Protokoły zachowujące prywatność w zawodnych systemach rozproszonych

Autoreferat

Krzysztof Grining

1 Tematyka rozprawy

Przedstawiona rozprawa dotyczy wybranych problemów agregacji danych z zachowaniem prywatności. W ostatnich latach tematyka ta cieszy się dużym zainteresowaniem. Dane stają się coraz tańsze do pozyskania, przechowywania i analizy. Zarówno pojemność dysków jak i moc obliczeniowa rośnie z dużą prędkością. Pomimo, że jest to bardzo pozytywne zjawisko zarówno dla statystyków jak i różnych zastosowań opartych na danych, powoduje jednak pewne zagrożenia i koszty. Niebezpieczeństwo utraty prywatności staje się coraz poważniejsze. Co gorsza, duża ilość danych z różnych, często pozornie niepowiązanych ze sobą, źródeł sprawia, że przypadki naruszenia prywatności mogą być coraz groźniejsze ([11, 12]). W trakcie projektowania protokołów czy algorytmów należy zadbać o to, by zebrane i wykorzystywane dane nie dawały żadnej informacji o konkretnym uczestniku, jednak były przydatne statystycznie do wnioskowań na temat całej populacji.

Rozważamy następujący problem. Istnieje zbiór *użytkowników* (będziemy ich również nazywać *węzłami*). Każdy z użytkowników posiada swoje dane, dla uproszczenia możemy o nich myśleć jak o wartościach liczbowych lub nawet bitowych (0 lub 1). Jest to równoważne bazie danych z n rekordami, z których każdy odpowiada jednemu użytkownikowi. Istnieje również uczestnik protokołu, zwany *agregatorem*, który na podstawie zebranych danych oblicza pewne ogólne statystyki (na przykład średnią czy medianę). Celem jest ujawnienie zebranych statystyk przy jednoczesnym zachowaniu *prywatności* poszczególnych uczestników. W ostatnich latach pojawiło się wiele obiecujących wyników, zarówno w przypadku, gdy danymi zarządza zaufany agregator, jak i w przypadku, gdy dane są rozproszone, a uczestnicy protokołu nie ufają agregatorowi zbierającemu dane. Z perspektywy zachowania prywatności, naszym celem jest ujawnić zebrane statystyki i utrzymać w sekrecie dane każdego z uczestników.

Pierwszym nietrywialnym wyzwaniem było formalne zdefiniowanie prywatności. Od kilku lat standardem jest koncepcja *prywatności różnicowej* (*differential privacy*). W odróżnieniu od poprzednich definicji anonimowości i prywatności, które okazały się wadliwe, jest to definicja oparta na formalizmie matematycznym.

W rozprawie skupiamy się na aspektach prywatności występujących w rozproszonych systemach z zawodnymi węzłami, ze względu na praktyczną wartość takich systemów oraz ich rosnącą liczbę (sieci mobilne, systemy IoT, autonomiczne pojazdy). Z praktycznego punktu widzenia musimy zakładać zawodność węzłów w sieci, zarówno z przyczyn losowych, jak i z powodu ataku adwersarza. Jest to ważna kwestia ze względu na to, że większość używanych aktualnie protokołów agregacji danych z zachowaniem prywatności w systemach rozproszonych opiera się o protokoły kryptograficzne, które często wymagają uczestnictwa wszystkich węzłów, by poprawnie zdeszyfrować wynik. Aby zwiększyć prywatność w takich systemach proponujemy różne podejścia do problemu, zarówno poprzez nowe protokoły, jak również przez nieco zmodyfikowany, choć nadal realistyczny w praktycznych zastosowaniach, model.

