

حمله به پروتکل های رمزنگاری توسط الگوریتم های متغیر پیشرفته دفاع پروپوزال

محمدعلی خواجه‌نیا

استاد راهنما زهرا شاطرزاده‌یزدی
دانشکده علوم مهندسی / دانشگاه تهران

۲۶ اردیبهشت ۱۴۰۴



فهرست

- ۱ مقدمه
- ۲ مفاهیم اولیه
 - زنجیره مارکوف
 - نظریه میدان متوسط
 - مدل‌های انتشار بیماری
 - منطق فازی
- ۳ کارهای پیشین
- ۴ حل مسئله
- ۵ منابع و مراجع
- ۶ تشکر از توجه شما
- ۷ صفحات پشتیبان

فهرست

- ۱ مقدمه
- ۲ مفاهیم اولیه
- ۳ کارهای پیشین
- ۴ حل مسئله
- ۵ منابع و مراجع
- ۶ تشکر از توجه شما
- ۷ صفحات پشتیبان

قسمت ۱

مقدمه

◀ این مورد برای یک ترکیب دولایه ای آماده شده

- این مورد فقط در قسمت اول دیده می شود
- این مورد تأکیدی در صفحه دوم دیده می شود
- موارد بیشتر



شکل ۱: اولین تصویر

◀ نمونه از یک لیست دولایه در کنار یک تصویر

- در این لیست موارد زیادی می تواند قرار بگیرد
- مثلاً
- ...

◀ این مورد برای یک ترکیب دولایه ای آماده شده

- این مورد فقط در قسمت اول دیده می شود
- این مورد تأکیدی در صفحه دوم دیده می شود
- موارد بیشتر



شکل ۱: اولین تصویر

◀ نمونه از یک لیست دولایه در کنار یک تصویر

- در این لیست موارد زیادی می تواند قرار بگیرد
- مثلاً
- ...

قسمت ۲

مفاهیم اولیه

زنجیره مارکوف

زنجیره مارکوف^۱

- ▶ مدلی برای توصیف توالی رخدادهای احتمالی (فرایند تصادفی^۲)
- ▶ احتمال هر رخداد فقط به وضعیت رخداد قبلی خود وابسته (بدون حافظه^۳)
- ▶ قابل تعریف در دو حالت: زمان گسسته و زمان پیوسته

¹Markov Chain

²Stochastic process

³Memory less

زنجیره مارکوف

زنجیره مارکوف^۱

- ▶ مدلی برای توصیف توالی رخدادهای احتمالی (فرایند تصادفی^۲)
- ▶ احتمال هر رخداد فقط به وضعیت رخداد قبلی خود وابسته (بدون حافظه^۳)
- ▶ 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

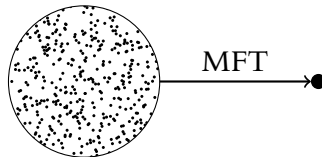
¹Markov Chain

²Stochastic process

³Memory less

نظریه میدان متوسط (MFT)^۴

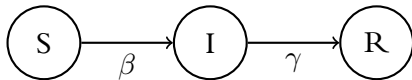
- ◀ رفتار مدل‌های بزرگ و پیچیده تصادفی را به کمک یک مدل ساده‌تر
 - تبدیل یک مسئله با تعداد بسیار زیادی از اجزای کوچک که با یکدیگر در ارتباط هستند و رفتار تصادفی دارند
 - به یک مسئله ساده تک ذره‌ای
 - تحلیل رفتار میانگین کل ذرات را مدل می‌کند
- ◀ تبدیل و تحلیل یک مسئله بین ذره‌ای برای تعداد بی‌شمار ذره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



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

⁴Mean Field Theory

مدل اولیه مستعد-بیمار-ایمن (SIR)



شکل ۳: مدل مارکوف انتشار بیماری SIR

◀ مدل SIR در سال ۱۹۲۷ میلادی، توسط آقای کرماک^۵ و آقای مک‌کندریک^۶

- سالم (در معرض ابتلا) در قالب $S(t)$
- مبتلا در قالب $I(t)$
- بهبود یافته (یا ایمن) در قالب $R(t)$

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

Kermack O. W.^۵
McKendrick G. A.^۶

مدل‌های معروف دیگر

- ◀ SIS: بازگشت به حالت مستعد پس از بیماری
- ◀ SIRS: بازگشت به دوره مستعد پس از یک دوره مشخص
- ◀ SEIS: وجود یک دوره 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

⁷Carrier⁸Vigilant

مدل‌های معروف دیگر

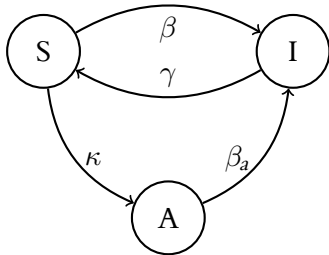
- ◀ SIS: بازگشت به حالت مستعد پس از بیماری
- ◀ SIRS: بازگشت به دوره مستعد پس از یک دوره مشخص
- ◀ SEIS: وجود یک دوره نهان و بدون علامت پس از ابتلا و قبل از بروز عفونت
- ◀ MSIR: در نظر گرفتن وضعیت مصونیت کودکان در مقابل بیماری
- ◀ SAIS: در نظر گرفتن وضعیت آگاه برای کاهش نرخ ابتلا
- ◀ SIRC: با وضعیت ناقل^۷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

