pytanie, może ustalić identyfikatory RFID-tagów w swoim zasięgu w takim samym czasie i z taką samą liczbą odczytów tagów, jak w przypadku gdy blocker jest wyłączony.

W pracy C2 pokazano trzy schematy, które z punktu widzenia użytkownika oferują taką sama funkcjonalność - aktywacja/deaktywacja pewnego urządzenia powoduje, że można/nie można odczytywać tagi. Urządzenie z pracy C2 określane zostało jako *allower*. Jest ono znacznie bardziej skomplikowane niż typowy RFID-tag - w szczególności musi mieć możliwość obliczenia wartości funkcji, która w praktyce jest jednokierunkowa. Podkreślmy jednak, że pojedynczy allower może być użyty w systemie z wieloma tagami - jest to typowa architektura jeden-do-wielu. Ponadto allower może być urządzeniem pasywnym a przede wszystkim jest wolny od wad opisanych wyżej.

W pracy C2 zaproponowano kilka schematów różniących się oferowanym poziomem bezpieczeństwa oraz wymaganiami sprzętowymi.

Schamt 1 (Rozdział IV.A) - Schemat ten nie wymaga od taga żadnych mocy obliczeniowych i oferuje bardzo wysoki poziom ochrony przed adwersarzem mogącym zarejestrować maksymalnie n odczytów z każdego taga. Z drugiej strony schemat ten wymaga relatywnie dużej pamięci rzędu $O(n)$ w każdym tagu.

Schamt 2/2+ (Rozdział IV.B-C) - Te protokoły wymagają od RFID-taga liczenia wartości funkcji haszującej, stąd mogą być używane jedynie do zaawansowanych i relatywnie drogich tagów. Z drugiej strony wymagają jedynie stałej pamięci.

Schemat 3 (Rozdział IV.D) - Schemat ten może stanowić wzmocnienie (dodatkową warstwę bezpieczeństwa) dla ultralekkich protokołów autoryzacji typu HB+ czy CKK.

Warto wspomnieć, że w Rozdziale V C2 pokazano liczne rozszerzenia bazowego protokołu - między innymi, jak można w łatwy sposób zbudować system, w którym do odczytania konkretnego

RFID-taga należy aktywować kilka allowerów. Pokazano także, że protokoły tego typu mogą ukrywać jedynie część danych zawartych w tagach. Rozszerzenia te dają możliwość implementowania w systemach RFID złożonych polityk bezpieczeństwa/dostępu.

Rozdział 4

Protokoły anonimowej komunikacji w rozproszonych systemach urządzeń o ograniczonych zasobach

Niniejszy rozdział traktuje o problemie anonimowej komunikacji w środowisku rozproszonym. W szczególności podsumowuje rezultaty z prac oznaczonych jako D1 oraz D2.

Aspektem bezpieczeństwa danych, który odgrywa coraz większą rolę w rzeczywistych systemach informatycznych jest *anonimowość*. W przeciwieństwie do poufności danych nie chodzi tu o ukrycie samej treści informacji a o to, aby ukryć fakt, że dwie strony nawiązywały ze sobą komunikację. Ujawnienie takigo faktu może mieć istotną wartość informacyjną nawet bez znajomości przekazywanych komunikatów (które mogą na przykład być zaszyfrowane). To, że sama komunikacja miała miejsce wraz z innymi, powiązanymi informacjami (np. czas, treść wpisu na powszechnie dostępnym forum) może spowodować wyciek danych wrażliwych dotyczących konkretnych osób – na przykład pobieranie informacji na temat specyficznych chorób przez osobę fizyczną może być dla firmy ubezpieczeniowej przyczyną[1] odmowy zawarcia umowy. Warto wskazać, że protokoły anonimowej komunikacji są obiektem bardzo intensywnych badań - od typowo aplikacyjnych (np. [34]) do silnie teoretycznych (np. [115]). Stale aktualizowane dane dotyczące stanu badań nad anonimową komunikacją można znaleźć na portalu [33].

Jak dotąd opracowano niewiele praktycznych algorytmów umożliwiających anonimowe komunikowanie się, z czego większość jest podatna na tzw. *atak powtórzeniowy* opisany w Podrozdziale 4.2. Typowa obrona przed nim wymaga bardzo dużej ilości pamięci, która nie może być zapewniona w systemach ograniczonych urządzeń. W rozdziale tym opiszemy krótko metody anonimowej komunikacji, ze szczególnym uwzględnieniem nowych wyników dotyczących protokołów stosowanych w systemach z ograniczoną pamięcią.

[1] faktyczną, jeśli nawet nie formalną

4.1 Anonimowość oparta o `MIX` Chauma

Warto wspomnieć, że samo pojęcie anonimowości jest przedmiotem badań. Definicje anonimowości były dyskutowane między innymi w pracach [32, 58, 110, 117, 118]. Rozważania te są jednak poza zakresem niniejszej pracy.

Idea anonimowej komunikacji może być realizowana różnymi metodami. Przykładami mogą być DC-networks ([20, 55]) czy protokół z [37] (S.Dolev *et.al.*) - nie mają one jednak znaczenia praktycznego. Nieco innym podejściem do zapewniania anonimowej komunikacji jest wykorzystanie metod *steganograficznych* ([22]). Mimo wielu ciekawych własności metody te okazały się niemożliwe do zastosowania w wielu rzeczywistych scenariuszach anonimizacji komunikacji a w niektórych są po prostu nieefektywne.

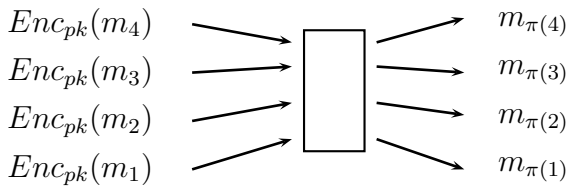
Obecnie niemal wszystkie liczące się implementacje oraz zdecydowana większość badań teoretycznych skupia się na paradygmacie zapoczątkowanym przez D.Chauma w protokole `MIX` ([19]) z początku lat 80. XX wieku. Schemat ten gwarantuje bezpieczeństwo oparte o trudność obliczeń, w przeciwieństwie np. do schematu z pracy [20], który oferuje bezpieczeństwo teorioinformacyjne.

Protokół `MIX` W modelu rozważa się grupę nadawców ponumerowanych unikalnymi liczbami od 1 do n, grupę odbiorców oraz trzecią stronę określaną jako MIX-serwer. Zakłada się, że wszyscy nadawcy znają klucz publiczny pk, taki że odpowiadający mu klucz prywatny sk jest dostępny tylko MIX-serwerowi. Działanie protokołu jest następujące:

1. Użytkownik i-ty szyfruje wiadomość m_i (zawierającą nazwę odbiorcy) otrzymując $Enc_{pk}(m_i)$ i przesyła ją do MIX-serwera.
2. MIX-serwer po otrzymaniu kryptogramów od wszystkich n użytkowników:
   - odszyfrowuje kryptogramy kluczem sk,
   - wybiera losową permutację zbioru n elementowego π z rozkładem jednostajnym z grupy symetrii $\mathbf{S}_n$,
   - przesyła właściwym odbiorcom kryptogramy w kolejności wskazanej przez permutację π. To znaczy
   $$m_{\pi(1)}, \ldots, m_{\pi(n)} \ .$$

Można zauważyć, że anonimowość w protokole osiągana jest w ten sposób, że dzięki MIX-serwerowi zostaje ukryta relacja między nadawcami a odbiorcami. Innymi słowy, nie jest wiadomo kto do kogo nadawał. Przedstawiona idea realizowana była w różny sposób - należy wspomnieć między innymi prace [19, 66, 67, 69].

Bezpieczeństwo protokołu Ten koncepcyjnie prosty algorytm, aby móc efektywnie i bezpiecznie działać w praktyce, wymaga drobiazgowej implementacji zależnej też od specyfiki otoczenia systemu, w jakim ma funkcjonować. Szczególnie ważną kwestią są możliwości adwersarza. Na



Rysunek 4.1: Schemat działania MIX-serwera dla permutacji π

przykład, gdy adwersarz może opóźniać wysyłanie wiadomości i preparować własne (na przykład kontrolując część użytkowników) możliwe są liczne ataki wskazane między innymi w pracy [77]. Podobnie, fundamentalne znaczenie ma zastosowany schemat szyfrowania. Już w klasycznej pracy [19] wskazano, że użyty schemat musi być zrandomizowany i ma zapewniać własność określaną jako *semantic security*. W pracy [111] pokazano jednak, że nawet zrandomizowany schemat szyfrowania zapewniający wysoki poziom poufności danych może stwarzać zagrożenie dla anonimowości, gdy jest zastosowany w protokole MIX. Na temat bezpieczeństwa protokołu MIX opublikowanych zostało wiele prac, z których większość została odnotowana w stale aktualizowanym serwisie [33].

Protokół cebulkowy i Onion Routing

Protokół MIX posiada wady, które znacząco ograniczają zakres jego funkcjonalności. Jest to protokół scentralizowany, trudny do implementacji w systemach rozproszonych. Co więcej anonimowość użytkowników w pełni zależy od uczciwości pojedynczego MIX-serwera. Z tego względu badane były rozszerzenia bazowego schematu - już w pracy [19] zaproponowano tzw. *MIX-kaskadę*, w której MIX-serwery połączone są szeregowo. Dalej, zaproponowano *równoległą kaskadę MIX-serwerów* badaną miedzy innymi w [56, 80]. W pełni rozproszonym algorytmem opartym na idei MIX-serwera jest *Onion Routing* określany czasem jako *Trasowanie Cebulowe*. Protokół jest przypisywany autorom pracy [52], choć jego ideę oraz nietrywialne dowody bezpieczeństwa zaprezentowali wcześniej C. Rackoff i D. Simon w [115].