Poza modelem rozproszonym z zawodnymi węzłami, zakładamy również, że agregator nie jest zaufany. Zakładamy, że wykonuje protokoły poprawnie, ale jego celem jest wydobycie

dodatkowych informacji dotyczących poszczególnych użytkowników oprócz ostatecznych statystyk. Innymi słowy agregator jest również adwersarzem w rozumieniu zachowania prywatności. Celem jest to, by agregator mógł poznać tylko końcowy rezultat protokołu zachowującego prywatność, ale bez żadnych pośrednich wyników (na przykład częściowych sum danych). Zauważmy, że tak silny model jest w praktyce najbardziej realistycznym w kontekście agregacji danych - zakładamy że użytkownik nie ufa firmie czy instytucji zbierającej dane i nie chce, by była ona w stanie naruszyć jego prywatność. Więcej informacji wstępnych znajduje się w **rozdziale pierwszym** rozprawy.

2 Metody agregacji danych z zachowaniem prywatności w zawodnych systemach rozproszonych z niezaufanym agregatorem

W **rozdziale drugim** proponujemy protokół agregacji danych zachowujący prywatność w zawodnych systemach rozproszonych z niezaufanym agregatorem, przy wykorzystaniu ograniczonej, lokalnej komunikacji pomiędzy węzłami. Ponadto analizujemy *Binary Protocol*, zaprezentowany w pracy [5] przez Chana et al. Ten protokół był uważany za najlepsze rozwiązanie problemu agregacji danych z zachowaniem prywatności w zawodnych systemach rozproszonych. Przy n użytkownikach i danych bitowych (tylko 0 lub 1) błąd protokołu wynosi $\tilde{O}\left((\log n)^{\frac{3}{2}}\right)$, co wydaje się bardzo dobrym wynikiem. Niestety, pomimo gwarancji asymptotycznych, pokazujemy, że w praktycznych zastosowaniach błąd w tym protokole pozostaje nieakceptowalnie wysoki, nawet dla niewielkiej liczby zawodnych węzłów.

Następnie pokazujemy, że zaproponowany przez nas protokół zapewnia dowodliwy poziom prywatności, pomimo dużej liczby zawodnych węzłów. Co więcej, wymaga mniejszej mocy obliczeniowej i oferuje lepsze gwarancje prywatności, co sprawia, że jest bardziej użyteczny w systemach z ograniczonymi zasobami (na przykład sieci sensorów). Co najważniejsze, nasz protokół ma znacznie lepszą dokładność, ponieważ wprowadzone szumy są znacząco mniejsze w porównaniu do *Binary Protocol*. Jeżeli mamy zagwarantowaną przynajmniej połowę działających poprawnie węzłów, oczekiwany błąd nie przekracza $2\sqrt{\log(1/\delta)}$, gdzie δ jest ustalonym parametrem prywatności. Aby osiągnąć te wyniki, musieliśmy nieco osłabić model, a mianowicie dopuścić ograniczoną komunikację pomiędzy węzłami. Nasze rozwiązanie jest ogólną metodą zwiększenia prywatności węzłów w sieciach, które dopuszczają ograniczoną komunikację. Rozdział drugi jest oparty na dwóch publikacjach autora tej rozprawy.

- "*Practical Fault-Tolerant Data Aggregation*", praca wspólna z Markiem Klonowskim i Piotrem Sygą. Opublikowana w Proceedings of International Conference on Applied Cryptography and Network Security (ACNS 2016) [9].
  Ta praca jest poświęcona protokołom agregującym dane z zachowaniem prywatności w zawodnych systemach rozproszonych. Analizujemy *Binary Protocol* zaprezentowany przez Chana et al. w [5]. Proponujemy nieco osłabiony model i precyzyjny protokół agregacji danych PAALC, który zapewnia dowodliwy poziom prywatności nawet z dużą liczbą zawodnych węzłów. Autor tej rozprawy dokonał analizy *Binary Protocol* i był współautorem protokołu PAALC.

- "*On Practical Privacy-Preserving Fault-Tolerant Data Aggregation*", rozszerzenie powyższej publikacji, praca wspólna z Markiem Klonowskim i Piotrem Sygą. Opublikowana w International Journal of Information Security [10].

