

شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی سازگارپذیر پیشرفته

محمدعلی خواجه‌نیا

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکده علوم مهندسی / دانشگاه تهران

۲۷ اردیبهشت ۱۴۰۴



فهرست

- ۱ تعریف مسئله
- ۲ اهداف
- ۳ ضرورت انجام پژوهش
- ۴ پرسش های پژوهش
- ۵ روش و فنون پژوهش
 - بخش تئوری
 - بخش پیاده سازی
- ۶ زمانبندی پیشنهادی
- ۷ پیشینه پژوهش
- ۸ منابع و مراجع

۱ تعریف مسئله

۴ پرسش های پژوهش

۲ اهداف

۵ روش و فنون پژوهش

۳ ضرورت انجام پژوهش

۶ زمانبندی پیشنهادی

۷ پیشینه پژوهش

۸ منابع و مراجع

قسمت ۱

تعریف مسئله

تعریف مسئله

الگوریتم های کوانتومی سازگارپذیر^۱ که از ترکیب پردازش کلاسیک و کوانتومی استفاده می کنند، گزینه ای مناسب برای رایانه های کوانتومی اندازه میانی پراختلال^۲ هستند. این پژوهش کارایی الگوریتم های کوانتومی سازگارپذیر را در شکستن رمزنگاری یکسان کلید^۳ و بهینه سازی این حمله ها بررسی می کند.

¹Variational Quantum Algorithms

²Noisy Intermediate Scale Quantum Device

³Symmetric-Key Cryptography

قسمت ۲

اهداف

اهداف پژوهش

اهداف اصلی این پروژه به شرح زیر هستند:

اهداف پژوهش

جدول ۱: حالت های معروف برای مدل مارکوف

حالت ها	زمان پیوسته	زمان گسسته
وضعیت گسسته	فرایند مارکوف	زنجیره مارکوف
وضعیت پیوسته	فرایند مارکوف وضعیت پیوسته	زنجیره مارکوف وضعیت پیوسته

قسمت ۳

ضرورت انجام پژوهش

ضرورت انجام پژوهش

دسته بندی کارهای پیشین در زمینه شبکه های اجتماعی و انتشار بیماری یا ویروس:

- ۱ انتشار بیماری
- ۲ ساختار عمومی انتشار بیماری
- ۳ تأثیر گذاری اجتماعی و نفوذ فکری
- ۴ تغییرات آگاهی و رفتار اجتماعی
- ۵ گراف پویا و تغییرات یال و گره
- ۶ تعادل و پایداری گراف
- ۷ کنترل شبکه و تغییر سیاست
- ۸ پیش بینی انتشار بیماری
- ۹ انتشار ویروس و بد افزار رایانه ای

ضرورت انجام پژوهش

دسته بندی کارهای پیشین در زمینه شبکه های اجتماعی و انتشار بیماری یا ویروس:

- ۱ انتشار بیماری
- ۲ ساختار عمومی انتشار بیماری
- ۳ تأثیر گذاری اجتماعی و نفوذ فکری
- ۴ تغییرات آگاهی و رفتار اجتماعی
- ۵ گراف پویا و تغییرات یال و گره
- ۶ تعادل و پایداری گراف
- ۷ کنترل شبکه و تغییر سیاست
- ۸ پیش بینی انتشار بیماری
- ۹ انتشار ویروس و بد افزار رایانه ای

- ◀ بررسی مدل آشکار و نهان بر میزان شیوع جامعه [۱]
- ◀ بررسی مدل SEIR برای بیماری کووید-۱۹ با توجه به ارتباطهای بین شهری و بین کشوری در اروپا [۳، ۲]
- ◀ بررسی نویز (خطا در اطلاعات ورودی) و تأثیر آن بر نتیجه تحلیل مدل SIS [۴]
- ◀ در نظر گرفتن واکسیناسیون در مدل SIS [۵]
- ◀ تطبیق اطلاعات بیماری کووید-۱۹ در کشور فرانسه بر روی مدل SEIR [۶]

