شکستن پروتکل‌های رمزنگاری با استفاده از حملات کوانتومی متغیر پیشرفته

دفاع پروپوزال

محمدعلی خواجه‌ئیان

استاد راهنما: زهرا شاطرزاده‌یزدی
دانشکدهٔ علوم مهندسی / دانشگاه تهران

۲۷ اردیبهشت ۱۴۰۴

فهرست

1. تعریف مسئله
2. اهداف
   - زنجیرهٔ مارکوف
   - نظریهٔ میدان متوسط
   - مدل‌های انتشار بیماری
   - منطق فازی
3. ضرورت انجام پژوهش
4. پرسش های پژوهش
5. روش و فنون پژوهش
   - بخش تئوری
   - بخش پیاده سازی
6. زمانبدی پیشنهادی
7. پیشینه پژوهش
8. منابع و مراجع
9. صفحات پشتیبان

فهرست

۱ تعریف مسئله
۲ اهداف
۳ ضرورت انجام پژوهش
۴ پرسش های پژوهش
۵ روش و فنون پژوهش
۶ زمانبدی پیشنهادی
۷ پیشینه پژوهش
۸ منابع و مراجع
۹ صفحات پشتیبان

قسمت ۱

تعریف مسئله

- نمونه از یک لیست دولایه در کنار یک تصویر
  - در این لیست موارد زیادی می‌تواند قرار بگیرد
  - مثلاً
  - ...
- این مورد برای یک ترکیب دولایه ای آماده شده
  - این مورد فقط در قسمت اول دیده می‌شود
  - این مورد تأکیدی در صفحهٔ دوم دیده می‌شود
  - موارد بیشتر

شکل ۱: اولین تصویر

- نمونه از یک لیست دولایه در کنار یک تصویر
  - در این لیست موارد زیادی می‌تواند قرار بگیرد
  - مثلاً
  - ...

- این مورد برای یک ترکیب دولایه ای آماده شده
  - این مورد فقط در قسمت اول دیده می‌شود
  - **این مورد تأکیدی در صفحهٔ دوم دیده می‌شود**
  - موارد بیشتر

شکل ۱: اولین تصویر

قسمت ۲

اهداف

زنجیرهٔ مارکوف

زنجیرهٔ مارکوف[1]

- مدلی برای توصیف توالی رخدادهای احتمالی (**فرایند تصادفی**[2])
- احتمال هر رخداد فقط به وضعیت رخداد قبلی خود وابسته (**بدون حافظه**[3])
- قابل تعریف در دو حالت: زمان گسسته و زمان پیوسته

[1] Markov Chain
[2] Stochastic process
[3] Memory less

زنجیرهٔ مارکوف

زنجیرهٔ مارکوف[1]

- مدلی برای توصیف توالی رخدادهای احتمالی (**فرایند تصادفی**[2])
- احتمال هر رخداد فقط به وضعیت رخداد قبلی خود وابسته (**بدون حافظه**[3])
- قابل تعریف در دو حالت: زمان گسسته و زمان پیوسته

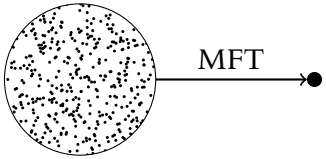
جدول ۱: حالت‌های معروف برای مدل مارکوف

حالت‌ها	زمان پیوسته	زمان گسسته
وضعیت گسسته	فرایند مارکوف	زنجیره مارکوف
وضعیت پیوسته	فرایند مارکوف وضعیت پیوسته	زنجیره مارکوف وضعیت پیوسته

[1] Markov Chain
[2] Stochastic process
[3] Memory less

نظریهٔ میدان متوسط (MFT[4])

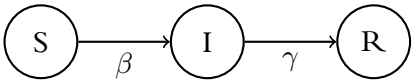
- رفتار مدل‌های بزرگ و پیچیدهٔ تصادفی را به کمک یک مدل ساده‌تر
  - تبدیل یک مسئله با تعداد بسیار زیادی از اجزای کوچک که با یکدیگر در ارتباط هستند و رفتار تصادفی دارند
  - به یک مسئله سادهٔ تک ذره‌ای
  - تحلیل رفتار میانگین کل ذرات را مدل می‌کند
- تبدیل و تحلیل یک مسئلهٔ بین ذره‌ای برای تعداد بی‌شمار ذره به یک روش تک ذره‌ای