W Onion Routingu zakładamy istnienie n węzłów, które pełnią jednocześnie role odbiorców, nadawców oraz serwerów świadczących usługi na rzecz innych węzłów. Zakładamy, że między każdymi dwoma użytkownikami istnieje bezpośrednie połączenie, to znaczy sieć jest grafem pełnym. Ponadto, każdy węzeł posiada parę kluczy asymetrycznego schematu szyfrowania. Klucz publiczny i-tego użytkownika pk_i jest znany wszystkim użytkownikom, a odpowiadający mu klucz prywatny sk_i znany jest tylko użytkownikowi i-temu. Zakładamy, że każdy z węzłów ma dokładnie jedną wiadomość do przesłania.

Każdy węzeł wykonuje następujące akcje:

Faza tworzenia kryptogramu

Niech $Enc_{pk}(m)$ oznacza kryptogram odpowiadający wiadomości m przy zastosowaniu klucza publicznego pk.

1. Węzeł A wybiera losowo z rozkładem jednostajnym, ciąg $\lambda-1$ węzłów pośrednich $J_1, \ldots, J_{\lambda-1}$ spośród wszystkich węzłów. Niech B będzie węzłem, do którego A chce nadać wiadomość. Przyjmujemy $B = J_\lambda$.

2. Węzeł A tworzy *cebulkę* $\mathcal{O}_1$ zdefiniowaną rekurencyjnie:

$$\begin{aligned} \mathcal{O}_\lambda &:= Enc_{pk_{J_B}}(m), \\ \mathcal{O}_j &:= Enc_{pk_{J_j}}(O_{j+1}||J_{j+1}) \text{ dla } 1 \leq j < \lambda. \end{aligned}$$

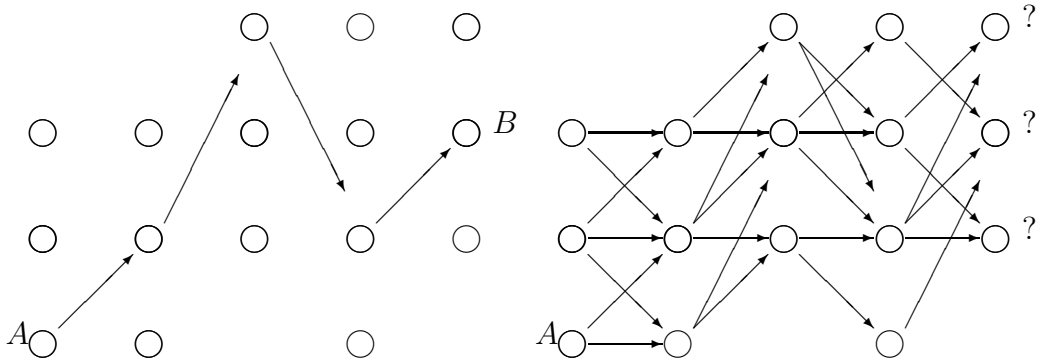
3. Przesyła cebulkę $\mathcal{O}_1$ do węzła J_1.

Charakterystyczna, warstwowa budowa tego kryptogramu spowodowała, że określa się go jako *kryptogram cebulkowy* lub potocznie *cebulkę (onion)*.

Faza przesyłania i przekodowywania cebulek

1. W danym kroku węzeł J_j otrzymuje kryptogramy, deszyfruje je uzyskując kolejne kryptogramy wraz z informacją, gdzie mają one zostać przesłane. W przypadku opisanej wyżej cebulki nadanej przez węzeł A, będzie to węzeł J_{j+1}.

2. Węzeł przesyła wszystkie otrzymane w danym kroku kryptogramy do wskazanych węzłów.



Rysunek 4.2: Onion routing - po lewej rzeczywista ścieżka. Po prawej obraz z punktu widzenia adwersarza przy 7 wiadomościach przesyłanych przez sieć.

Anonimowość W klasycznym modelu GPA (*Global Pasive Adversary*) zakłada się, że adwersarz ograniczony jest do obserwacji całej komunikacji pomiędzy węzłami, bez poznawania akcji wykonywanych lokalnie przez węzły. W szczególności, nie jest w stanie poznać treści zaszyfrowanych komunikatów. Anonimowość w protokole Onion Routing osiągana jest na tej samej zasadzie jak w przypadku protokołu `MIX` – gdy kilka wiadomości w tym samym czasie znajdzie się w tym samym węźle, stają się (z punktu widzenia adwersarza) nierozróżnialne. Istotnie, w przypadku konkretnego węzła adwersarz podczas obserwacji poznaje jedynie liczbę cebulek przesyłanych z i wysyłanych do konkretnych węzłów. Formalna analiza bezpieczeństwa protokołu, nawet w uproszczonym modelu, wymaga zaawansowanych technik matematycznych i sprowadza się do badania grafowego procesu stochastycznego ([115]). Badane były także inne, bardziej realistyczne modele np. model BFT, w którym adwersarz może obserwować jedynie część połączeń pomiędzy węzłami ([9]). Efektywna analiza bezpieczeństwa dla tego modelu została przeprowadzona w [58] za pomocą argumentu *couplingowego*.

Należy stwierdzić, że mimo powszechnego używania schematów anonimizacji opartych o paradygmat wyznaczony przez algorytm `MIX`, nie powstał dotąd protokół o udowodnionym bezpieczeństwie w realistycznym modelu.

Perspektywa implementacyjna Obecnie istnieje wiele implementacji rozproszonych protokołów opartych o schemat `MIX` - między innymi Tarzan ([46]), AN.ON ([52]) oraz najbardziej rozpowszechniony TOR, z którego obecnie korzystają setki tysięcy użytkowników ([2, 34]). Protokoły anonimowej komunikacji są używane także do realizacji e-usług. Między innymi stosuje się je jako podprocedury przy wyborach elektronicznych [90], e-aukcjach czy nawet protokołach typu SFE [68].

4.2 Atak powtórzeniowy i URE-Cebulki

Idea ataku powtórzeniowego

Zagrożenie *atakiem powtórzeniowym (repetitive attack)* w kontekście sieci anonimizujących zostało wskazane już w pracy [19]. Dotyczy ono zarówno najprostszego protokołu Chauma jak też wysokopoziomowych implementacji jak protokół TOR, co pokazano w [114]. Idea ataku powtórzeniowego jest następująca - adwersarz kontroluje w sieci pewną liczbę węzłów. Jeśli jeden z węzłów kontrolowanych przez adwersarza otrzymuje cebulkę może próbować ją śledzić. W tym celu wykonuje jej kopię. We właściwym kroku cebulkę przesyła do kolejnego węzła. Kopia jest po t rundach wysyłana po raz kolejny do tego samego węzła. Jeśli zawartość cebulki jest unikalna, adwersarz znajdując w dwóch kontrolowanych przez siebie węzłach w odstępie t rund cebulki o tej samej zawartości, może założyć że jest to ta sama wiadomość po przekodowaniu. Z tego faktu adwersarz może wywnioskować część ścieżki po jakiej porusza się wiadomość. Atak taki występuje w wielu formach i może być w różny sposób modyfikowany, w celu zwiększenia efektywności i utrudnienia jego wykrycia.

Metody ochrony Zauważmy, że repetitive attack jest atakiem aktywnym - to znaczy wymaga od adwersarza kontroli nad użytkownikiem systemu i wykonywania akcji nieprzewidzianych protokołem. Z tego względu w przypadku wielu badań teoretycznych w ogóle nie jest on brany pod uwagę (np. [9, 58, 115]). W protokole działającym w praktyce atak powtórzeniowy może jednak stanowić duże zagrożenie. Podstawową techniką zabezpieczenia jest zapamiętywanie przez każdy z węzłów wszystkich wiadomości przesłanych i odrzucanie powtórzeń. Rozwiązanie takie zapewnia pełną ochronę przed atakiem powtórzeniowym, jednak jest niepraktyczne w systemach działających przez długi czas w sposób ciągły. Ponadto jest niemożliwe do zastosowania w systemach ograniczonych urządzeń, w których węzły mają małą pamięć oraz moce obliczeniowe.

Protokół `ModOnions`

Aby w sposób efektywny zaradzić atakowi powtórzeniowemu bez użycia gigantycznej pamięci zaproponowany został w pracy [57] protokół `ModOnions` (jako skrót od *Modified Onions*). Protokół ten oparty został na URE-szyfrowaniu – schemacie szyfrowania z pracy [54], które umożliwia tzw. *reszyfrowanie uniwersalne*[2]. Termin ten oznacza, że protokół umożliwia reszyfrowanie kryptogramu **bez znajomości klucza publicznego**. Wynika z tego, że trzecia strona może reszyfrować wiadomości nie znając ani nadawcy, ani odbiorcy. (Sam protokół szyfrowania stanowi rozszerzenie schematu ElGamala i został szczegółowo opisany w Rozdziale 2 pracy D1). Poniżej opisujemy najważniejsze (ze względu na zastosowanie w protokołach anonimizujących) własności URE-szyfrowania.

- **Wielokrotne szyfrowanie:** Wiadomość m może zostać zaszyfrowana wielokrotnie różnymi kluczami publicznymi $y_1, y_2, \ldots, y_n$ (którym odpowiadają klucze prywatne $x_1, x_2, \ldots, x_n$).
- **Częściowe deszyfrowanie:** Kryptogram zaszyfrowany wieloma kluczami może zostać odszyfrowany dowolnym kluczem x_i ze zbioru $\{x_1, x_2, \ldots, x_n\}$. To oznacza, że kolejność deszyfrowania może być dowolna.
- **Reszyfrowanie Uniwersalne:** Kryptogram może być reszyfrowany bez znajomości klucza publicznego i prywatnego. Ponadto nie da się ustalić związku kryptogramu przed i po reszyfrowaniu bez znajomości wszystkich kluczy prywatnych.

Własności te redukują się do bezpieczeństwa podstawowego schematu ElGamala. Są one opisane między innymi w [54].

