ФОРМИРОВАНИЕ АНАЛИТИЧЕСКОЙ МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ ПАРАМЕТРОВ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Камкамидзе Константин, Двалишвили Михаил, Камкамидзе Елена

Грузинский Технический Университет

Резюме

Поставлена задача создания аналитической модели распространения угрозы запрещенной информации в телекоммуникационных сетях. Для получения экспериментальных результатов для синтезирования аналитической модели необходима имитационная модель. Создана имитационная модель угроз запрещенной информации в телекомуникационной сети, учитывающая топологические характеристики сети. С ее помощью проведены эксперименты, результаты которых показали зависимость реализации угрозы от топологической уязвимости сети. Примеры эффективного апробирования механизмов прогнозирования угроз в телекомуникационной сети дают основание констатировать адекватность и функциональность основных теоретических построений и разработанных на их основе алгоритмических и инструментальных средств.

Ключевые слова: атакующие узлы. Запрещенный контент. Аналитическая модель.

1. Введение

Информационно-телекоммуникационные сети обеспечивают практически полный спектр возможностей для обмена информацией между пользователями - сетевыми абонентами. Современной проблемой таких систем является их низкий уровень информационной безопасности. Для обеспечения защиты информации в телекоммуникационных сетях, включая Интернет, разработано множество методов и средств. Тем не менее, эффективной защиты абонентов от угроз распространения запрещенной информации, в частности в условиях широкого использования индивидуально-ориентированных сервисов и связанных с ними протоколов и технологий (SOAP, CORBA, REST и др.), не существует. Среди множества функций защиты принципиальной в отношении данных систем является функция предупреждения проявления запрещенной информации. Она реализуется за счет механизмов прогнозирования угрозы распространения и рассылки сообщений с предупреждениями о последствиях действий с запрещенным контентом. Одним из подходов к прогнозированию угрозы распространения запрещенной информации является моделирование.Моделирование принято рассматривать в двух аспектах. Первый касается моделирования топологии сети, а второй затрагивает проблему изучения процессов, проходящих в ней. В нашем случае это угроза распространения запрещенной информации.

2. Основная часть

В информационно-телекоммуникационных сетях существуют узлы трех типов. Первый тип – атакующие узлы, это узлы, распространяющие запрещенную информацию. Второй тип – защищенные узлы, характеризующиеся тем, что не принимают участие в распространении запрещенной информации и никогда не будут этим заниматься. Третий тип – потенциально уязвимые. Узлы такого типа не участвуют в процессе распространения угрозы, но могут быть подвержены негативному влиянию со стороны атакующих узлов и могут начать распространять запрещенную информацию [1,2]. Допустим, N – количество узлов, равное числу абонентов сети, I_0 – количество абонентов-злоумышленников – изначальных источников угрозы, R_0 – количество абонентов изначально невосприимчивых к атакующим воздействиям, β -параметр, отражающий силу угрозы, вероятность осуществления атаки, γ -параметр отражающий степень противодействия угрозе, вероятность защиты абонента (β и γ в данном исследовании

определены как константы, но могут быть выражены как функции, зависящие от психосемантических профилей абонентов). φ - коэффициент топологической уязвимости сети, отражающий внутреннее свойство телекомуникационной сети, основанное на характеристиках ее топологии, t - время процесса (в условных единицах времени). Требуется разработать аналитическую модель динамики атаки $I(t)$ и защиты узлов $R(t)$.

Методика включает в себя последовательность следующих действий:

- формирование имитационной модели для исследования характера и параметров процесса телекомуникационной сети;
- синтез аналитических зависимостей параметров процесса;
- проведение экспериментов с целью проверки точности модели.

Приведем алгоритм реализации телекомуникационной сети, основываясь на описании процессов, протекающих в реальных сетях. Схема реализации угрозы представлена на рисунке 1.