شکل ۲: تبدیل مسئله بسیار ذره‌ای به تک ذره‌ای برای تحلیل رفتار کل ذرات در کنار هم به کمک نظریهٔ میدان متوسط

[4] Mean Field Theory

مدل اولیهٔ مستعد_بیمار_ایمن (SIR)



شکل ۳: مدل مارکوف انتشار بیماری SIR

- مدل SIR در سال ۱۹۲۷ میلادی، توسط آقای کِرماک[۵] و آقای مَک‌کِندریک[۶]
  - سالم (در معرض ابتلا) در قالب $S(t)$
  - مبتلا در قالب $I(t)$
  - بهبود یافته (یا ایمن) در قالب $R(t)$

$$\begin{aligned} \frac{dS}{dt} &= -\frac{\beta SI}{N} \\ \frac{dI}{dt} &= \frac{\beta SI}{N} - \gamma I \\ \frac{dR}{dt} &= \gamma I \end{aligned} \qquad (۱)$$

[۵] Kermack O. W.
[۶] McKendrick G. A.

مدل‌های معروف دیگر

- SIS: بازگشت به حالت مستعد پس از بیماری
- SIRS: بازگشت به دورهٔ مستعد پس از یک دورهٔ مشخص
- SEIS: وجود یک دورهٔ نهان و بدون علامت پس از ابتلا و قبل از بروز عفونت
- MSIR: در نظر گرفتن وضعیت مصونیت کودکان در مقابل بیماری
- SAIS: در نظر گرفتن وضعیت آگاه برای کاهش نرخ ابتلا
- SIRC: با وضعیت ناقل[۷]
- SIRV: با وضعیت هوشیاری[۸]

[7] Carrier
[8] Vigilant

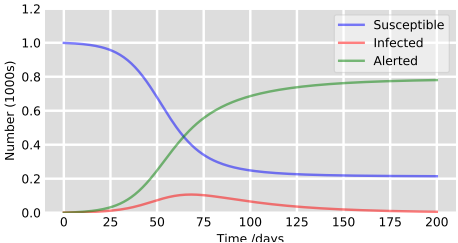
مدل‌های معروف دیگر

- SIS: بازگشت به حالت مستعد پس از بیماری
- SIRS: بازگشت به دورهٔ مستعد پس از یک دورهٔ مشخص
- SEIS: وجود یک دورهٔ نهان و بدون علامت پس از ابتلا و قبل از بروز عفونت
- MSIR: در نظر گرفتن وضعیت مصونیت کودکان در مقابل بیماری
- SAIS: در نظر گرفتن وضعیت آگاه برای کاهش نرخ ابتلا
- SIRC: با وضعیت ناقل[۷]
- SIRV: با وضعیت هوشیاری[۸]

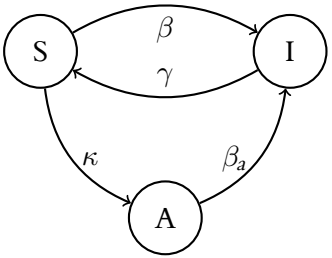
[7] Carrier
[8] Vigilant

مدل مستعد_آگاه_بیمار_مستعد (SAIS)

- کاهش نرخ ابتلا از β به β_a برای افراد آگاه و مراقب
- تغییر وضعیت به حالت آگاه و مراقب با نرخ κ



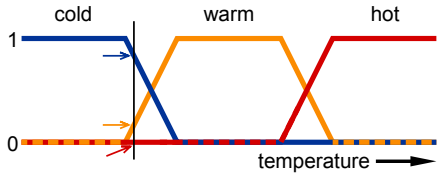
شکل ۴: تغییرات گذرا برای مدل SAIS



شکل ۵: مدل مارکوف انتشار بیماری SAIS

منطق فازی - ۱

- روشی برای مدل کردن ارتباط بین ورودی و خروجی
- تعریف **مجموعهٔ فازی**[۹]
- اعضای مجموعهٔ فازی شامل **متغیرهای زبانی** هستند که مقادیر آن‌ها از **مقادیر زبانی**[۱۰] انتخاب می‌شود.
- تعریف مقدار حدودی بین ۰ تا ۱ برای ورودی و خروجی‌ها (**درجهٔ عضویت**[۱۱])