Opis protokołu `ModOnion` (z pracy [57]) jest podobny do podstawowego protokołu cebulkowego, w szczególności wiadomość jest przesyłana poprzez λ węzłów pośrednich, w których jest przekodowywana. Atoli konstrukcja kryptogramu, określanego jako *URE-Cebulka*[3] jest inna:

[2] *Universal Re-Encryption* (URE)
[3] URE-Onion

- Przetwarzaną URE-Cebulkę tworzy $\lambda + 1$ bloków. Każdy blok to URE-kryptogram zaszyfrowany kluczami wszystkich węzłów ze ścieżki. Jeden blok zawiera właściwą wiadomość dla adresata a pozostałych λ zawiera adresy kolejnych węzłów ścieżki.

- Po otrzymaniu URE-Cebulki węzeł reszyfruje wszystkie bloki. Następnie węzeł dokonuje częściowego deszyfrowania wszystkich bloków swoim kluczem prywatnym. Specjalne kodowanie zapewnia, że dokładnie jeden blok zawiera odczytywalną wiadomość - w przypadku ostatniego węzła jest to nadana, właściwa przesyłana wiadomość. Węzły pośrednie odczytują adres kolejnego węzła na ścieżce, zastępują blok losową wartością i przesyłają wszystkie bloki do kolejnego węzła na ścieżce.

Dzięki odejściu od warstwowej konstrukcji każda część wiadomości będzie niezależnie reszyfrowana a przesłana dwa razy będzie miała inną postać w każdym węźle pośrednim. Szczegółowy opis protokołu przedstawiony jest w Rozdziale 2 pracy D1 oraz Rozdziale 3 pracy D2. Schemat ten, mimo że dawał dowodliwą odporność na atak powtórzeniowy, został skutecznie zaatakowany w pracy G. Danezisa ([29]), gdzie przedstawiono *detur attack*. Atak ten zakładał, że adwersarz w pełni kontroluje jeden z węzłów w sieci, przez który przetwarzana jest URE-Cebulka. Opierał się on na następującym pomyśle. Po otrzymaniu URE-Cebulki:

- węzeł adwersarza J_j szyfruje każdy z bloków **dodatkowym kluczem**. Ponadto dodaje jeden blok zaszyfrowany kluczem J_{j+1}, który wskazuje J_j jako kolejny węzeł na ścieżce. Następnie przesyła wszystkie bloki do J_{j+1};

- zgodnie z protokołem J_{j+1} odszyfrowuje wszystkie bloki i przesyła je z powrotem do J_j;

- węzeł J_j odszyfrowuje wszystkie bloki **dodatkowym kluczem**. W ten sposób jest w stanie odczytać z jednego bloku właściwy następnik węzła J_{j+1}, czyli węzeł J_{j+2}. W przypadku gdy J_{j+1} był ostatnim węzłem na ścieżce, jest w stanie odczytać przesyłaną do niego wiadomość.

Zauważmy, że adwersarz może swój atak iterować dla kolejnych węzłów i w ten sposób odkryć całą ścieżkę. Warto wspomnieć, że atak opisany powyżej, do pewnego stopnia, może być też wykorzystany przeciw niektórym protokołom z pracy [83]. Autor [29] prezentuje także inne ataki przeciw różnym schematom opartym o URE-szyfrowanie (np. [43]).

4.3 Nowe wyniki – odporne wersje protokołu ModOnion (prace D1 i D2)

Główną ideą protokołów z rodziny ModOnion jest budowa obiektów algebraicznych, które nie będą oparte o paradygmat enkapsulacji kryptogramów (jak w przypadku cebulek) a jednocześnie

umożlią przekodowanie całej struktury przez wyznaczonych uczestników rozproszonego protokołu, tak by zewnętrzny obserwator nie mógł powiązać wiadomości po ich przetworzeniu. Podstawową metodą jest rozdzielenie na rozłączne bloki (kryptogramy typu ElGamala) informacji o trasie przetwarzanych kryptogramów oraz stosowanie reszyfrowania uniwersalnego do każdego z bloków. Takie podejście otwiera drogę innym atakom opartym na analizie poszczególnych części przesyłanych wiadomości.

W niniejszym podrozdziale podsumujemy wyniki z prac D1 (praca [81]) oraz D2/D2' (praca [14] / [13]). Jak wskazano w wymienionych publikacjach możliwości ataków na protokoły typu `ModOnion` wynikają z trzech zaobserwowanych własności.

1. URE-cebulka może być modyfikowana w taki sposób, aby spowodować określone zmiany w odpowiadającym mu tekście jawnym bez użycia klucza prywatnego.

2. URE-cebulka składa się bloków, które można przetwarzać niezależnie od siebie.

3. Mając kryptogram URE pewnej wiadomości można **bez znajomości klucza publicznego** stworzyć kryptogram dla dowolnej innej wiadomości, zaszyfrowany tym samym kluczem.

Pierwsza własność określana jest w literaturze jako *malleablity* a typowym jej przejawem jest tzw. *atak multiplikatywny*. Z drugiej strony warto zauważyć, że właśnie te własności umożliwiają niezależne reszyfrowanie informacji dla wszystkich węzłów pośrednich, co daje odporność przed atakiem powtórzeniowym. Wyniki prac omawianych w niniejszym rozdziale stanowią modyfikacje protokołu `ModOnion`, takie że powyższe własności są istotnie ograniczane a jednocześnie zachowana pozostaje możliwość reszyfrowania dająca ochronę przed atakiem powtórzeniowym.

Modyfikacje opracowane i opublikowane w pracach D1 tudzież D2 to głównie dwie techniki – deszyfrowanie kontekstowe (ang. *context-sensitive decryption*) oraz rozszerzenie paradygmatu szyfrowania ze znacznikiem (ang. *tag-based encryption*) na schematy typu URE.

4.3.1 Protokół odporny na *detour attack*

W pracy D1 ([81]) zaprezentowany został wariant protokołu ModOnion, który jest odporny na *detour attack*. Główny pomysł opisany w Rozdziale 5 polegał na stosowaniu dwóch par kluczy przez każdy z węzłów. Pierwszy klucz prywatny węzła j-tego (x_j), określany jako klucz transportowy (*transport key*), ma funkcje takie jak standardowy klucz protokołu `ModOnion`. Klucz prywatny x_j^*, nazywany kluczem docelowym (*destination key*) używany był do szyfrowania wiadomości, która miała być odczytywana w danym węźle. Pojedynczy blok w zmodyfikowanej konstrukcji kodujący wiadomość m, która ma być przetwarzana przez węzły $x_{J_1}, \ldots, x_{J_k}$, ma postać

$$E_{x_{J_1}+\ldots+x_{J_k}+x^*_{J_k}}(m),$$

[3]W tym kontekście termin ten można przetłumaczyć jako *plastyczność*.

gdzie $E_k(\cdot)$ jest kryptogramem rozszerzonego schematu ElGamala z pracy [54] z użyciem klucza prywatnego k.

W trakcie dekodowania, w węzłach $J_1, \ldots, J_k$ blok jest deszyfrowany odpowiednimi kluczami transportowymi. Dodatkowo węzeł J_k, dla którego przeznaczona jest wiadomość m, deszyfruje kryptogram kluczem $x^*_{J_k}$. W ten sposób adwersarz kontrolujący węzeł J_{k-1} nie jest w stanie wymusić na węźle J_k wskazanie kolejnego węzła (czyli J_{j+1}) na ścieżce. Istotnie, poprzez dodanie odpowiedniego bloku adwersarz potrafi zmienić trasę URE-Cebulki, tak aby została przesłana przez J_k z powrotem do J_{k-1}, jednak bez deszyfrowania wiadomości zakodowanej w odpowiednim bloku.

Warto zauważyć, że schemat jest możliwy do zrealizowania głównie dzięki temu, że do jednego bloku można stosować jednocześnie klucze transportowe i te stosowane do szyfrowania wiadomości docelowej. Jest to kolejna ciekawa własność schematu URE. Należy też podkreślić, że zaproponowany schemat ma jedynie niewiele większą złożoność obliczeniową niż oryginalny protokół ModOnion.

Analiza protokołów W pracy D1 uzasadniono miedzy innymi następujący fakt

Fakt 12. *Zmodyfikowany protokół ModOnion jest odporny na detour attack. W szczególności jego zastosowanie jest zawsze wykrywane.*

Uzasadniono także następujący fakt dotyczący protokołu z pracy D1.

Fakt 13. ***Aktywny*** *adwersarz w zmodyfikowanym protokole ModOnion nie uzyska tekstu jawnego zawartego w żadnym z bloków poza tymi, które mają być być odszyfrowane w kontrolowanych przez niego węzłach.*

Uzasadnienie tego faktu przedstawione jest w Rozdziale 6.2 pracy D1. Oczywiście z faktu tego nie wynika jeszcze, że żadne ataki nie są możliwe. Zapewnia on jedynie, że nowa konstrukcja uniemożliwia odszyfrowanie zakodowanych w cebulce informacji przez niepowołaną stronę. Adwersarz może je jednak wywnioskować np. na podstawie zachowania uczciwych węzłów. Oczywiście uzasadnienie korzysta z założenia o niemożliwości kryptoanalizy podstawowego schematu szyfrowania URE ([54]).

Inne rezultaty pracy D1 Wskazano też inne techniki zwiększające bezpieczeństwo schematów opartych o protokół URE (rozdział 5.1). W szczególności wskazano proste techniki obrony przed atakiem multiplikatywnym (*multiplicative attack*), który może stanowić punkt wyjścia do innych ataków, między innymi na niektóre zastosowania protokołu podpisów cyfrowych [82]. Zaproponowane zostały dwie podstawowe techniki:

- zastąpienie szyfrowanej wiadomości m przez $m||H(m)$, gdzie H jest silnie bezkonfliktową funkcją haszującą;

- podnoszenie przez każdy serwer pośredni z prawdopodobieństwem $1/2$ wszystkich elementów każdego bloku do kwadratu (w odpowiedniej grupie multiplikatywnej).