ساختار عمومی انتشار بیماری

- ◀ ساختار عمومی انتشار بیماری برای مدل های رایج (مثل SIS, SAIS) [۷]
- ◀ بررسی ساختارهای متداول بیماری بر روی شبکه های چند لایه [۸]

تأثیر گذاری اجتماعی و نفوذ فکری

- ▶ تحلیل انتشار شایعه در شبکه‌های اجتماعی برخط با در نظر گرفتن مدل نظریه بازی [۹]
- ▶ ارائه یک مدل شبیه‌سازی برای بررسی شرایط و نتیجه رسیدن به اجماع در یک شبکه برخط با دو گروه فکری مخالف با در نظر گرفتن کیفیت ارتباطات [۱۰، ۱۱]
- ▶ بررسی تأثیر اخبار انتشار بیماری کووید-۱۹ در شبکه‌های اجتماعی برخط [۱۲]

تغییرات آگاهی و رفتار اجتماعی

- بررسی مدل بیماری SEIV⁴ برای یک شبکه و تأثیر هوشیاری افراد بر تعداد ارتباط های فعال با دیگران و زمان رسیدن به حالت پایدار بدون بیماری [۱۳، ۱۴]
- تأثیر آگاهی و میزان شیوع بیماری در ارتباط بین افراد در یک شبکه دو لایه (یک لایه ثابت و یک لایه متغیر) [۱۵]

⁴Susceptible-Exposed-Infected-Vigilant

قسمت ۴

پرسش های پژوهش

فرایند کلی حل مسئله

شبیه سازی:

- ۱ تصادفی (محاسبه وضعیت و شرایط جدید هر گره و به روز کردن همه گره ها در یک لحظه)
- ۲ آماری (محاسبه امید ریاضی و میانگین وضعیت و شرایط انتقال برای کل شبکه در مدل مارکوف)

مدل سازی:

- ۱ تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
- ۲ تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی های مسئله)
- ۳ تعریف روابط ریاضی تجمیع سازی برای هر گره
- ۴ تعریف مدل مارکوف معادل
- ۵ تعریف روابط آماری و کلی (مبتنی بر نظریه میدان متوسط)
- ۶ تعریف الگوی بیماری
- ۷ شبیه سازی

فرایند کلی حل مسئله

شبیه سازی:

- ۱ تصادفی (محاسبه وضعیت و شرایط جدید هر گره و به روز کردن همه گره ها در یک لحظه)
- ۲ آماری (محاسبه امید ریاضی و میانگین وضعیت و شرایط انتقال برای کل شبکه در مدل مارکوف)

مدل سازی:

- ۱ تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
- ۲ تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی های مسئله)
- ۳ تعریف روابط ریاضی تجمیع سازی برای هر گره
- ۴ تعریف مدل مارکوف معادل
- ۵ تعریف روابط آماری و کلی (مبتنی بر نظریه میدان متوسط)