شکل ۶: تابع عضویت فازی برای دمای محیط

[9] Fuzzy Set
[10] Linguistic values
[11] Membership grade

روش عملکرد منطق فازی

1. تبدیل ورودی‌های عددی به **متغیرهای زبانی**[12] (غیر دقیق و حسی) یا **فازی سازی**
   - بر اساس **تابع عضویت فازی**
2. **استنتاج فازی** مطابق با **قواعد فازی** تعریف شده (بر اساس توصیف زبانی اگر ← آنگاه)
3. تبدیل خروجی فازی به یک متغیر عددی (**فازی گشایی**)
   - بر اساس **تابع عضویت فازی**
   - به کمک روش‌های تجمیع سازی نتایج

[12] Linguistic variable

قسمت ۳

ضرورت انجام پژوهش

کارهای پیشین

دسته بندی کارهای پیشین در زمینهٔ شبکه‌های اجتماعی و انتشار بیماری یا ویروس:

1. انتشار بیماری
2. ساختار عمومی انتشار بیماری
3. تأثیر گذاری اجتماعی و نفوذ فکری
4. تغییرات آگاهی و رفتار اجتماعی
5. گراف پویا و تغییرات یال و گره
6. تعادل و پایداری گراف
7. کنترل شبکه و تغییر سیاست
8. پیش‌بینی انتشار بیماری
9. انتشار ویروس و بد افزارِ رایانه‌ای

کارهای پیشین

دسته بندی کارهای پیشین در زمینهٔ شبکه‌های اجتماعی و انتشار بیماری یا ویروس:

1. انتشار بیماری
2. ساختار عمومی انتشار بیماری
3. تأثیر گذاری اجتماعی و نفوذ فکری
4. تغییرات آگاهی و رفتار اجتماعی
5. گراف پویا و تغییرات یال و گره
6. تعادل و پایداری گراف
7. کنترل شبکه و تغییر سیاست
8. پیش‌بینی انتشار بیماری
9. انتشار ویروس و بد افزارِ رایانه‌ای

انتشار بیماری

- 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 [۲، ۳]
- بررسی نویز (خطا در اطلاعات ورودی) و تأثیر آن بر نتیجهٔ 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 مدل‌های رایج (مثل SIS, SAIS) [۷]
- بررسی ساختارهای متداول بیماری بر روی شبکه‌های چند لایه [۸]

تأثیر گذاری اجتماعی و نفوذ فکری

- تحلیل انتشار شایعه در شبکه‌های اجتماعی برخط با در نظر گرفتن مدل نظریهٔ بازی [۹]
- ارائهٔ یک مدل شبیه‌سازی برای بررسی شرایط و نتیجه رسیدن به اجماع در یک شبکهٔ برخط با دو گروه فکری مخالف با در نظر گرفتن کیفیت ارتباط‌ها [۱۰، ۱۱]
- بررسی تأثیر اخبار انتشار بیماری کووید_۱۹ در شبکه‌های اجتماعی برخط [۱۲]

تغییرات آگاهی و رفتار اجتماعی

- بررسی مدل بیماری SEIV[13] برای یک شبکه و تأثیر هوشیاری افراد بر تعداد ارتباط‌های 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 شبکهٔ دو لایه (یک لایه ثابت و یک لایهٔ متغیر)[۱۵]

[13] Susceptible-Exposed-Infected-Vigilant

قسمت ۴

پرسش های پژوهش

فرایند کلی حل مسئله

شبیه‌سازی:

1. تصادفی (محاسبهٔ وضعیت و شرایط جدید هر گره و به روز کردن همه گره‌ها در یک لحظه)
2. آماری (محاسبهٔ امید ریاضی و میانگین وضعیت و شرایط انتقال برای کل شبکه در مدل مارکوف)