Pierwsza metoda jest znaną techniką generyczną zaadoptowaną jedynie do URE-szyfrowania. Druga metoda wymaga odpowiedniego kodowania i deszyfrowania przesyłanych kryptogramów w węzłach pośrednich. Dzięki niej adwersarz kontrolujący węzeł, nawet znając kolejne węzły na ścieżce, nie jest w stanie przewidzieć postaci kryptogramu, bo zależy ona od losowych wyborów poprzednich węzłów. Z drugiej strony przesłanie kilkakrotnie tego samego kryptogramu powoduje, że jest on inaczej zakodowany, co stanowi podstawę ochrony przed atakiem powtórzeniowym. Opis metody znajduje się w Rozdziale 5.1 pracy D1. Zaproponowane techniki znacząco ograniczają własności 1 i 2 opisane na początku rozdziału.

4.3.2 Dalsze wzmocnienia protokołu `ModOnion`

Zmodyfikowany protokół `ModOnion`, chociaż zapewnia odporność na atak powtórzeniowy i *detour attack*, okazał się być podatny na inne, nieznane wcześniej, rodzaje ataków. Praca D2 ([14]) prezentuje nową klasę ataków na protokoły oparte na URE. Ataki te są znacznie mniej efektywne niż atak powtórzeniowy oraz *detur attack* G. Danazisa - w szczególności adwersarz jest zmuszony wygenerować i przesłać znacznie większą liczbę komunikatów oraz kontrolować większą liczbę węzłów w sieci. Niemniej ataki te mogą być skutecznie zastosowane z istotnym z praktycznego punktu widzenia prawdopodobieństwem.

Ataki

Pierwszy z ataków opisany w Rozdziale 3.1 pracy D2 opiera się na fakcie, że adwersarz może zgadywać kolejne fragmenty ścieżki danego kryptogramu a następnie weryfikować swoją hipotezę poprzez przesyłanie kryptogramów z dodanymi, odpowiednio spreparowanymi blokami. Atak nie jest efektywny bo w ogólnym przypadku wymaga przesłania aż $\Omega(n^{\lambda})$ wiadomości, aby odkryć całą ścieżkę od nadawcy do odbiorcy, gdzie n jest liczbą węzłów w sieci. Atak opisany w Rozdziale 3.2 jest bardziej efektywny. Adwersarz może odkrywać kolejne węzły na ścieżce wysyłając jedynie $\Theta(\lambda n^2)$ spreparowanych wiadomości w średnim przypadku.

Metody ochrony przed nowymi atakami

W Rozdziale 4 pracy D2 zaproponowano metody ochrony przed atakami opisanymi w poprzednim podrozdziale. Mają one na celu uniemożliwienie adwersarzowi modyfikowanie bloków w niewykrywalny sposób. Zaproponowane zostało między innymi podejście *context-sensitive encryption* (szyfrowanie zależne od kontekstu), polegające na tym, że klucz używany do szyfrowania bloków dla węzła J_j zależy od węzła J_{j-1} oraz J_{j+1} , co znacznie ogranicza możliwości modyfikowania ścieżki przez adwersarza. Uzasadniony został między innymi następujący fakt:

Fakt 14. *Zmodyfikowany schemat* `ModOnion` *zapewnia, że Two-Hop Attack zostanie wykryty z prawdopodobieństwem* $1 - 1/n^4$*, gdzie* n *jest liczbą węzłów w sieci.*

Zaproponowano także podejście polegające na zaadoptowaniu metod szyfrowania ze znacznikiem (*tagged encryption*) z pracy [94] do schematu reszyfrowania uniwersalnego (Rozdział 4.2 pracy D2). Idea szyfrowania ze znacznikiem polega na tym, że deszyfrowanie kryptogramu możliwe jest tylko przy użyciu dodatkowego znacznika jako argumentu funkcji deszyfrującej. W rozdziale 4.2 wykazano, że tzw. *tag* potrzebny do deszyfrowania może być poprawnie reszyfrowany, zachowując wszystkie operacje algebraiczne schematu URE. Jest to wykorzystane w kolejnej modyfikacji protokołu `ModOnion` zaprezentowanej w Rozdziale 4.3. W konstrukcji URE-Cebulki tagi w kolejnych blokach jednoznacznie kodują całą jej wcześniejszą drogę, co uniemożliwia niezauważalną modyfikację cebulki.

4.4 Perspektywy dalszych badań

Można zauważyć, że zaproponowane schematy mają małe (w porównaniu z innymi protokołami anonimizującymi) wymagania dotyczące zasobów pamięci – aby uchronić system przed atakiem powtórzeniowym nie ma konieczności zapamiętywania całego dotychczasowego ruchu przetwarzanego przez konkretny węzeł. Z tego powodu mogą one być stosowane w systemach urządzeń o ograniczonej pamięci. Z praktycznego punktu widzenia nie ma możliwości zastosowania ich jednak na przykład w systemach sensorów, ze względu na złożoność obliczeniową. Obiektem badań są obecnie protokoły, które mają jednocześnie niskie wymagania dotyczące zarówno pamięci, jak i mocy obliczeniowych.

Podsumowanie

W autoreferacie przedyskutowane zostały tylko niektóre z podstawowych problemów bezpieczeństwa systemów urządzeń o silnie ograniczonych zasobach. Obserwując obecne trendy i stan badań do najważniejszych wyzwań, z praktycznego punktu widzenia, należą:

- Zbudowanie dowodliwie bezpiecznego, efektywnego protokołu anonimowej komunikacji dla heterogenicznych systemów słabych urządzeń. Szczególnie istotnym wyzwaniem wydaje się budowa protokołów tego typu dla systemów o dużej dynamice.
- Stworzenie efektywnego pod względem złożoności komunikacyjnej a jednocześnie dowodliwie bezpiecznego protokołu uwierzytelniania dla ultralekkich urządzeń takich jak RFID-tagi.
- Budowa bardziej efektywnych protokołów samoorganizacji dla radiowych sieci ad hoc, które byłyby odporne na działanie adwersarza w bardziej realistycznym modelu.

Bibliografia

[1] *http://www.sagedata.com/the_company/*.

[2] Tor. *https://www.torproject.org/*.

[3] *Valentin Fedorovich Kolchin and Boris Aleksandrovich Sevastianov and Vladimir Pavlovich Chistiakov*. V. H. Winston, 1978.

[4] *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2005 and 9th InternationalWorkshop on Randomization and Computation, RANDOM 2005, Berkeley, CA, USA, August 22-24, 2005, Proceedings*, volume 3624 of *Lecture Notes in Computer Science*. Springer, 2005.

[5] Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*. ACM, 2004.

[6] Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors. *Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings*, volume 5037 of *Lecture Notes in Computer Science*, 2008.

[7] Josh Cohen Benaloh and Michael de Mare. One-way accumulators: A decentralized alternative to digital sinatures (extended abstract). In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 274–285. Springer, 1993.

[8] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. In *IEEE Trans. Info. Theory*, pages 384–386, 1978.

[9] Ron Berman, Amos Fiat, and Amnon Ta-Shma. Provable unlinkability against traffic analysis. In Ari Juels, editor, *Financial Cryptography*, volume 3110 of *Lecture Notes in Computer Science*, pages 266–280. Springer, 2004.

[10] Marcin Bienkowski, Marek Klonowski, Miroslaw Korzeniowski, and Dariusz R. Kowalski. Dynamic sharing of a multiple access channel. In Jean-Yves Marion and Thomas Schwentick, editors, *STACS*, volume 5 of *LIPIcs*, pages 83–94. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2010.

[11] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *J. ACM*, 50(4):506–519, 2003.

[12] Jacir Luiz Bordim, Yasuaki Ito, and Koji Nakano. Randomized leader election protocols in noisy radio networks with a single transceiver. In Minyi Guo, Laurence Tianruo Yang, Beniamino Di Martino, Hans P. Zima, Jack Dongarra, and Feilong Tang, editors, *ISPA*, volume 4330 of *Lecture Notes in Computer Science*, pages 246–256. Springer, 2006.

[13] Nikita Borisov, Marek Klonowski, Miroslaw Kutylowski, and Anna Lauks-Dutka. Attacking and repairing the improved modonions protocol. In Donghoon Lee and Seokhie Hong, editors, *ICISC*, volume 5984 of *Lecture Notes in Computer Science*, pages 258–273. Springer, 2009.

[14] Nikita Borisov, Marek Klonowski, Miroslaw Kutylowski, and Anna Lauks-Dutka. Attacking and repairing the improved modonions protocol-tagging approach. *TIIS*, 4(3):380–399, 2010.

[15] Clay Shields Brian Neil Levine and N. Boris Margolin. A survey of solutions to the sybil attack, 2006. Available from World Wide Web: `http://prisms.cs.umass.edu/brian/bubs/levine.sybil.tr.2006.pdf`.

[16] Julien Bringer, Hervé Chabanne, and Emmanuelle Dottax. Hb^{++}: a lightweight authentication protocol secure against some attacks. In *SecPerU*, pages 28–33. IEEE Computer Society, 2006.

[17] Julien Bringer, Hervé Chabanne, Tom A. M. Kevenaar, and Bruno Kindarji. Extending match-on-card to local biometric identification. In *COST 2101/2102 Conference*, volume 5707 of *Lecture Notes in Computer Science*, pages 178–186. Springer, 2009.

[18] Kamalika Chaudhuri and Nina Mishra. When random sampling preserves privacy. In Cynthia Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 198–213. Springer, 2006.

[19] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.

[20] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *J. Cryptology*, 1(1):65–75, 1988.

[21] Wenyi Che, Huan Deng, Wang Tan, and Junyu Wang. A random number generator for application in rfid tags. In Damith C. Ranasinghe and Peter H. Cole, editors, *Networked RFID Systems and Lightweight Cryptography*, pages 279–287. Springer Berlin Heidelberg, 2008.

[22] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt. Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3):727–752, 2010.

[23] Bogdan S. Chlebus and Dariusz R. Kowalski. A better wake-up in radio networks. In Soma Chaudhuri and Shay Kutten, editors, *PODC*, pages 266–274. ACM, 2004.

