Краевая научно-практическая конференция

учебно-исследовательских работ учащихся 6-11 классов

«Прикладные и фундаментальные вопросы математики»

Математическое моделирование

Математическая модель динамики эпидемии сетевых червей

Никулин Денис Вениаминович,
11 кл., МБОУ Лицей №1, г. Пермь,
Лихачев Арсений Алексеевич
11 кл., МБОУ Лицей №1, г. Пермь,
НикитюкАлександр Сергеевич,
учитель информатики,
аспирант ИМСС УрО РАН.

Пермь, 2016

Оглавление

Введение

Целью работы является разработка математической модели, которая позволит нам изучить динамику эпидемии сетевых червей и оценить степень угрозы на различных стадиях.

Модель должна позволять:

- Предсказывать время распространения сетевых червей в определенной сети
- Определить количество зараженных хостов за время эпидемии

Исходные данные:

- Количество зараженных хостов и хостов находящихся под угрозой заражения.
- Скорость распространения сетевых червей
- Скорость обнаружения зараженных хостов
- Скорость излечения зараженных хостов
- Время «жизни» сетевого червя

Концептуальная постановка(SIS модель)

Для решения поставленной задачи достаточно исследовать математическую модель эпидемии сетевых червей.

Гипотезы

- Объектом исследования является эпидемия сетевых червей
- Предметной областью анной задачи является информационная защита
- Эпидемия происходит в сети состоящих из N хостов.
- Рассматриваем один тип сетевого червя
- Скорость заражения хоста примерно Vs(из жизни)
- Топология сети : полносвязная
- Каждый хост может находиться в двух состояниях(уязвим к заражению, заражен)
- Всеми внешними воздействиями мы пренебрегаем

Математическая постановка(SIS модель)

Введем переменную ***b*** ,которая будет означать скорость заражения 1 хоста . В нашем случае она будет определятся формулой :

b = Vs * N / Nip (1) , где ***Nip*** – размер адресного пространства, в спецификации протокола IP4 ***Nip***=2^32.

Для описания динамики доли инфицированных хостов введем переменные ***i = I / N (2)*** и ***s = S / N (3)***

Уравнение для описания динамики доли инфицированных хостов будет выглядеть следующим образом:

di / dt = b * (1 – i) * i (4)

Для реализации моделей такого типа мы используем численный метод Эйлера:

i(t+dt)= i(t) i(t)* (1-i(t))*b*dt

Исходные данные:

Nip = 2^32; максимальное кол-во хостов в сети по протоколу IP4

N= 2^16; кол-во хостов в сети

Vs= 2^1I =4; скорость сканирования червем сети

dt = 10; промежутки времени

I=4; начальное количество инфицированных хостов

b=3.051757;скорость заражения хостов

Результат SIS модели

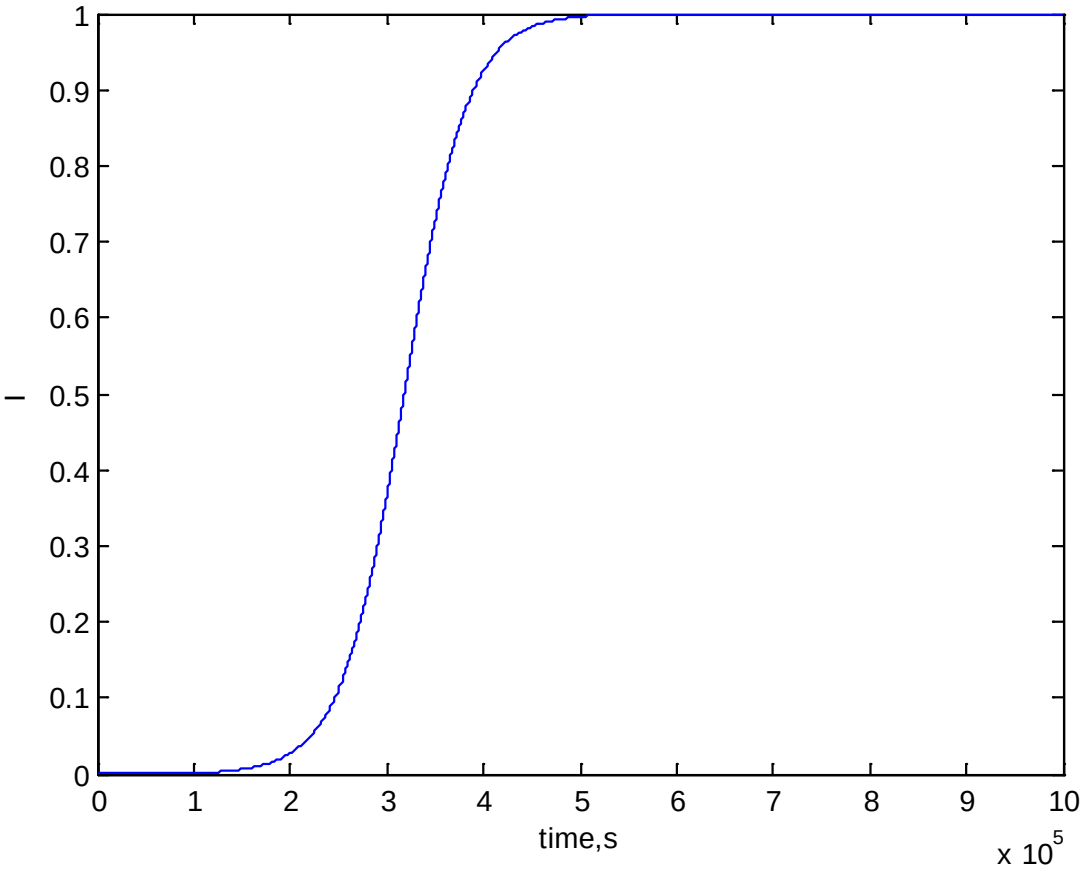

Рис. 1 График зависимости динамики заражения от времени

Итоги (SIS модель)

Динамика функции характеризуется тремя четко различимыми этапами :

- 1-й этап – медленное нарастание доли зараженных хостов (до i=0.05)
- 2-й этап – взрыв эпидемии ,очень быстрый рост доли зараженных хостов (до i=0.95)
- 3-й этап – насыщение при котором инфицированные хосты чаще взаимодействуют друг с другом чем с чистыми ,из-за чего хосты могут оставаться чистыми неопределенно долгий промежуток времени

Концептуальная постановка (SIR модель (1))

Модифицируем нашу модель

- Каждый хост может находится в трех состояниях (уязвимый(S), инфицированный(I), неуязвимый(R))
- Все хосты (N) состоят из уязвимых(S) ,инфицированных(I) и неуязвимых(R)

Математическая постановка (SIR модель(1))

Введем переменную для обозначения доли неуязвимых хостов :

r = R / N (5)

Вводим среднюю скорость «иммунизации» хостов внутри сети и обозначаем ее переменной ***y***

Составим модель на основе данной системы уравнений :

ds / dt = -b * i* s (6),

di / dt = b * i * s – y * i (7),

dr / dt = y * i (8).

Также для начала эпидемии в данной математической модели необходимо выполнение условия :

s(0) > y / b

Исходные данные:

y **=** 3.051757; скорость иммунизации хостов

R = 100; начальное количество неуязвимых хостов

I = 2000; начальное количество инфицированных хостов

S= 63436;начальное количество уязвимых хостов

b**=** 9.765625;скорость заражения хостов

Результаты (SIR модель (1))

