ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

Ф. Галиндо, Н. В. Дмитриенко, А. Карузо, А. Россодивита, А. А. Тихомиров, А. И. Труфанов, Е. В. Шубников

МОДЕЛИРОВАНИЕ СЛОЖНЫХ АТАК НА КОМПЛЕКСНЫЕ СЕТИ

Введение

Устойчивость сетевой архитектуры является одной из важнейших проблем построения эффективных сложных социальных, биологических, технических и других систем. Стоит обратить внимание, что для ряда сложных систем характерна высокая численность элементов, которая может достигать десятков и сотен тысяч, и нерегулярность связей. Таким системам и их сетевым моделям, обладающим нетривиальными топологическими свойствами, в наибольшей степени отвечает термин «комплексные».

Наиболее популярными и отвечающими реальности комплексными сетями в настоящее время являются модели Эрдёша—Реньи [1] и Барабаши—Альберта [2]. В первой плотность распределения связей отвечает закону Пуассона:

$$P(k) \sim e^{-\lambda} (\lambda^k)/k!$$

Эти сетевые модели также носят название случайных или экспоненциальных (E-сети). Во второй половине XX в. экспоненциальные сети являлись базовыми для анализа систем. С такого рода моделями связано развитие теории графов.

В 1998 г. в своей основополагающей работе [2] А.-Л. Барабаши (Albert Laslo Barabasi) с сотрудниками обратил внимание исследователей на то, что многие реальные сети (коммуникационные, веб-, социальные и метаболические) носят иной, нежели описываемые экспоненциальной моделью, характер. Авторами была предложена сетевая модель, в которой:

а) распределение связности (числа связей, или степени) отвечает степенному закону

$$P(k) \sim k^{-\gamma};$$

б) характеристикой является рост сети с введением новых узлов и новых связей, причем наблюдается так называемое предпочтительное присоединение;

в) использована терминология, простая и понятная для специалистов различных дисциплин.

Такая модель сети носит название безмасштабной (SF).

Графическое представление из [2] (Рис. 1) обошло весь мир и широко используется для демонстрации топологии экспоненциальных и безмасштабных сетей.