[24] Marek Chrobak, Leszek Gasieniec, and Dariusz R. Kowalski. The wake-up problem in multihop radio networks. *SIAM J. Comput.*, 36(5):1453–1471, 2007.

[25] Jacek Cichon, Rafal Kapelko, Jakub Lemiesz, and Marcin Zawada. On alarm protocol in wireless sensor networks. In Nikolaidis and Wu [104], pages 43–52.

[26] Jacek Cichon, Jakub Lemiesz, and Marcin Zawada. On cardinality estimation protocols for wireless sensor networks. In Hannes Frey, Xu Li, and Stefan Rührup, editors, *ADHOC-NOW*, volume 6811 of *Lecture Notes in Computer Science*, pages 322–331. Springer, 2011.

[27] B.N. Levine C.Piro, C.Shields. Detecting the sybil attack in ad hoc networks. In *Proc. IEEE/ACM SecureComm*, pages 1–11, 2006.

[28] Jurek Czyzowicz, Leszek Gasieniec, Dariusz R. Kowalski, and Andrzej Pelc. Consensus and mutual exclusion in a multiple access channel. In Idit Keidar, editor, *DISC*, volume 5805 of *Lecture Notes in Computer Science*, pages 512–526. Springer, 2009.

[29] George Danezis. Breaking four mix-related schemes based on universal re-encryption. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006.

[30] George Danezis, Chris Lesniewski-Laas, M. Frans Kaashoek, and Ross J. Anderson. Sybil-resistant dht routing. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, *ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2005.

[31] Sylvie Delaët, Partha Sarathi Mandal, Mariusz A. Rokicki, and Sébastien Tixeuil. Deterministic secure positioning in wireless sensor networks. *Theor. Comput. Sci.*, 412(35):4471–4481, 2011.

[32] Claudia Díaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards measuring anonymity. In Dingledine and Syverson [35], pages 54–68.

[33] Roger Dingledine. Anonymity bibliography. `http://freehaven.net/anonbib/`.

[34] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320. USENIX, 2004.

[35] Roger Dingledine and Paul F. Syverson, editors. *Privacy Enhancing Technologies, Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002, Revised Papers*, volume 2482 of *Lecture Notes in Computer Science*. Springer, 2003.

[36] Shlomi Dolev, Seth Gilbert, Rachid Guerraoui, and Calvin C. Newport. Secure communication over radio channels. In Rida A. Bazzi and Boaz Patt-Shamir, editors, *PODC*, pages 105–114. ACM, 2008.

[37] Shlomi Dolev, Andreas Pfitzmann, and Rafail Ostrovsky. 05411 abstracts collection – anonymous communication and its applications. In Shlomi Dolev, Rafail Ostrovsky, and Andreas Pfitzmann, editors, *Anonymous Communication and its Applications*, volume 05411 of *Dagstuhl Seminar Proceedings*. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, 2005.

[38] John R. Douceur. The sybil attack. In Druschel et al. [39], pages 251–260.

[39] Peter Druschel, M. Frans Kaashoek, and Antony I. T. Rowstron, editors. *Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002, Revised Papers*, volume 2429 of *Lecture Notes in Computer Science*. Springer, 2002.

[40] Cynthia Dwork. Differential privacy: A survey of results. In Manindra Agrawal, Ding-Zhu Du, Zhenhua Duan, and Angsheng Li, editors, *TAMC*, volume 4978 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2008.

[41] Cynthia Dwork. The promise of differential privacy: A tutorial on algorithmic techniques. In Rafail Ostrovsky, editor, *FOCS*, pages 1–2. IEEE, 2011.

[42] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. Springer, 1992.

[43] Peter Fairbrother. An improved construction for universal re-encryption. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 79–87. Springer, 2004.

[44] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for rfid systems using the aes algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer, 2004.

[45] Philippe Flajolet. Singularity analysis and asymptotics of bernoulli sums. *Theor. Comput. Sci.*, 215(1-2):371–381, 1999.

[46] Michael J. Freedman, Emil Sit, Josh Cates, and Robert Morris. Introducing tarzan, a peer-to-peer anonymizing network layer. In Druschel et al. [39], pages 121–129.

[47] Dmitry Frumkin and Adi Shamir. Un-trusted-hb: Security vulnerabilities of trusted-hb. Cryptology ePrint Archive, Report 2009/044, 2009.

[48] Simson L. Garfinkel, Ari Juels, and Ravikanth Pappu. Rfid privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy*, 3(3):34–43, 2005.

[49] Leszek Gasieniec, Andrzej Pelc, and David Peleg. The wakeup problem in synchronous broadcast systems. *SIAM J. Discrete Math.*, 14(2):207–222, 2001.

[50] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. $\text{Hb}^{\#}$: Increasing the security and efficiency of hb^{+}. In *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 361–378. Springer, 2008.

[51] Seth Gilbert, Rachid Guerraoui, and Calvin C. Newport. Of malicious motes and suspicious sensors: On the efficiency of malicious interference in wireless networks. In Alexander A. Shvartsman, editor, *OPODIS*, volume 4305 of *Lecture Notes in Computer Science*, pages 215–229. Springer, 2006.

[52] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Onion routing. *Commun. ACM*, 42(2):39–41, 1999.

[53] Zbigniew Golebiewski, Krzysztof Majcher, Filip Zagorski, and Marcin Zawada. Practical attacks on hb and hb+ protocols. In Claudio Agostino Ardagna and Jianying Zhou, editors, *WISTP*, volume 6633 of *Lecture Notes in Computer Science*, pages 244–253. Springer, 2011.

[54] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul F. Syverson. Universal re-encryption for mixnets. In Tatsuaki Okamoto, editor, *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 163–178. Springer, 2004.

[55] Philippe Golle and Ari Juels. Dining cryptographers revisited. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 456–473. Springer, 2004.

[56] Philippe Golle and Ari Juels. Parallel mixing. In Atluri et al. [5], pages 220–226.

[57] Marcin Gomulkiewicz, Marek Klonowski, and Miroslaw Kutylowski. Onions based on universal re-encryption - anonymous communication immune against repetitive attack. In Chae Hoon Lim and Moti Yung, editors, *WISA*, volume 3325 of *Lecture Notes in Computer Science*, pages 400–410. Springer, 2004.

[58] Marcin Gomulkiewicz, Marek Klonowski, and Miroslaw Kutylowski. Provable unlinkability against traffic analysis already after o(log(n)) steps! In Kan Zhang and Yuliang Zheng, editors, *ISC*, volume 3225 of *Lecture Notes in Computer Science*, pages 354–366. Springer, 2004.

[59] Nathan Good, David Molnar, Jennifer M. Urban, Deirdre K. Mulligan, Elizabeth Miles, Laura Quilter, and David Wagner. Radio frequency id and privacy with information goods. In Vijay Atluri, Paul F. Syverson, and Sabrina De Capitani di Vimercati, editors, *WPES*, pages 41–42. ACM, 2004.

[60] Ghaith Hammouri and Berk Sunar. Puf-hb: A tamper-resilient hb based authentication protocol. In Bellovin et al. [6], pages 346–365.

[61] Johan Håstad. Some optimal inapproximability results. In *STOC*, pages 1–10, 1997.

[62] Tatsuya Hayashi, Koji Nakano, and Stephan Olariu. Randomized initialization protocols for packet radio networks. In *IPPS/SPDP*, pages 544–. IEEE Computer Society, 1999.

[63] Daniel E. Holcomb, Wayne P. Burleson, and Kevin Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Computers*, 58(9):1198–1210, 2009.

[64] Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. *Lecture Notes in Computer Science*, 2248, 2001. Available from World Wide Web: `citeseer.ist.psu.edu/hopper01secure.html`.

[65] Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors. *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, Washington, DC, USA, October 27-30, 2003*. ACM, 2003.

[66] Markus Jakobsson. A practical mix. In *EUROCRYPT*, pages 448–461, 1998.

[67] Markus Jakobsson. Flash mixing. In *PODC*, pages 83–89, 1999.

[68] Markus Jakobsson and Ari Juels. Mix and match: Secure function evaluation via ciphertexts. In Tatsuaki Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 162–177. Springer, 2000.

[69] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In Dan Boneh, editor, *USENIX Security Symposium*, pages 339–353. USENIX, 2002.

[70] Ari Juels and Ravikanth Pappu. Squealing euros: Privacy protection in rfid-enabled banknotes. In Rebecca N. Wright, editor, *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121. Springer, 2003.

[71] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In Jajodia et al. [65], pages 103–111.

[72] Ari Juels and Stephen A. Weis. *Authenticating Pervasive Devices with Human Protocols*, volume 3621. November 2005.

[73] Tomasz Jurdzinski and Grzegorz Stachowiak. Probabilistic algorithms for the wake-up problem in single-hop radio networks. *Theory Comput. Syst.*, 38(3):347–367, 2005.

[74] Jedrzej Kabarowski, Miroslaw Kutylowski, and Wojciech Rutkowski. Adversary immune size approximation of single-hop radio networks. In Jin yi Cai, S. Barry Cooper, and Angsheng Li, editors, *TAMC*, volume 3959 of *Lecture Notes in Computer Science*, pages 148–158. Springer, 2006.

[75] Jonathan Katz. Efficient cryptographic protocols based on the hardness of learning parity with noise. In Steven D. Galbraith, editor, *IMA Int. Conf.*, volume 4887 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2007.

[76] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the hb and hb^+ protocols. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2006.

[77] Dogan Kesdogan, Jan Egner, and Roland Büschkes. Stop-and-go-mixes providing probabilistic anonymity in an open system. In David Aucsmith, editor, *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 83–98. Springer, 1998.

[78] Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi. Efficient authentication from hard learning problems. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 7–26. Springer, 2011.

[79] Marek Klonowski and Michal Koza. Pow-based approach to sybil-type attacks in wireless sensor network. *Praca zgłoszona do publikacji*.