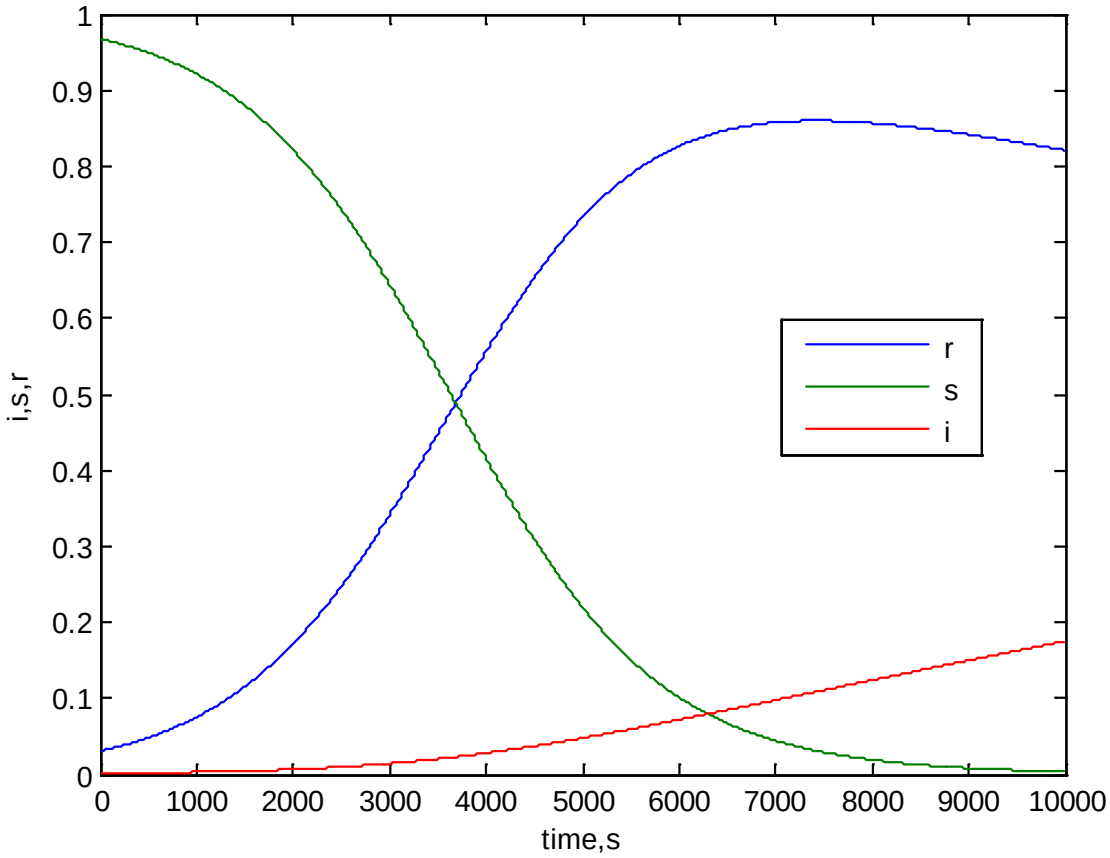

Рис.2 График зависимости доли инфицированных хостов от времени, доли неуязвимых хостов от времени, долю уязвимых к заражению хостов от времени

Итоги (SIR модель (1))

Мы можем наблюдать ,что доля уязвимых хостов (s)уменьшается со временем уменьшается и достигает 0 ,в то время как доля неуязвимых(r) резко возрастает ,однако, через некоторое время начинается медленное уменьшение этой доли. Доля инфицированных узлов(i) медленно возрастает.

Математическая постановка (SIR модель(2))

Далее нашу модель можно улучшить путем добавления в нее переменного число узлов

Так как в нашу модель добавилось переменное число узлов ,то добавим скорость прироста новых уязвимых хостов (S) и назовем ее ***a***

Тогда наша система приобретет следующий вид :

ds / dt = - b * i * s – (y + a) * s + a (9),

di / dt = b* i * s – (y + a) * i (10),

dr / dt = y * (1 – r) – a * r (11).