۶ تعریف الگوی بیماری

۷ شبیه سازی

قسمت ۵

روش و فنون پژوهش

قسمت ۶

زمانبندی پیشنهادی

قسمت ۷

پیشینه پژوهش

قسمت ۸

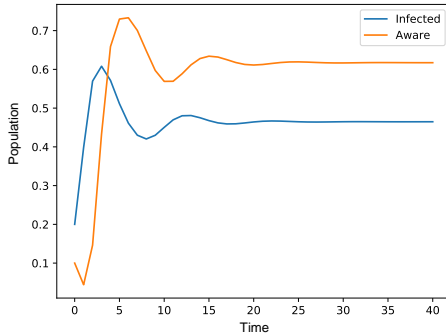
منابع و مراجع

- [1] Chen, Yi-Cheng, Lu, Ping-En, Chang, Cheng-Shang, and Liu, Tzu-Hsuan.
A time-dependent sir model for covid-19 with undetectable infected persons.
IEEE Transactions on Network Science and Engineering, 7(4):3279–3294, 2020.
- [2] Wang, Wei, Liu, Quan-Hui, Liang, Junhao, Hu, Yanqing, and Zhou, Tao.
Coevolution spreading in complex networks.
Physics Reports, 820:1–51, 2019.
- [3] Estrada, Ernesto.
Covid-19 and sars-cov-2. modeling the present, looking at the future.
Physics Reports, 2020.
- [4] Vizuete, Renato, Frasca, Paolo, and Garin, Federica.
Graphon-based sensitivity analysis of sis epidemics.
IEEE Control Systems Letters, 4(3):542–547, 2020.
- [5] Khanjanianpak, Mozhgan, Azimi-Tafreshi, Nahid, and Castellano, Claudio.
Competition between vaccination and disease spreading.
Physical Review E, 101(6):062306, 2020.
- [6] Efimov, Denis and Ushirobira, Rosane.
On interval prediction of covid-19 development in france based on a seir epidemic model.
in *2020 59th IEEE Conference on Decision and Control (CDC)*, pp. 3883–3888. IEEE, 2020.

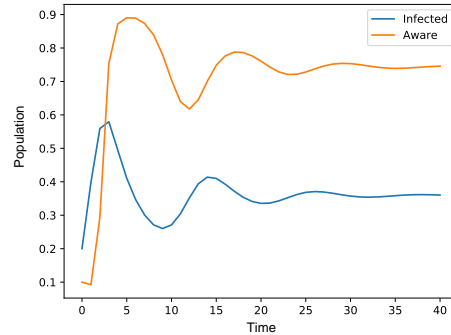
- [7] Moon, Sifat Afroj, Sahneh, Faryad Darabi, and Scoglio, Caterina.
Group-based general epidemic modeling for spreading processes on networks: Groupgem.
IEEE Transactions on Network Science and Engineering, pp. 1–1, 2020.
- [8] Abhishek, Vishal and Srivastava, Vaibhav.
Sis epidemic model under mobility on multi-layer networks.
in *2020 American Control Conference (ACC)*, pp. 3743–3748. IEEE, 2020.
- [9] Huang, D. W., Yang, L. X., Li, P., Yang, X., and Tang, Y. Y.
Developing cost-effective rumor-refuting strategy through game-theoretic approach.
IEEE Systems Journal, pp. 1–12, 2020.
- [10] Bolzern, P., Colaneri, P., and De Nicolao, G.
Opinion dynamics in social networks: The effect of centralized interaction tuning on emerging behaviors.
IEEE Transactions on Computational Social Systems, 7(2):362–372, 2020.
- [11] Nettasinghe, Buddhika, Krishnamurthy, Vikram, and Lerman, Kristina.
Diffusion in social networks: Effects of monophilic contagion, friendship paradox, and reactive networks.
IEEE Transactions on Network Science and Engineering, 7(3):1121–1132, 2019.
- [12] Cinelli, Matteo, Quattrociocchi, Walter, Galeazzi, Alessandro, Valensise, Carlo Michele, Brugnoli, Emanuele, Schmidt, Ana Lucia, Zola, Paola, Zollo, Fabiana, and Scala, Antonio.
The covid-19 social media infodemic.
Scientific Reports, 10(1):1–10, 2020.

- [13] Li, Zhixun, Hong, Jie, Kim, Jonghyuk, and Yu, Changbin.
Control design and analysis of an epidemic seiv model upon adaptive network.
in *2019 18th European Control Conference (ECC)*, pp. 2492–2497. IEEE, 2019.
- [14] Bhowmick, Sourav and Panja, Surajit.
Influence of opinion dynamics to inhibit epidemic spreading over multiplex network.
IEEE Control Systems Letters, 5(4):1327–1332, 2020.
- [15] Sahneh, F. D., Vajdi, A., Melander, J., and Scoglio, C. M.
Contact adaption during epidemics: A multilayer network formulation approach.
IEEE Transactions on Network Science and Engineering, 6(1):16–30, 2019.

نتیاج شبیه سازی آماری



(ب) یادگیری = ۰.۵ و فراموشی = ۰.۷۵



(آ) یادگیری = ۰.۷۵ و فراموشی = ۰.۵

شکل ۱: نتیجه اجرای شبیه سازی آماری در دو حالت