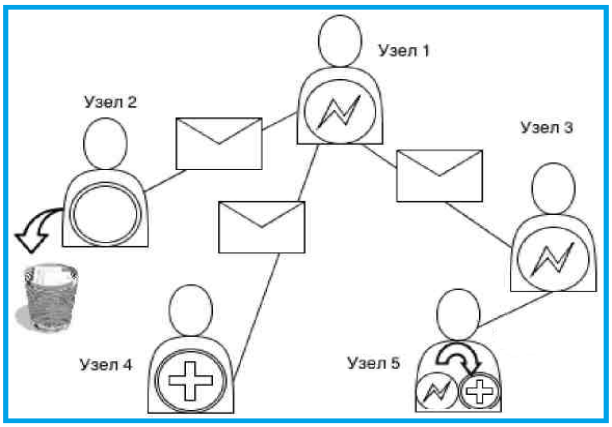

Рис.1. Схема угроз в телекомуникационных сетях

Шаг1. Распространение запрещенной информации (ЗИ) (далее процесс «атаки») инициирует какой-либо абонент-злоумышленник (на рисунке -узел1), распространяя сообщения с ЗИ (реализует угрозу) по его списку контактов. Атаку может начинать один злоумышленник или группа;

Шаг 2. Абоненты-получатели (узлы 2,3,4), приняв сообщение с ЗИ, читают его и включаются в процесс атаки, распространяя ее дальше по своему списку контактов (узел 3), либо игнорируют или вообще удаляют сообщение (узел 2), т.е. в атаке не участвуют. Процесс атаки обычно идет лавинообразно. Атакующие абоненты не заканчивают атаку, единожды передав сообщение с запрещенной информацией. Окно атаки, как правило, продолжается в течение довольно значительного промежутка времени и зависит от типа подачи ЗИ в сообщении, заинтересованности абонента и т.д.;

Шаг 3. Абоненты могут перестать воспринимать и, соответственно, распространять ЗИ (узел 5) (далее процесс «защиты»), вследствие воздействия механизмов защиты, поэтому сообщения с ЗИ от атакующих абонентов будут постоянно отвергаться;

Шаг 4. Процесс продолжается пока в сети есть абоненты-злоумышленники, либо есть потенциально уязвимые узлы, если отсутствует процесс защиты.

Таким образом, телекомуникационная сеть представляет собой сложный динамический процесс, состоящий из двух противоборствующих подпроцессов атаки и защиты узлов сети На основе описанного алгоритма построена имитационная модель, которая состоит из разработанной программы Model Graph и данных, которые могут быть сгенерированы с помощью ПО Pajek [3,4]. Входные данные: N, κ - средняя степень связности узлов, a - параметр, отражающий среднюю длину пути и уровень сетевой кластеризации, β, γ (в модели считается, что β и γ одинаковы для каждого абонента), $I0$, $R0$. Выходные данные: $I(t)$, $R(t)$, $S(t)$ - численные массивы данных, описывающие динамический процесс реализации угроз (количестве атакующих, защищенных и потенциально уязвимых узлов в каждую условную единицу времени соответственно).

Шаг 1. Создание топологии телекомуникационной сети – графа $Gsw = <V, E>$, где Gsw - граф small-world сети , $V = \{vi\}$ - множество вершин, $E = \{ ei\ j \}$ - множество ребер, $i=1,..N$, $j=1,..N$. Данный шаг осуществляется за счет задаваемых топологических параметров N, κ, a.

Шаг 2. Сформировать множество $K=\{ VI, VS, VR \}$, где $VI =\{v^1_i\}$ – множество атакующих

узлов (|*VI* |= *I0*), , *VR* - множество защищенных узлов, *(VR =Ro),VS* - множество потенциально уязвимых узлов (|*VS* |= *N -1o- Ro).*

Шаг 3. С вероятностью β выполнить: *VS* и *VI* , с вероятностью γ выполнить: *VI*.

Шаг 4. Если *VI* =Ø или γ=0 и *VS*=Ø, то конец алгоритма, иначе перейти к шагу 3.

ModelGraph - программа для имитационного моделирования угрозы запрещенной информации в телекомуникационной сети [4]. Данный программный продукт является однопоточным приложением. Программа состоит из исполняемого файла Model Graph.exe и библиотеки chartdir50.dll для построения графиков. После выбора типа сети и ввода ее параметров происходит имитационное моделирование по алгоритму. Затем результаты отправляются в функцию построения графиков для вывода результатов в графическом виде.