А условие развития эпидемии принимает вид :

s > (y + a) / b

Исходные данные:

Используются те же данные что и в SIR модели (1)

a = 3.051757; скорость прироста новых уязвимых хостов

Результат (SIR модель(2))

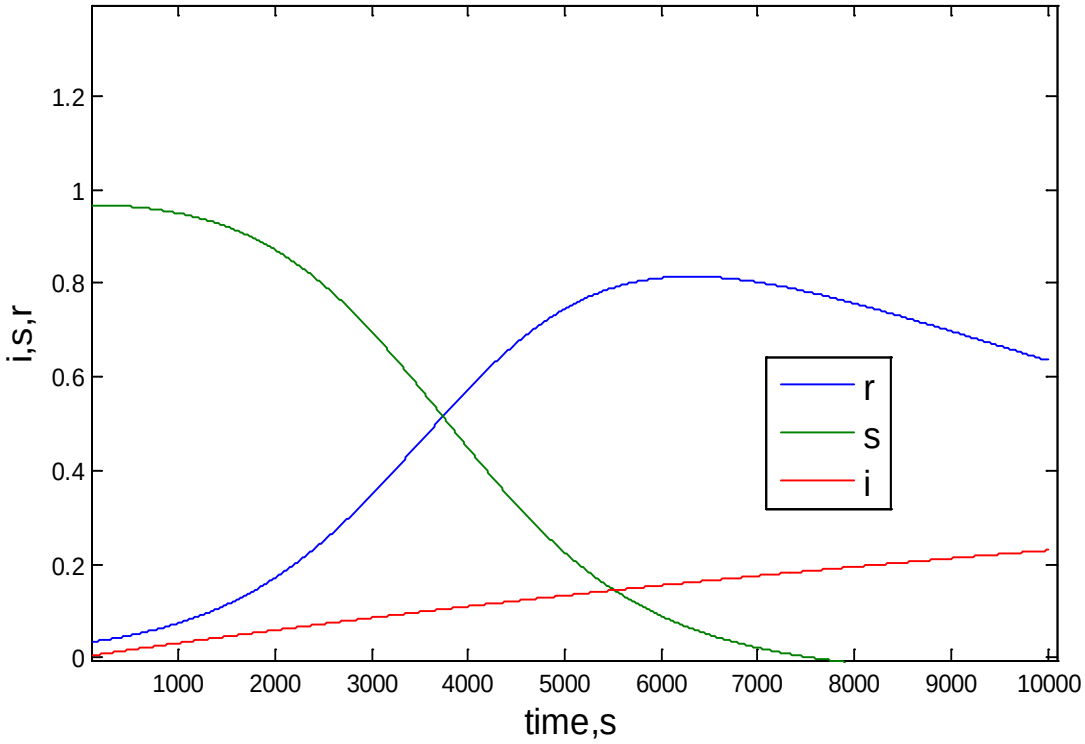

Рис.3 График зависимости доли инфицированных хостов от времени, доли неуязвимых хостов от времени, долю уязвимых к заражению хостов от времени, все это с учетом присоединения новых хостов, которые уязвимы к заражению

Итоги (SIR модель(2))

Как и в случае с SIR моделью (1) доля уязвимых хостов(s) снижаясь достигает 0

Также ,в отличие от не модифицированной модели , происходит более резкое увеличение доли неуязвимых хостов(r) ,но и более быстрое начало ее снижения.

Далее ,мы видим что происходит более резкое увеличение доли инфицированных хостов(i) .

Заключение

Нам удалось реализовать несколько моделей эпидемий сетевых червей, но для них мы не использовали определенный тип сетевого червя, мы занимались только отладкой получившихся моделей. С использованием этих моделей нам удалось получить, несколько зависимостей распространения в сети червя за определенный отрезок времени - это доказывает что модели, которые мы реализовали, отлажены.