[80] Marek Klonowski and Miroslaw Kutylowski. Provable anonymity for networks of mixes. In Mauro Barni, Jordi Herrera-Joancomartí, Stefan Katzenbeisser, and Fernando Pérez-González, editors, *Information Hiding*, volume 3727 of *Lecture Notes in Computer Science*, pages 26–38. Springer, 2005.

[81] Marek Klonowski, Miroslaw Kutylowski, and Anna Lauks. Repelling detour attack against onions with re-encryption. In Bellovin et al. [6], pages 296–308.

[82] Marek Klonowski, Miroslaw Kutylowski, Anna Lauks, and Filip Zagorski. Universal re-encryption of signatures and controlling anonymous information flow. *Tatra Mountains Mathematical Publications*, 33:179–188, 2006.

[83] Marek Klonowski, Miroslaw Kutylowski, and Filip Zagorski. Anonymous communication with on-line and off-line onion encoding. In Peter Vojtás, Mária Bieliková, Bernadette Charron-Bost, and Ondrej Sýkora, editors, *SOFSEM*, volume 3381 of *Lecture Notes in Computer Science*, pages 229–238. Springer, 2005.

[84] Marek Klonowski and Kamil Wolny. Immune size approximation algorithms in ad hoc radio network. In Nikolaidis and Wu [104], pages 43–52.

[85] Dariusz R. Kowalski. On selection problem in radio networks. In Marcos Kawazoe Aguilera and James Aspnes, editors, *PODC*, pages 158–166. ACM, 2005.

[86] Matthias Krause and Dirk Stegemann. More on the security of linear rfid authentication protocols. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 182–196. Springer, 2009.

[87] Hugo Krawczyk. Lfsr-based hashing and authentication. In Yvo Desmedt, editor, *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 129–139. Springer, 1994.

[88] Miroslaw Kutylowski and Wojciech Rutkowski. Adversary immune leader election in ad hoc radio networks. In Giuseppe Di Battista and Uri Zwick, editors, *ESA*, volume 2832 of *Lecture Notes in Computer Science*, pages 397–408. Springer, 2003.

[89] Miroslaw Kutylowski and Wojciech Rutkowski. Secure initialization in single-hop radio networks. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *ESAS*, volume 3313 of *Lecture Notes in Computer Science*, pages 31–41. Springer, 2004.

[90] Miroslaw Kutylowski and Filip Zagorski. Scratch, click & vote: E2e voting over the internet. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*, pages 343–356. Springer, 2010.

[91] Marc Langheinrich. A survey of rfid privacy approaches. *Personal and Ubiquitous Computing*, 13(6):413–421, 2009.

[92] Éric Levieil and Pierre-Alain Fouque. An improved lpn algorithm. In *SCN*, pages 348–359, 2006.

[93] Vadim Lyubashevsky. The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In *APPROX-RANDOM* [4], pages 378–389.

[94] Philip D. MacKenzie, Michael K. Reiter, and Ke Yang. Alternatives to non-malleability: Definitions, constructions, and applications (extended abstract). In Moni Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 171–190. Springer, 2004.

[95] Dominik Pajak Marek Klonowski. On k-alert problem. In *IPDPS (Accepted)*. IEEE, 2012.

[96] Robert Metcalfe and David Boggs. Ethernet: Distributed packet switching for local computer networks. *Commun. ACM*, 19(7):395–404, 1976.

[97] David Molnar and David Wagner. Privacy and security in library rfid: issues, practices, and architectures. In Atluri et al. [5], pages 210–219.

[98] Thomas Moscibroda, Pascal von Rickenbach, and Roger Wattenhofer. Analyzing the energy-latency trade-off during the deployment of sensor networks. In *INFOCOM*. IEEE, 2006.

[99] Paul A. Moskowitz, Andris Lauris, and Stephen S. Morris. A privacy-enhancing radio frequency identification tag: Implementation of the clipped tag. In *PerCom Workshops*, pages 348–351. IEEE Computer Society, 2007.

[100] Jorge Munilla and Alberto Peinado. Hb-mp: A further step in the hb-family of lightweight authentication protocols. *Computer Networks*, 51(9):2262–2267, 2007.

[101] Koji Nakano and Stephan Olariu. Randomized o (log log n)-round leader election protocols in packet radio networks. In Kyung-Yong Chwa and Oscar H. Ibarra, editors, *ISAAC*, volume 1533 of *Lecture Notes in Computer Science*, pages 209–218. Springer, 1998.

[102] Koji Nakano and Stephan Olariu. Randomized leader election protocols in radio networks with no collision detection. In D. T. Lee and Shang-Hua Teng, editors, *ISAAC*, volume 1969 of *Lecture Notes in Computer Science*, pages 362–373. Springer, 2000.

[103] James Newsome, Elaine Shi, Dawn Xiaodong Song, and Adrian Perrig. The sybil attack in sensor networks: analysis & defenses. In Kannan Ramchandran, Janos Sztipanovits, Jennifer C. Hou, and Thrasyvoulos N. Pappas, editors, *IPSN*, pages 259–268. ACM, 2004.

[104] Ioanis Nikolaidis and Kui Wu, editors. *Ad-Hoc, Mobile and Wireless Networks, 9th International Conference, ADHOC-NOW 2010, Edmonton, Alberta, Canada, August 20-22, 2010. Proceedings*, volume 6288 of *Lecture Notes in Computer Science*. Springer, 2010.

[105] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani. *Algorithmic Game Theory*. Cambridge University Press, New York, NY, USA, 2007.

[106] Khaled Ouafi, Raphael Overbeck, and Serge Vaudenay. On the security of hb# against a man-in-the-middle attack. In Josef Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *Lecture Notes in Computer Science*, pages 108–124. Springer, 2008.

[107] Christos M. Papadimitriou. *Computational complexity*. Addison-Wesley, Reading, Massachusetts, 1994.

[108] Adrian Perrig, John A. Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.

[109] C. S. Petrie and J. Alvin Connelly. The sampling of noise for random number generation. In *ISCAS (6)*, pages 26–29. IEEE, 1999.

[110] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity - a proposal for terminology. In Hannes Federrath, editor, *Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 2000.

[111] Birgit Pfitzmann and Andreas Pfitzmann. How to break the direct rsa-implementation of mixes. In *EUROCRYPT*, pages 373–381, 1989.

[112] Robert Sedgewick Philippe Flajolet. *ANALYTIC COMBINATORICS*. Cambridge University Press, New York, NY, USA, 2009.

[113] Selwyn Piramuthu. Hb and related lightweight authentication protocols for secure rfid tag/reader authentication. Proceedings of the Conference on Collaborative Electronic Commerce Technology and Research (CollECTer Europe), pp. 239-247, 2006.

[114] Ryan Pries, Wei Yu, Xinwen Fu, and Wei Zhao. A new replay attack against anonymous communication networks. In *ICC*, pages 1578–1582. IEEE, 2008.

[115] Charles Rackoff and Daniel R. Simon. Cryptographic defense against traffic analysis. In *STOC*, pages 672–681, 1993.

[116] Ronald L. Rivest. Chaffing and winnowing: Confidentiality without encryption, 1998. Available from World Wide Web: `http://theory.lcs.mit.edu/~rivest/chaffing.txt`.

[117] Andrei Serjantov and George Danezis. Towards an information theoretic metric for anonymity. In Dingledine and Syverson [35], pages 41–53.

[118] Luis von Ahn, Andrew Bortz, and Nicholas J. Hopper. k-anonymous message transmission. In Jajodia et al. [65], pages 122–130.

[119] Dan E. Willard. Log-logarithmic selection resolution protocols in a multiple access channel. *SIAM J. Comput.*, 15(2):468–477, 1986.

Część II

Omówienie pozostałych osiągnięć naukowo - badawczych

Inne prace naukowe

Ponad 40 prac z mojego dorobku naukowego zostało opublikowanych w recenzowanych wydawnictwach o zasięgu międzynarodowym. W tym

- 5 przed uzyskaniem stopnia doktora, które nie weszły w skład rozprawy doktorskiej (**ANO5, ANO6, SD4, SEC5, SIG6**);
- 5 zawartych w pierwszej rozprawie doktorskiej (**ANO1, ANO2, ANO3, ANO7, SEC8**);
- 4 zawarte w drugiej rozprawie doktorskiej (**ANO4, SD2, SD3, SD5**);
- 28 po uzyskaniu stopnia doktora, które nie weszły w skład żadnej z rozpraw doktorskich (w tym **DA1, DA2, DA3, DA4, MAT1, MAT2, SD1, SD6, SEC1, SEC2, SEC3, SEC4, SEC6, SEC7, SEC9, SIG1, SIG2, SIG3, SIG4, SIG5,** . . .).

Poniżej zamieszczona została lista prac **z wyłączeniem pozycji opisanych we wcześniejszej części autoreferatu** wraz etykietami używanymi wyżej. Pełna lista znajduje się w odrębnym załączniku.

ANO1 Marek Klonowski, Mirosław Kutyłowski: *Provable Anonymity for Networks of Mixes*, Seria Lecture Notes in Computer Science (Springer Verlag) 3727, str. 26 - 28. (Konferencja Information Hiding 2005).