Программа написана в среде разработки Microsoft Visual Studio .NET 2008. Исходными данными для гетерогенной сети является файл формата .net, определенный в программе Pajek. ПО Pajek представляет собой программу, предназначенную для анализа и визуализации больших сетей. Данная программа находится в свободном доступе и предназначена для некоммерческого использования. Проанализируем подпроцесс атаки без защиты, проведя ряд экспериментов с использованием имитационной модели.

Эксперимент 1. Влияние силы атаки на процесс. Эксперименты проводились при следующих значениях параметров: *N*=1000, φ=20, *I*0=1, β=0,1..0,9 .

Эксперимент 2. Влияние значения средней степени связности узлов в сети на процесс. Эксперименты проводились при следующих значениях параметров: *N*=1000, φ=0,5...60, *I*0=1, β=0,5 (рисунок 2).

Эксперимент 3. Влияние количества изначально атакующих узлов на процесс. Эксперименты проводились при следующих значениях параметров: *N*=1000, φ=20, *I*0=1..40, β=0,5 (рисунок 3).

Каждый из трех типов экспериментов проводился 100 раз, брались усредненные значения. По результатам экспериментов 1-3 можно сделать следующие выводы:

- процесс атаки *I(t)* имеет экспоненциальную зависимость, при увеличении значений φ, *I*0, β возрастает динамика заражения узлов (интенсивность атаки) (эксперимент 1,2,3);
- при росте вероятности проведения атаки β от 0,1 до 0,9, время процесса снижается в два раза (с 8 до 4 условных единиц времени) (эксперимент 1);
- коэффициент топологической уязвимости φ имеет самое большое влияние (в сравнении с *I*0, β) на длительность процесса. Например, при φ = 0,5 (низкая уязвимость) атака длится 24 условные единицы времени, а при φ = 60 всего лишь 4 (эксперимент 2); большое количество изначально атакующих узлов *I*0 снижает время, за которое происходит заражение всех узлов в сети. Например, при *I*0=40 длительность процесса составляет 3 условные единицы времени (эксперимент 3).

Усложним условия экспериментов, добавив подпроцесс защиты, который зависит от начального количества защищенных узлов *R0* и вероятности защиты γ.

Эксперимент 4. Влияние вероятности защиты.

Эксперименты проводились при следующих значениях параметров: *N*=1000, φ = 20, *I*0=1, β=0,5, γ =0,1..0,9, *R*0 =0. (рисунок 4).

Эксперимент 5. Влияние начального количества защищенных узлов.

Эксперименты проводились при следующих значениях параметров: *N*=1000, φ = 20, *I*0=1, β=0,5, γ =0,5, *R*0 =0..200. (рисунок 5).

По результатам экспериментов 4 и 5 можно сделать следующие выводы: введение подпроцесса защиты увеличивает время всего процесса угрозы запрещенной информации в телекоммуникационной сети. (эксперимент 4,5); при небольших значениях вероятности защиты (γ<0,3) угроза реализуется практически на всех узлах в сети (эксперимент 4); при небольших значениях вероятности защиты (γ<0,3) время процесса составляет более 50 условных единиц времени

(эксперимент 4); при большой вероятности защиты (≈0,9) процесс длится ≈7 условных единиц времени и максимальное количество атакующих узлов снижается в зависимости от вероятности проведения атаки (эксперимент 4).