W tej pracy dokonaliśmy pełnej analizy *Binary Protocol* zaprezentowanego przez Chana et al. w [5]. Pokazujemy analitycznie, że pomimo gwarancji asymptotycznych, wielkość błędu w praktycznych przypadkach jest nieakceptowalnie wysoka. Dokonaliśmy również eksperymentów na istniejących sieciach, by porównać nasz protokół z *Binary Protocol*. Autor tej rozprawy dokonał pełnej analizy błędów *Binary Protocol* oraz wykonał eksperymenty.

3 Zwiększanie prywatności z wykorzystaniem lokalnej wiedzy w zawodnych sieciach

Nasze wyniki z rozdziału drugiego wskazują na zalety posiadania przez sieć lokalnych grup z możliwością komunikacji, w których węzły ufają sobie wzajemnie. Konsekwencją tej obserwacji była próba modyfikacji istniejącej sieci, by miała tę własność. W naturalnie pojawiających się sieciach użytkownicy mają zazwyczaj dość ograniczoną liczbę zaufanych kontaktów. Co więcej, ich wiedza o całej sieci jest głównie lokalna (ograniczona do węzłów będących sąsiadami). Rozważamy rozproszoną sieć składającą się z węzłów, których celem jest zbudowanie dużej, połączonej grupy w sposób efektywny i bez wiedzy o topologii całej sieci. Aby pozostać w realistycznym modelu używanym w tej rozprawie, będziemy zakładać, że węzły mogą być zawodne zarówno z przyczyn losowych, jak również w wyniku działań adwersarza. Może to prowadzić do stanu, w której sieć nie jest połączona, a niektóre węzły, lub grupy węzłów, są odizolowane. Taka sytuacja wpływa negatywnie na protokół opisany przez nas w poprzednim rozdziale.

W związku z tym, w **rozdziale trzecim** proponujemy i rozważamy **lokalne** strategie tworzenia dużych grup użytkowników oparte na lokalnych relacjach zaufania z małym narzutem komunikacyjnym i obliczeniowym. Strategie te są efektywne nawet w przypadku silnego adwersarza mogącego kontrolować **większość** użytkowników. Jest to nietrywialna własność w prawdziwych sieciach. Są one bowiem modelowane z wykorzystaniem grafów *preferential attachment*, które są wrażliwe na utratę głównych węzłów. Analitycznie pokazujemy, że wykorzystując nasze protokoły możemy uzyskać podobną odporność, jak w przypadku grafów $G(n, p)$, które z kolei są odporne na ataki skierowane w konkretne węzły.

Przeprowadziliśmy dokładne testy naszych protokołów na zbiorach danych odpowiadających prawdziwym sieciom. Ponadto, udowadniamy pewne własności takich sieci, przy założeniu, że są one wygenerowane jako proces *preferential attachment*. Istnieją liczne publikacje wskazujące, że złożone, realistyczne sieci przejawiają strukturę, którą można modelować grafami *preferential attachment* (między innymi [1, 2]).

Co więcej, oprócz kwestii prywatności, nasze wyniki mogą być uznane jako pewne fundamentalne obserwacje dotyczące prawdziwych sieci. Dzięki naszym rezultatom można, wykorzystując tylko lokalną wiedzę o sieci, zebrać dużą grupę użytkowników, nawet w wysoce dynamicznym scenariuszu z adwersarzem. Z matematycznego punktu widzenia nasz wkład dotyczy problemu konstruowania strategii zwiększających spójność grafu poprzez dodawanie (w sposób lokalny i niezależny) pewnej liczby dodatkowych krawędzi.

Rozdział trzeci jest oparty na dwóch publikacjach autora tej rozprawy.

- "*How to Cooperate Locally to Improve Global Privacy in Social Networks? On Amplification of Privacy Preserving Data Aggregation*", praca wspólna z Markiem Klonowskim i Małgorzatą Sulkowską. Opublikowana w Proceedings of TrustCom 2017, 16th IEEE International Conference On Trust, Security And Privacy In Computing And Communications [7].