ANO2 Marek Klonowski, Mirosław Kutyłowski, Filip Zagórski: *Anonymous communication with on-line and off-line onion encoding*, Seria Lecture Notes in Computer Science (Springer Verlag) 3381, str. 229 - 238. (Konferencja SOFSEM 2005)

ANO3 Marcin Gomułkiewicz, Marek Klonowski, Mirosław Kutyłowski: *Onion Routing Based on Universal Re–Encryption Immune against Repetitive Attack*, Seria Lecture Notes in Computer Science (Springer Verlag) 3325, str. 400 - 410. (Konferencja WISA 2005)

ANO4 Marcin Gomułkiewicz, Marek Klonowski, Mirosław Kutyłowski: *Provable Unlinkability Against Traffic Analysis already after $\mathcal{O}(\log(n))$ steps !*, Seria Lecture Notes in Computer Science (Springer Verlag) 3225, str. 346 - 366. (Konferencja ISC 2004)

ANO5 Marcin Gomułkiewicz, Marek Klonowski, Mirosław Kutyłowski: *Rapid mixing and security of Chaum's visual electronic voting*, Seria Lecture Notes in Computer Science (Springer Verlag) 2808, str. 135 - 146. (Konferencja ESORICS 2003)

ANO6 Marek Klonowski, Mirosław Kutyłowski, Bartłomiej Różański: *Hiding Data Sources in P2P Networks*, Proceedings of Applied Public Key Infrastructure w serii Frontiers in Artificial Intelligence and Applications (128), (IOS Press), str. 23 -34. (Konferencja IWAP 2005)

ANO7 Jan Iwanik, Marek Klonowski, Mirosław Kutyłowski: *DUO–Onions and Hydra–Onions – failure and adversary resistant onion protocols*, Proceedings of IFIP Conference on Communications and Multimedia Security (Springer Verlag), str. 1-15. (Konferencja CCMS 2004)

DA1 Andreé Brinkman, Marcin Bieńkowski, Marek Klonowski, Mirosław Korzeniowski: *Skew CCC+: Heterogenious Distributed Hash Table*, Seria Lecture Notes in Computer Science (Springer Verlag) 6490, str. 219 - 234. (Konferencja OOPODIS 2010)

DA2 Marcin Bieńkowski, Leszek Gąsieniec, Marek Klonowski, Mirosław Korzeniowski, Stefan Schmid: *Event Extent Estimation*, Seria Lecture Notes in Computer Science (Springer Verlag) 6058, str. 57 - 71. (Konferencja SIRROCCO 2010)

DA3 Marcin Bieńkowski, Marek Klonowski, Dariusz R. Kowalski , Mirosław Korzeniowski: *Dynamic sharing of a multiple access channel*. Proceedings of 27th International Symposium on Theoretical Aspects of Computer Science LIPIcs (5) (Schloss Dagstuhl- Leibniz-Zentrum fuer Informatik), str. 83 - 94. (Konferencja STACS 2010)

DA4 Marek Klonowski, Dominik Pająk: *On k-Alert problem* (**PRZYJĘTA** na IPDPS 2012.)

MAT1 Jacek Cichoń, Marek Klonowski: *A Note on Invariant Random Variables*, DMTCS proc. AM (Discrete Mathematics and Theoretical Computer Science), str. 107-116. (Konferencja AofA 2010)

MAT2 Jacek Cichoń, Marek Klonowski, Łukasz Krzywiecki, Bartłomiej Różański, Paweł Zieliński: *Random Subsets of Interval and P2P Protocols*, Seria Lecture Notes in Computer Science (Springer Verlag) 4627, str. 409 - 421. (Konferencja RANDOM 2007)

SD1 Marek Klonowski, Mirosław Kutyłowski, Michał Koza: *How to Transmit Messages via WSN in a Hostile Environment*, Proceedings of the International Conference on Security and Cryptography - SECRYPT (SciTePress), str. 387-390. (Konferencja SECRYPT 2011)

SD2 Jacek Cichoń, Marek Klonowski, Mirosław Kutyłowski: *Distributed Verification of Mixing - Local Forking Proofs Model*, Seria Lecture Notes in Computer Science (Springer Verlag) 5107, str. 128 - 140. (Konferencja ACISP 2008)

SD3 Marek Klonowski, Mirosław Kutyłowski, Michał Ren, Katarzyna Rybarczyk: *Forward-secure Key Evolution Protocol in Wireless Sensor Networks*, Seria Lecture Notes in Computer Science (Springer Verlag) 4856, str. 102 - 120. (Konferencja CANS 2007)

SD4 Marcin Gogolewski, Marek Klonowski, Mirosław Kutyłowski: *Local View Attack on Anonymous Communication*, Seria Lecture Notes in Computer Science (Springer Verlag) 3679, str. 475 - 488. (Konferencja ESORICS 2005)

SD5 Jacek Cichoń, Marek Klonowski, Mirosław Kutyłowski: *Privacy Protection for Dynamic Systems Based on RFID Tags*, Proceedings of 4th IEEE International Workshop on Pervasive Computing and Communication Security (IEEE Computer Society), str. 235-240. (Konferencja PerCom 2007)

SD6 Marek Klonowski, Kamil Wolny: *Immune Size Approximation Algorithms in Ad Hoc Radio Network,* **PRZYJĘTA** do druku w serii Lecture Notes in Computer Science (Springer Verlag) oraz do prezentacji na konferencji EWNS 2012.

SEC1 Marek Klonowski, Michał Przykucki, Tomasz Strumiński, Małgorzata Sulkowska: *Practical universal random sampling*, Seria Lecture Notes in Computer Science (Springer Verlag) 6434, str. 84 - 100. (Konferencja IWSEC 2010)

SEC2 Marek Klonowski, Michał Przykucki, Tomasz Strumiński: *Data Deletion with Provable Security*, Seria Lecture Notes in Computer Science (Springer Verlag) 5379, str. 240 - 255. (Konferencja WISA 2009)

SEC3 Marek Klonowski, Tomasz Strumiński: *Proofs of communication and its application for fighting SPAM*, Seria Lecture Notes in Computer Science (Springer Verlag) 4910, str. 720 - 730. (Konferencja SOFSEM 2008)

SEC4 Marcin Gogolewski, Marek Klonowski, Mirosław Kutyłowski, Przemysław Kubiak, Anna Lauks, Filip Zagórski: *Kleptographic Attacks on E-voting Schemes*, Seria Lecture Notes in Computer Science (Springer Verlag) 3995, str. 494 - 508. (Konferencja ETRICS 2006)

SEC5 Marek Klonowski, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski: *A Practical Voting Scheme with Receipts*, Seria Lecture Notes in Computer Science (Springer Verlag) 3650, str. 490 - 497. (Konferencja ISC 2005)

SEC6 Krzysztof Barczyński, Przemysław Błaśkiewicz, Marek Klonowski, Mirosław Kutyłowski: *Self-keying identification mechanism for small devices*. Rozdział w Secure and Trust Computing, Data Management and Applications – Communications in Computer and Information Science (Springer Verlag) 186 (1), str. 37 - 44.

SEC7 Marek Klonowski, Michał Przykucki, Tomasz Strumiński: *Data deletion with time-aware adversary model* Proceedings of 12th IEEE/IFIP International Symposium on Trusted Computing and Communications (IEEE Computer Society), str. 659 - 664. (Konferencja CSE 2011)

SEC8 Marek Klonowski, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski: *Universal Re-Encryption of signatures and controlling anonymous information flow*, Tatra Mountains Mathematical Publications 33(2006), str. 179-188.

SEC9 Joanna Boroń, Marek Klonowski: *Single Transferable Vote Analogue of Desmedet-Kurosawa Protocol* Tatra Mountains Mathematical Publications 41(2008), str. 93-106.

SIG1 Marek Klonowski, Mirosław Kutyłowski, Łukasz Krzywiecki, Anna Lauks: *Step-out Group Signatures*, Computing (Springer Verlag) 85(1-2), str. 137-151.

SIG2 Marek Klonowski, Mirosław Kutyłowski, Łukasz Krzywiecki, Anna Lauks: *Step-out Ring Signatures*, Seria Lecture Notes in Computer Science (Springer Verlag) 5162, str. 431 - 442. (Konferencja MFCS 2008)

SIG3 Marek Klonowski, Przemysław Kubiak, Mirosław Kutylowski: *Practical Deniable Encryption*, Seria Lecture Notes in Computer Science (Springer Verlag) 4910, str. 599 - 609. (Konferencja SOFSEM 2008)

SIG4 Marek Klonowski, Anna Lauks: *Extended Sanitizable Signatures*, Seria Lecture Notes in Computer Science (Springer Verlag) 4296, str. 343 - 356. (Konferencja ICISC 2006)

SIG5 Marek Klonowski, Przemysław Kubiak, Mirosław Kutyłowski, Anna Lauks: *How to Protect a Signature from Being Shown to a Third Party*, Seria Lecture Notes in Computer Science (Springer Verlag) 4083, str. 192 - 202. (Konferencja TrustBus 2006)

SIG6 Marek Klonowski, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski: *Conditional Digital Signatures*, Seria Lecture Notes in Computer Science (Springer Verlag) 3592, str. 206 - 215. (Konferencja TrustBus 2005)

Omówienie tematyki badań Wymienione prace wpisują się w kilka nurtów badań umiejscowionych na pograniczu teorii bezpieczeństwa komputerowego i algorytmów rozproszonych. Szczególnie w latach 2003–2008 główny obiekt moich zainteresowań stanowiły badania nad anonimową komunikacją. W pracach **ANO1, ANO3, ANO4** analizowano rozproszone protokoły anonimizujące. Badania dyskutowanych modeli w znacznej części sprowadzały się do analizy tempa zbieżności pewnych łańcuchów Markowa a do ich analizy wykorzystano głównie metody *couplingowe* – w szczególności technikę *path coupling*. Dalsze prace z zakresu anonimowości dotyczyły ulepszeń znanych algorytmów. Duża ich część oparta była na wykorzystywaniu struktur algebraicznych używanych w szyfrach homomorficznych (szczególnie wariantów protokołu ElGamala) i przystosowaniu ich do protokołów anonimizacyjnych. Wskazywano także na możliwości użycia technik anonimowej komunikacji dla zwiększenia bezpieczeństwa sieci P2P (**ANO6**).

Część prac należy zakwalifikować jako typowe prace z algorytmów rozproszonych, bez odniesienia do zagadnień bezpieczeństwa. W tym kontekście wymienić należy prace **DA3, DA4**, gdzie bada się problemy związane z komunikacją w różnych modelach MAC[4] oraz pracę **DA2**, która traktuje o efektywnych metodach eksploracji sieci po częściowej awarii. Wyniki w ramach tego nurtu prac uzyskano dzięki wykorzystaniu stosunkowo szerokiego spektrum technik matematycznych - poza standardowymi jak nierówności Cheroffa i Hoeffdinga czy twierdzenia dla modelu balls-and-bins[5] użyte były własności pewnych (np. planarnych) klas grafów, metoda probabilistyczna czy tzw. *superimposed codes*.