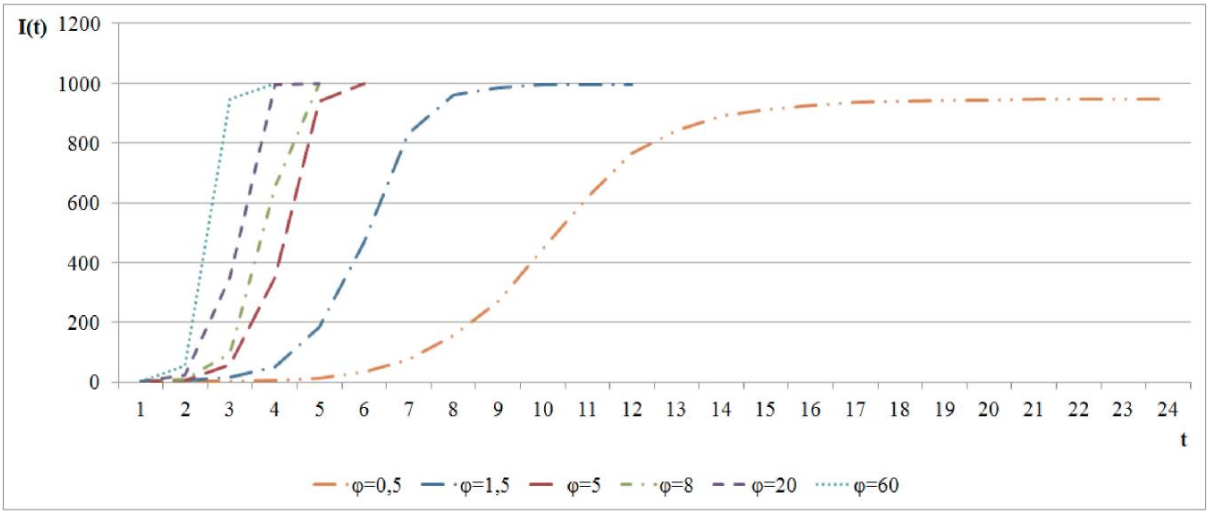

Рис.2. Влияние φ на процесс атаки

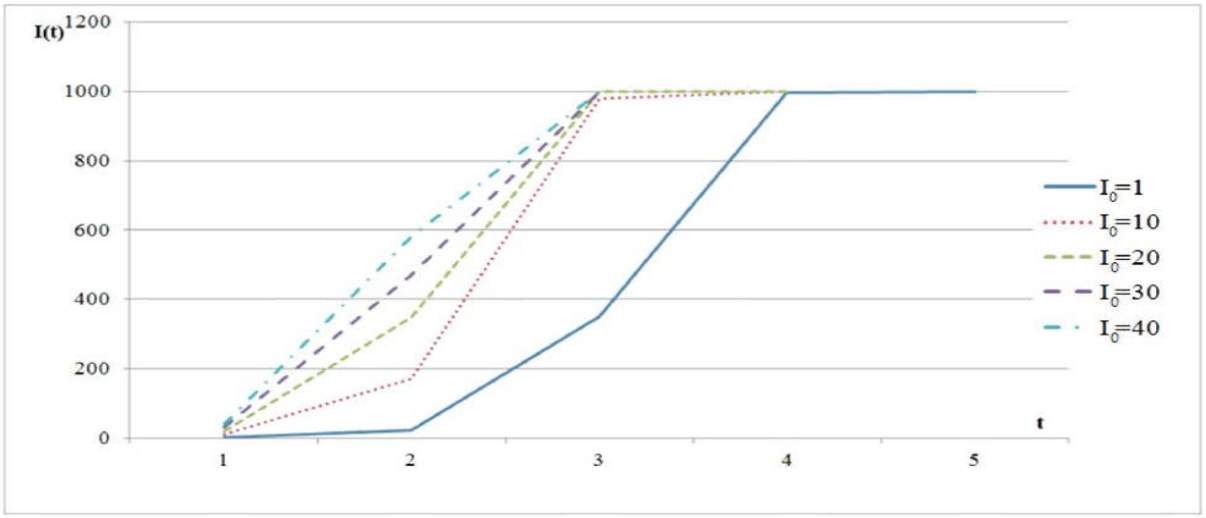

Рис.3. Влияние $I0$ на процесс атаки

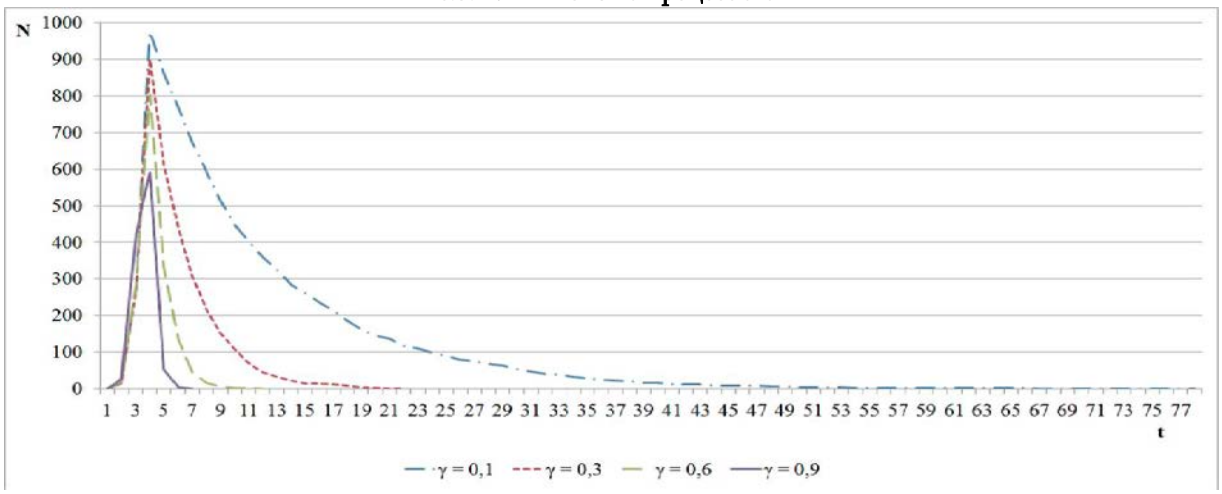

Рис.4. Влияние γ на процесс атаки

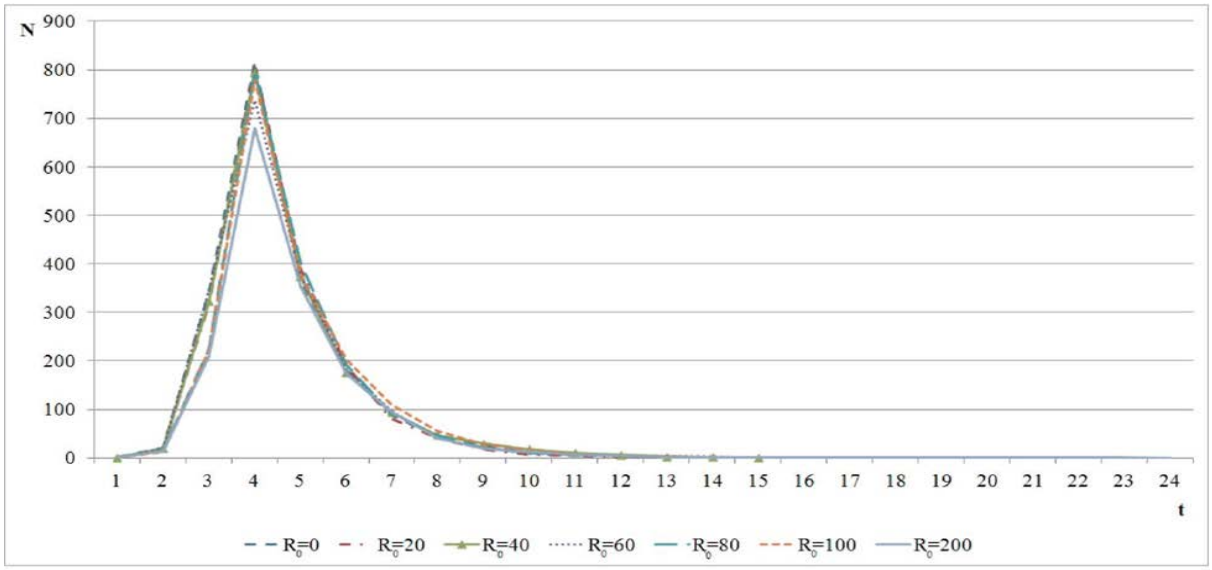

Рис.5. Влияние R0 на процесс атаки

При случайном выборе изначально защищенных узлов картина процесса атаки практически не изменяется (эксперимент 5); при высокой топологической уязвимости возрастает длительность процесса угрозы запрещенной информации в телекомуникационной сети.

Создана имитационная модель угроз запрещенной информации в телекомуникационной сети, учитывающая топологические характеристики сети, а также особенности информационного взаимодействия абонентов как человеко-машинных систем. С ее помощью проведены эксперименты, результаты которых показали зависимость реализации угрозы от топологической уязвимости сети. Релевантность результатов подтверждена серией экспериментов на топологии реальной сети с использованием имитационного моделирования. При этом погрешность для процесса защиты составила не более 10%, для процесса атаки - не более 15%.