مدل‌سازی:

1. تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
2. تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی‌های مسئله)
3. تعریف روابط ریاضی تجمیع سازی برای هر گره
4. تعریف مدل مارکوف معادل
5. تعریف روابط آماری و کلی (مبتنی بر نظریهٔ میدان متوسط)
6. تعریف الگوی بیماری
7. شبیه‌سازی

فرایند کلی حل مسئله

شبیه‌سازی:

1. تصادفی (محاسبهٔ وضعیت و شرایط جدید هر گره و به روز کردن همه گره‌ها در یک لحظه)
2. آماری (محاسبهٔ امید ریاضی و میانگین وضعیت و شرایط انتقال برای کل شبکه در مدل مارکوف)

مدل‌سازی:

1. تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
2. تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی‌های مسئله)
3. تعریف روابط ریاضی تجمیع سازی برای هر گره
4. تعریف مدل مارکوف معادل
5. تعریف روابط آماری و کلی (مبتنی بر نظریهٔ میدان متوسط)
6. تعریف الگوی بیماری
7. شبیه‌سازی

قسمت ۵

روش و فنون پژوهش

قسمت ۶

زمانبدی 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.

قسمت ۹

صفحات پشتیبان

مثال

این یک مثال است.

تعریف

این یک تعریف است.

قضیه

این یک قضیه است.

اثبات ریاضی

قضیه (Pythagoras)

$a^2 + b^2 = c^2$ یا

$$c^2 = a^2 + b^2$$

اثبات ریاضی

قضیه (Pythagoras)

$a^۲ + b^۲ = c^۲$ یا

$$c^۲ = a^۲ + b^۲$$

اثبات.

$\omega + \phi = \epsilon$ □

اثبات ریاضی

قضیه (Pythagoras)

$a^2 + b^2 = c^2$ یا

$$c^2 = a^2 + b^2$$

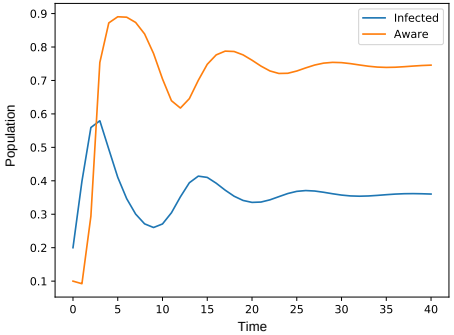
اثبات.

$\omega + \phi = \epsilon$ □

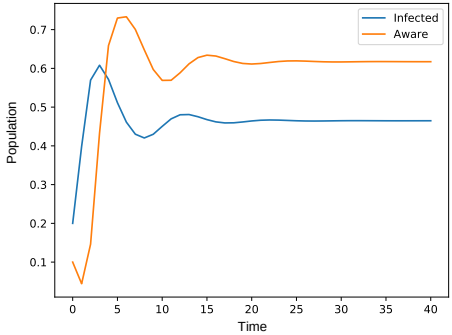
نتیجه

$x + y = y + x$

نتیاج شبیه‌سازی آماری



(آ) یادگیری=۰.۷۵ و فراموشی=۰.۵



(ب) یادگیری=۰.۵ و فراموشی ۰.۷۵

شکل ۷: نتیجهٔ اجرای شبیه‌سازی آماری در دو حالت

Algorithm ۱ الگوریتم اجرای برنامهٔ شبیه‌سازی برای حالت امید ریاضی

ورودی: زمان t_{max} به عنوان زمان لازم برای انجام شبیه‌سازی،
ورودی: توزیع درجهٔ گراف برای شبیه‌سازی،
خروجی: ماتریس تغییرات گراف از لحظهٔ ۰ تا t_{max}.

۱: **برای** t از ۰ **تا** t_{max} **انجام بده**
۲: محاسبهٔ نرخ انتقال بیماری
۳: محاسبهٔ نرخ یادگیری‌ـ فراموشی
۴: محاسبهٔ وضعیت جدید مدل مارکوف بیماری و آگاهی
۵: **پایان حلقهٔ برای**
۶: **بازگردان** ماتریس تغییرات زمانی