W dorobku znalazły się także dwie prace o charakterze bardziej matematycznym, choć inspirowane zagadnieniami informatycznymi. W pracy **MAT1** pokazaliśmy pewne własności dla

[4] *Multiple Access Channel*

[5] Model określany też jako *random allocation*

zmiennych losowych o wartościach w zbiorze z działaniem grupy[6]. W szczególności pokazano jak można w efektywny sposób znajdować momenty pewnej klasy zmiennych losowych. Teoria ta może zostać wykorzystana badania schematów predystrybucji kluczy kryptograficznych w sieciach ad hoc. Praca **MAT2** przedstawia pewne własności losowych odcinków oraz ich zastosowanie do sieci P2P ze szczególnym uwzględnieniem protokołu CHORD.

Prace **SD1-SD6** dotyczą bezpieczeństwa w systemach rozproszonych i są tematycznie związane z pracami omówionymi w poprzedniej części autoreferatu. Publikacje te dotyczą między innymi systemów RFID oraz technik weryfikowania w systemach anonimizujących (**SD2**) oraz zagrożeń protokołu routingu, gdy adwersarz kontroluje część stacji (**SD1**). Przy tym samym założeniu w pracy **SD6** badany jest problem *size approximation*, gdy adwersarz kontroluje część stacji. Warto wspomnieć też pracę **SD3**, w której pokazany jest schemat ewolucji kluczy kryptograficznych zapewniający jednocześnie własności *foreward-security* oraz *backward-security*. W przypadku wielu prac z tego nurtu pokazane zostało, że analiza bezpieczeństwa może zostać zredukowana do badania własności naturalnych obiektów matematycznych. W szczególności bezpieczeństwo protokołu z pracy **SD5** sprowadza się do badania zmodyfikowanego klasycznego spaceru po hiperkostce. Własności spacerów losowych stanowiły też podstawę analizy protokołów z prac **SD2, SD3**. Ostania praca wykorzystywała ponadto analizę średnicy pewnych digrafów losowych.

Prace **SEC1-SEC9** dotyczą typowych zagadnień bezpieczeństwa komputerowego. Ich tematyką jest między innymi konstrukcja i analiza protokołów e-wyborów (**SEC5, SEC9**). W innej pracy (**SEC8**) zaproponowane, przeanalizowane i zaimplementowane zostały nowe metody ochrony przed SPAMem oparte o tzw. dowody komunikacji. Prace **SEC2, SEC7** traktują o trwałym usuwaniu danych z dysków magnetycznych w ujęciu formalnym. W ramach tego nurtu badań analizowane były także schematy uwierzytelniania dla małych urządzeń (**SEC6**) oraz techniki anonimizacji zapytań do baz danych (**SEC1**). Prace z tego nurtu także oparte były w dużej mierze na analizie struktur losowych. W niektórych pracach analiza okazywała się być zaskakująco prosta. Na przykład w **SEC1** za pomocą elementarnych metod, które nie wykraczają poza nierówności Chernoffa udało się poprawić wynik Chaudhuri oraz Mishri z CRYPTO '06.

Istotną i zamkniętą już obecnie część pracy poświęciłem technologiom podpisów cyfrowych (**SIG1-SIG7**). W pracach tych zaprezentowano protokoły podpisów elektronicznych oferujące niestandardowe, choć naturalne, funkcjonalności. W szczególności przedstawiono protokoły o ograniczonej możliwości udowodnienia poprawności podpisu osobom trzecim (**SIG1,SIG3,SIG5,SIG6**) oraz protokoły umożliwiające ograniczone modyfikacje wiadomości przez trzecią stronę, tak by mogła być poprawnie weryfikowana z oryginalnym podpisem (**SIG4**). Podjęto też próbę wykorzystania do protokołów podpisu cyfrowego wybranych struktur kombinatorycznych- w szczególności użyto filtrów Blooma jako zamiennika nieefektywnych obliczeniowo *akumulatorów kryptograficznych*[7]. Większość jednak konstrukcji została zbudowana jako modyfikacje protokołów szyfrowania homomorficznego w grupach cyklicznych (głównie modyfikacje protokołu ElGamala).

[6] Group action

[7] Technika zaproponowana w [7]

Projekty naukowe

Uczestnictwo w programach europejskich i innych programach międzynarodowych lub krajowych

Wykonywane:

- Grant własny, *Algorytmika sieci Ad Hoc*, NN206 3697 39, Politechnika Wrocławska, główny wykonawca.

Wykonane:

- Grant własny MNiSW 2008-2011, *Protokoły bezpiecznej komunikacji dla urządzeń o silnie ograniczonych zasobach*, NN206 2573 35, Politechnika Wrocławska, **kierownik**;
- **Projekt UE**: FRONTS (Foundations of Adaptive Networked Societies of Tiny Artefacts) - projekt w ramach 7 PR;
- **Projekt UE**: DELIS (Dynamically Evolving large Information Systems) - projekt w ramach 6 PR;
- **Projekt UE**: *Nowoczesne technologie informatyczne i ich zastosowanie w administracji publicznej i sektorze usług bankowych*. Projekt realizowany w ramach działania 2.6 ZPORR *Regionalne Strategie Innowacyjne i Transfer wiedzy*;
- Projekt badawczo–wdrożeniowy, *Infrastructure of secure administration signature* (Podpis urzędowy), wykonawca;
- Grant własny, *Zaawansowane metody randomizacyjne w systemach rozproszonych*, NN206 1842 33, Politechnika Wrocławska, Politechnika Wrocławska, główny wykonawca;
- Grant własny, *Teoretyczne aspekty bezpieczeństwa informacji, komunikacji oraz protokołów kryptograficznych*, KBN NN206 2701 33, Uniwersytet Adama Mickiewicza, główny wykonawca;
- Grant promotorski, *Algorytmy zapewniające anonimowość i ich analiza*, KBN 3T11C 011 26, Politechnika Wrocławska, główny wykonawca;
- Grant własny, *Technologie ochrony danych i komunikacji oparte na technikach kryptograficznych*, KBN 4T11D 005 24, Uniwersytet Adama Mickiewicza, wykonawca;
- Grant własny, *Samoorganizujące się sieci mobilne - podstawowe problemy algorytmiczne*, KBN 3T11C 011 26, Politechnika Wrocławska, główny wykonawca;
- *Algorytmy anonimowej komunikacji*, Roczny grant wewnętrzny Politechniki Wrocławskiej dla doktorantów;

Nagrody

- Stypendium Ministerialne dla Wybitnych Młodych Naukowców (2009-2012);
- Nagroda im. Witolda Lipskiego (2008);
- Stypendium Fundacji na Rzecz Nauki Polskiej na rok 2006 (Po weryfikacji osiągnięć przedłużone na rok 2007);
- Nominacja do międzynarodowej nagrody PET-Award (rok 2004) przyznawanej za osiągnięcia w dziedzinie badań na anonimowością (wspólnie z prof. M.Kutyłowskim oraz M. Gomułkieiczem);
- Nagrody JM Rektora Politechniki Wrocławskiej (2006,2009);
- Nagroda dla najlepszego absolwenta Wydziału PPT Politechniki Wrocławskiej (2003);
- Stypendium habilitacyjne PWr (2009-2010);
- Stypendium w ramach nagrody FNP dla prof. Mirosława Kutyłowskiego (program MISTRZ);
- Best Paper Award na STA 2011;

Inne

Cytowania

Wg. WoS h-index 5 oraz 62 cytowania. (Niestety większość prac nie jest indeksowana.)
Wg. Google Scholar h-index 10, ponad 230 cytowań.

Referaty i konferencje

Uczestniczyłem w ponad 50. konferencjach z zakresu szeroko pojętej informatki - od inżynierii oprogramowania, teorii bezpieczeństwa komputerowego aż po matematyczne podstawy informatyki. Brałem także udział w kilkunastu konferencjach matematycznych. Wygłosiłem ponad dwadzieścia referatów podczas naukowych imprez o zasięgu międzynarodowym. Najważniejsze to:

- *A Note on Invariant Random Variables*, 21-th International Meeting on Probabilistic, Combinatorial and Asymptotic Methods in the Analysis of Algorithms (AofA), Wiedeń, 2010.
- *Energy Efficient Alert in Single-Hop Networks of Extremely Weak Devices*, ALGOSENSORS 2009, Rhodos (Grecja), 2009.

- *Towards Fair Leader Election in Wireless Networks*, Workshop on Reliability and Security in Wireless Networks - konferencja przy DISC 2009, Elche (Hiszpania), 2009.
- *Privacy Protection for RFID's – Hidden Subset Identifiers*, 6-th International Conference on Pervasive Computing – PERVASIVE 2008, Sydney, 2008.
- *Practical Deniable Signatures*, SOFSEM 2008, Nový Smokovec (Słowacja), 2008.
- *Extended Sanitizible Signatures*, International Conference on Information Security and Cryptology 2006, Busan (Korea), 2006.
- *Number and Size of Nodes in Chord Protocol*, Workshop on Optimisation in Complex Networks, Oxford, 2006.
- *Provable Anonymity for Networks of Mixes*, Information Hiding 2005, Barcelona, 2005.
- *DUO–Onions and Hydra–Onions – failure and adversary resistant onion protocols*, Communications and Multimedia Security 2004, Windermere (Wielka Brytania), 2004.
- *Research on anonymity at TU Wrocław*, Privacy Enchancing Technologies 2004, Toronto, 2004.
- *Rapid Mixing and Security of Chaum's Visual Electronic Voting*, European Symposium on Security in Computer Research, Gjovik (Norwegia), 2003.

Osiągnięcia o charakterze organizacyjnym i dydaktycznym zostały opisane w osobnym załączniku.