3. Выводы

Информационно-телекоммуникационные сети являются крупномасштабными сетями с постоянно растущим числом абонентов. С бурным ростом числа пользователей возникают проблемы информационной безопасности и защиты информации в них. Анализ проблем информационной безопасности выявил, что кроме проблем, связанных с использованием глобальной сети Интернет как распределенной информационно-телекоммуникационной системы, которые достаточно хорошо известны и решаемы, существует малоизученная проблема запрещенного контента. Создание моделей и алгоритмов распространения угрозы запрещенной информации – один из ключевых подходов при решении данной задачи. Проведенный анализ публикаций по данной тематике показывает, что существующие решения малоэффективны. Обычно при моделировании распространения угрозы запрещенной информации не учитывается топология телекоммуникационной системы (модель сети – полносвязный граф). А, если топология учитывается, то, как правило, используется простейшая SIS модель, а структура сети отражается SF сетью. При моделировании телекоммуникационной системы важно иметь топологию, отражающую структуру связей реальной сети, а также использовать адекватную модель информационного взаимодействия узлов. Еще одной важной проблемой является крупномасштабность телекомуникационной сети, которая мешает получить данные с имитационной модели за приемлемое время.

Литература:

1. Брэгг Р., Родс-Оусли М., Страссберг К. (2006). Безопасность сетей. Полное руководство. - М.: Эком.

2. Биячуев Т.А. (2004). Безопасность корпоративных сетей .учеб. пособие. под ред. Осовецкого Л.Г. - СПб.: ГУ ИТМО.

3. Бреер В.В. (2009). Стохастические модели социальных сетей / В.В. Бреер; Управление большими системами, № 27.

4. Программное обеспечение Pajek [Электронный ресурс] / Vladimir Batagelj, Andrej Mrvar; - Режим доступа: http://pajek.imfm.si/doku.php

5. Gjoka M., Kurant M., Butts C.T., Markopoulou A.A. (2010). Walk in Facebook: Uniform Sampling of Users in Online Social Networks. IEEE INFOCOM '10. IEEE Journal on Selected Areas in Communications.

DEVELOPMENT OF AN ANALYTICAL MODEL FOR THE RESEARCH OF THE TELECOMMUNICATION NETWORK PARAMETERS

Kamkamidze Konstantin, Dvalishvili Mikheil, Kamkamidze Elene
Georgian Technical University

Summary

Article discusses development of a model for analyzing threat of the dissemination of restricted informational through the telecommunication network. In order to obtain the trial results to synthesize analytical model – simulation modeling of the existing telecommunication network topology is required. The simulation model of restricted informational threats in telecommunication network was developed taking into account network topological features. Experiments showed some dependence of the threat realization on the network topology. The examples of effective implementation of the threat prognosticating mechanism in the telecommunication network gives the reason to ascertain the adequacy and functionality of the main theoretical concepts and developed from the latter algorithmic and instrumental tools.

სატელეკომუნიკაციო ქსელის პარამეტრების კვლევის ანალიტიკური მოდელის ფორმირება

კონსტანტინე კამკამიძე, მიხეილ დვალიშვილი, ელენე კამკამიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია სატელეკომუნიკაციო ქსელში აკრძალული ინფორმაციის გავრცელების საფრთხის ანალიტიკური მოდელის დამუშავების ამოცანა. ანალიტიკური მოდელის სინთეზისათვის ექსპერიმენტული შედეგების მისაღებად აუცილებელია არსებული სატელეკომუნიკაციო ქსელის ტოპოლოგიის იმიტაციური მოდელირება. დამუშავებულია სატელეკომუნიკაციო ქსელში აკრძალული ინფორმაციის საფრთხის იმიტაციური მოდელი, რომელიც ითვალისწინებს ქსელის ტოპოლოგიურ მახასიათლებს. ჩატარებული ექსპერიმენტების შედეგებმა აჩვენა აკრძალული ინფორმაციის გავრცელების საფრთხის რეალიზაციის გარკვეული დამოკიდებულება ქსელის ტოპოლოგიაზე. საფრთხეების პროგნოზირების მექანიზმის ეფექტური აპრობაციის მაგალითები ასახავენ ძირითადი თეორიული გათვლების და მათ საფუძველზე ალგორითმული საშუალებების დამუშავების მართებულობას.