W tej pracy zaproponowaliśmy dwa protokoły, dzięki którym możemy efektywnie konstruować duże grupy użytkowników opierając się tylko na lokalnej znajomości sieci i lokalnych relacjach zaufania. Pokazujemy, że te protokoły wymagają niewielkiego narzutu komunikacyjnego. Przedstawiamy sieć jako graf i wykorzystujemy tak zwany model *preferential attachment*, który pojawia się naturalnie w prawdziwych sieciach. Ponadto, przeprowadzamy eksperymenty na prawdziwych sieciach. Obydwa protokoły oraz eksperymenty wykonał autor tej rozprawy.

- "*Stronger Trust and Privacy in Social Networks via Local Cooperation*", kontynuacja powyższej publikacji, praca wspólna z Markiem Klonowskim i Małgorzatą Sulkowską. Opublikowana w Journal of Complex Networks [8].
  W tej pracy proponujemy kolejny lokalny protokół konstruowania dużych grup użytkowników oraz podejście oparte na łączeniu pozostałych protokołów. Ponadto przeprowadzamy szersze eksperymenty i formalną analizę problemu. Zarówno protokół jak i eksperymenty wykonał autor tej rozprawy.

4 Rozszerzenie *Noiseless Privacy*

W poprzednich rozdziałach zaproponowaliśmy protokoły pozwalające na agregację danych w systemach rozproszonych z zachowaniem prywatności uczestników, pomimo niezaufanego agregatora. Tym niemniej, nie zawsze możemy zapewnić komunikację pomiędzy węzłami, czy wzmocnić spójność sieci. Z drugiej strony, pokazaliśmy, że rozwiązania nie korzystające z tych metod mają często małą dokładność w praktycznych zastosowaniach, szczególnie gdy sieć jest dynamiczna, czyli znaczna część węzłów zawodzi. W **rozdziale czwartym** nieco zmieniliśmy podejście i skupiliśmy się na samej definicji prywatności. Standardowa prywatność różnicowa niesie ze sobą konieczność randomizacji wyników (na przykład poprzez dodawanie szumów), co może powodować znaczące błędy w końcowej, zagregowanej statystyce.

W części czwartej rozważamy osłabienie modelu prywatności różnicowej, nazywane *noiseless privacy* (prywatność bez szumów), które było już wcześniej zaprezentowane w [4]. Intuicja stojąca za *noiseless privacy* jest taka, że w praktycznych zastosowaniach zakładanie, że adwersarz zna niemal każdy rekord bazy danych wydaje się zbyt pesymistyczne. Pojawiło się kilka publikacji dotyczących tej tematyki, do najważniejszych z nich należą [3, 4], gdzie proponowane są osłabienia modelu prywatności różnicowej. W osłabionych modelach wykorzystywana jest losowość w danych, która może pochodzić zarówno od samych danych, jak również modelować niepewność adwersarza.

Niestety, poprzednie wyniki były głównie asymptotyczne, a co za tym idzie, trudne do zastosowania w praktyce. Dokonaliśmy szczegółowej, nieasymptotycznej analizy osłabionego modelu, by otrzymać **jawne oszacowania** parametrów prywatności. Co więcej, nasze oszacowania okazały się dokładniejsze niż te z pracy [4]. W przeciwieństwie do poprzedników, którzy skupiali się na danych niezależnych i konkretnych rozkładach, my oszacowaliśmy parametry prywatności dla **dowolnych** rozkładów i szerokiej klasy zależności. Ponadto przedstawiamy model *noiseless privacy* w inny sposób, który jest prostszy i wygodniejszy do analizy.

Następnie skupiliśmy się na rozszerzaniu rozkładów danych mających odpowiednie własności prywatności oraz na wprowadzaniu zależności w danych i łączeniu *noiseless privacy* ze standardowym podejściem prywatności różnicowej. Ważne są dla nas praktyczne zastosowania, więc nasze wyniki są przedstawione w taki sposób, aby można było je łatwo zaaplikować do realistycznych scenariuszy agregacji danych. Wykorzystujemy również model *noiseless privacy*, a szczególnie dokładne wyniki jakie otrzymaliśmy, by pozbyć się, lub przynajmniej zmniejszyć,