⁷ Carrier⁸ Vigilant

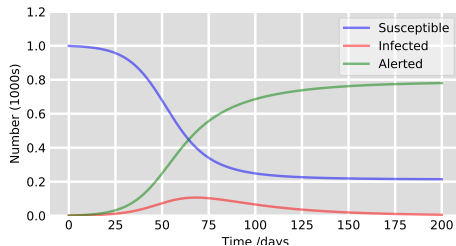
مدل مستعد-آگاه-بیمار-مستعد (SAIS)

کاهش نرخ ابتلا از β به β_a برای افراد آگاه و مراقب

تغییر وضعیت به حالت آگاه و مراقب با نرخ κ



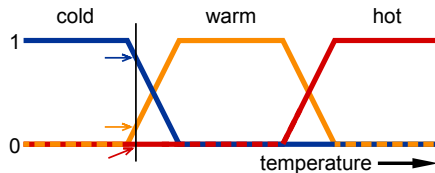
شکل ۵: مدل مارکوف انتشار بیماری SAIS



شکل ۴: تغییرات گذرا برای مدل SAIS

منطق فازی - ۱

- ▶ روشی برای مدل کردن ارتباط بین ورودی و خروجی
- ▶ تعریف مجموعه فازی^۹
- ▶ اعضای مجموعه فازی شامل متغیرهای زبانی هستند که مقادیر آنها از مقادیر زبانی^{۱۰} انتخاب می شود.
- ▶ تعریف مقدار حدودی بین ۰ تا ۱ برای ورودی و خروجی ها (درجه عضویت^{۱۱})



شکل ۶: تابع عضویت فازی برای دمای محیط

⁹Fuzzy Set

¹⁰Linguistic values

¹¹Membership grade

- ۱ تبدیل ورودی‌های عددی به متغیرهای زبانی^{۱۲} (غیر دقیق و حسی) یا فازی سازی
 - بر اساس تابع عضویت فازی
- ۲ استنتاج فازی مطابق با قواعد فازی تعریف شده (بر اساس توصیف زبانی اگر ← آنگاه)
- ۳ تبدیل خروجی فازی به یک متغیر عددی (فازی گشایی)
 - بر اساس تابع عضویت فازی
 - به کمک روش‌های تجميع سازی نتایج

¹²Linguistic variable

قسمت ۳

کارهای پیشین

دسته بندی کارهای پیشین در زمینه شبکه‌های 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 پیش‌بینی انتشار بیماری
- ۹ انتشار ویروس و بد افزار رایانه‌ای

دسته بندی کارهای پیشین در زمینه شبکه‌های 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 پیش‌بینی انتشار بیماری
- ۹ انتشار ویروس و بد افزار رایانه‌ای

- 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 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 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 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]

- بررسی مدل بیماری SEIV^{۱۳} 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 شبکه دو لایه (یک لایه ثابت و یک لایه متغیر) [۱۵]

¹³Susceptible-Exposed-Infected-Vigilant

قسمت ۴

حل مسئله

فرایند کلی حل مسئله

شبیه‌سازی:

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

مدل‌سازی:

- ۱ تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
- ۲ تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی‌های مسئله)
- ۳ تعریف روابط ریاضی تجميع 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 شبیه‌سازی

فرایند کلی حل مسئله

شبیه‌سازی:

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

مدل‌سازی:

- ۱ تعریف متغیرهای فازی و توابع عضویت (فضای پیوسته)
- ۲ تعریف جدول قواعد فازی (ارتباط بین ورودی و خروجی‌های مسئله)
- ۳ تعریف روابط ریاضی تجميع 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 شبیه‌سازی

قسمت ۵

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] Vizuite, Renato, Frasca, Paolo, and Garin, Federica. Graphon-based sensitivity analysis of sis epidemics. *IEEE Control Systems Letters*, 4(3):542–547, 2020.
- [5] Khanjanianpak, Mozghan, 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 ۶

تشکر از توجه شما

قسمت ۷

صفحات پشتیبان

مثال

این یک مثال است.

تعریف

این یک تعریف است.

قضیه

این یک قضیه است.

قضیه (Pythagoras)

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

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

قضیه (Pythagoras)

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

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

اثبات.

$$\omega + \phi = \epsilon$$



قضیه (Pythagoras)

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

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

اثبات.

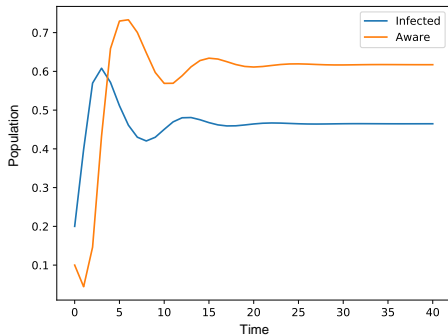
$$\omega + \phi = \epsilon$$



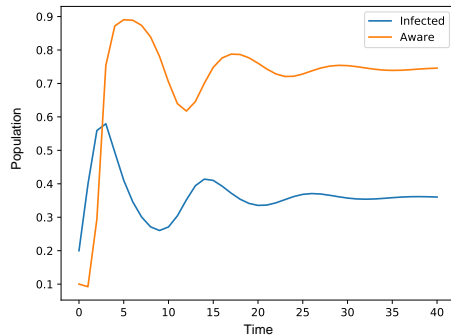
نتیجه

$$x + y = y + x$$

نتیاج شبیه سازی آماری



(ب) یادگیری=0.5 و فراموشی=0.75



(آ) یادگیری=0.75 و فراموشی=0.5

شکل ۷: نتیجه اجرای شبیه سازی آماری در دو حالت

Algorithm ۱ اجرای برنامه 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 یادگیری-فراموشی

۴: محاسبهٔ وضعیت جدید مدل مارکوف بیماری و آگاهی

۵: پایان حلقهٔ برای

۶: بازگردان ماتریس تغییرات زمانی