niezbędny szum dodawany w trakcie agregacji danych zachowującej prywatność. Według naszej wiedzy, koncepcja łączenia standardowych technik prywatności różnicowej z niepewnością adwersarza nie były wcześniej rozważane w literaturze. Intuicyjnie możemy o tym myśleć w ten sposób, że w przypadku, gdy z punktu widzenia adwersarza dane są wystarczająco losowe, powinniśmy być w stanie dodawać mniej szumu niż w przypadku, gdy dane są, z punktu widzenia adwersarza, deterministyczne. Co za tym idzie, otrzymujemy większą dokładność protokołów. Pokazujemy oszacowania na parametry prywatności, które pozwalają nam badać synergię między prywatnością różnicową, a *noiseless privacy*. Wyniki w tej części są oparte na publikacji autora tej rozprawy.

- "Towards Extending Noiseless Privacy: Dependent Data and More Practical Approach", praca wspólna z Markiem Klonowskim. Opublikowana w Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2017) [6].
  W tej pracy wykorzystujemy istniejące osłabienie modelu prywatności różnicowej i rozwijamy je. Przedstawiamy precyzyjne wyniki dla niezależnych danych (dotychczas znane były głównie wyniki asymptotyczne) oraz dla danych z zależnościami, które nie były wcześniej rozważane w tym modelu. Ponadto pokazujemy, jak łączyć standardową prywatność różnicową z *noiseless privacy* by otrzymać lepsze wyniki. Autor tej rozprawy dokonał formalnej analizy zarówno przypadku niezależnych jak i zależnych danych oraz zaproponował metodę łączenia *noiseless privacy* z prywatnością różnicową.

Literatura

[1] Réka Albert and Albert-László Barabási, *Statistical mechanics of complex networks*, Reviews of Modern Physics **74** (2002), no. 1, pp. 47–101.

[2] Albert-László Barabási and Eric Bonabeau, *Scale-free networks*, Scientific American **288** (2003), no. 5, pp. 50–59.

[3] Raef Bassily, Adam Groce, Jonathan Katz, and Adam Smith, *Coupled-worlds privacy: Exploiting adversarial uncertainty in statistical data privacy*, IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS), 2013, pp. 439–448.

[4] Raghav Bhaskar, Abhishek Bhowmick, Vipul Goyal, Srivatsan Laxman, and Abhradeep Thakurta, *Noiseless database privacy*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2011, pp. 215–232.

[5] T.-H. Hubert Chan, Elaine Shi, and Dawn Song, *Privacy-preserving stream aggregation with fault tolerance.*, Financial Cryptography, Lecture Notes in Computer Science, vol. 7397, Springer, 2012, pp. 200–214.

[6] Krzysztof Grining and Marek Klonowski, *Towards extending noiseless privacy: Dependent data and more practical approach*, Proceedings of the 12th ACM on Asia Conference on Computer and Communications Security (AsiaCCS), 2017, pp. 546–560.

[7] Krzysztof Grining, Marek Klonowski, and Małgorzata Sulkowska, *How to cooperate locally to improve global privacy in social networks? On amplification of privacy preserving data aggregation*, Proceedings of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2017, pp. 464–471.

[8] Krzysztof Grining, Marek Klonowski, and Małgorzata Sulkowska, *Stronger trust and privacy in social networks via local cooperation*, Journal of Complex Networks (2019).

[9] Krzysztof Grining, Marek Klonowski, and Piotr Syga, *Practical fault-tolerant data aggregation*, International Conference on Applied Cryptography and Network Security (ACNS), Springer, 2016, pp. 386–404.

[10] Krzysztof Grining, Marek Klonowski, and Piotr Syga, *On practical privacy preserving fault tolerant data aggregation*, International Journal of Information Security **18** (2019), no. 3, pp. 285–304.

[11] Arvind Narayanan and Vitaly Shmatikov, *Robust de-anonymization of large sparse datasets*, 29th IEEE Symposium on Security and Privacy, 2008, pp. 111–125.

[12] Arvind Narayanan and Vitaly Shmatikov, *De-anonymizing social networks*, arXiv preprint arXiv:0903.3276 (2009).