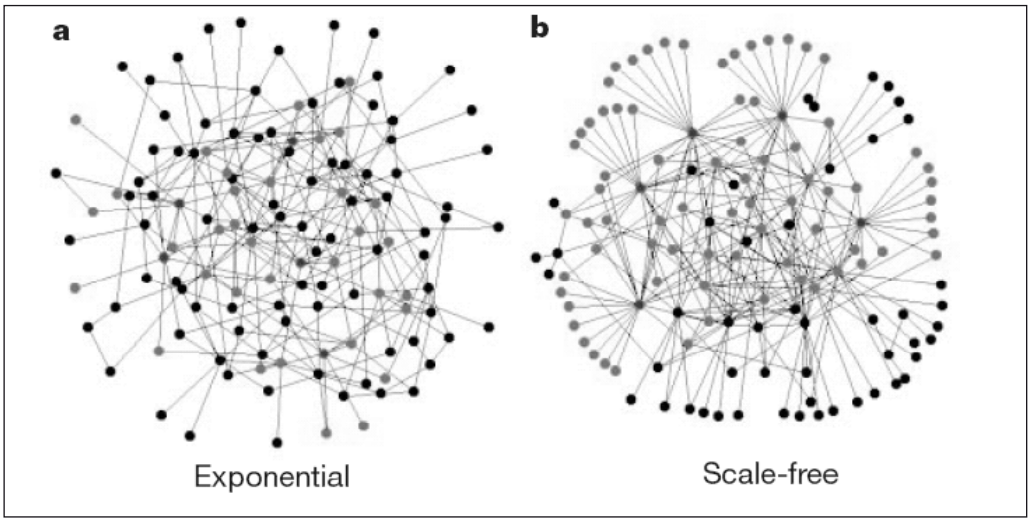


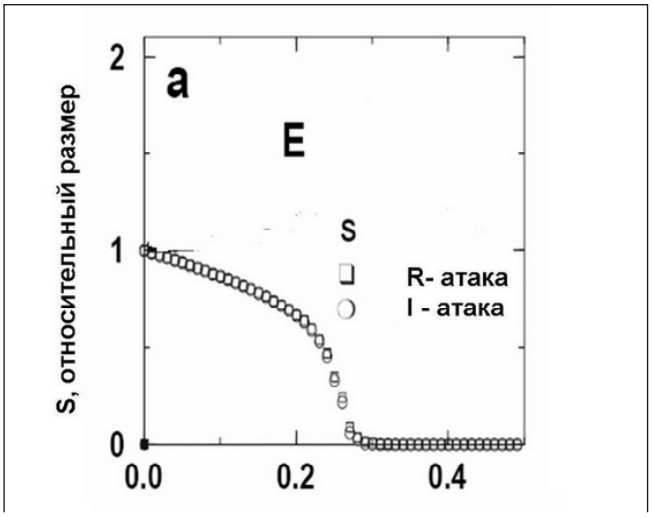
Рис. 1. Экспоненциальная (a) и безмасштабная (b) сети

Устойчивость этих двух разных архитектур, экспоненциальной и безмасштабной, к двум основным классам атак на узлы сети: случайным и целенаправленным, как оказалось, оказалась существенно различается.

Случайным атакам (отказам, сбоям, R-атакам) присущ случайный выбор атакуемого (уничтожаемого) узла. Классическая стратегия целенаправленных атак (I-атак) заключается в последовательном уничтожении узлов с максимальной связностью. Обычно последствия атак исследуемых сетей анализируются с помощью широкого набора метрик: регистрируются изменения диаметра, среднего связующего, среднего разделяющего, коэффициента кластеризации различных центральностей, размера максимального кластера и его относительных величин. На примере расчетов [3] (Рис. 2) изменения относительного размера максимального кластера S было установлено, что экспоненциальные сети в одинаковой степени уязвимы к R- и I-атакам (Рис. 2a). Безмасштабные же сети оказались устойчивы к случайным атакам и крайне уязвимы к атакам целенаправленным (Рис. 2b).

Действительно, целенаправленные атаки на SF-сети более эффективны, но они и более дорогостоящи.

В реальной жизни наблюдаются более сложные ситуации, т. е. обладающие различной уязвимостью элементы — узлы и связи — сетей различной топологии подвергаются неоднородным случайным и целенаправленным угрозам, причем в разнообразных комбинациях.



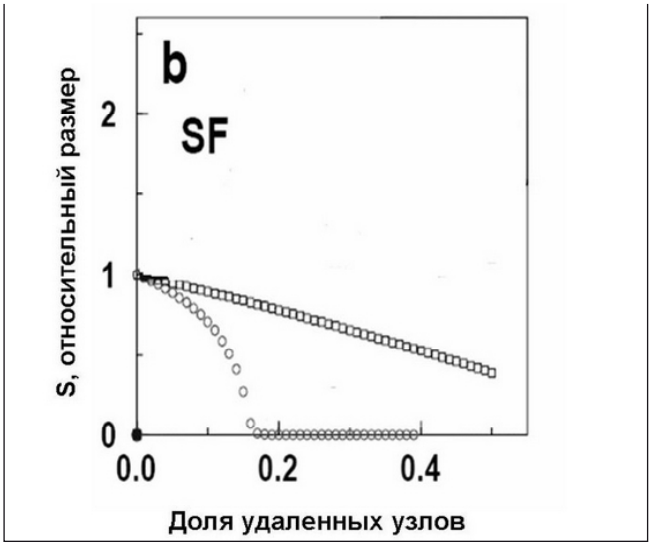


Рис. 2. Зависимость относительного размера максимального кластера в экспоненциальных (a) и безмасштабных (b) сетях, подвергнутых случайным (□) и преднамеренным (○) атакам

Модель и метод исследования

Нами разработана обобщенная агентная модель эволюции сетевого ансамбля в условиях дестабилизирующих угроз. Эта модель, которую мы назвали RT-моделью, не только отражает топологию сетей, подобно известным подходам, но и включает ряд новаций, нацеленных именно на решение проблем безопасности.

Основными компонентами описательной конструкции сети являются: ***модель эволюции*** и ***модель безопасности***.

Модель эволюции сети включает а) генерацию новых узлов, б) генерацию связей между узлами — в случайной, предпочтительной или иерархической схеме, б) «естественную» ликвидацию узлов и связей. Формируемые — эволюционирующие — сети отражают возможные случайную, безмасштабную и иерархическую топологии.

Модель безопасности учитывает, что основной мерой безопасности является риск:

РИСК = ρ* ЦЕНА ПОТЕРИ,

где ρ — вероятность атаки.

В настоящее время исследователи стойкости комплексных сетей обычно полагают, что любые проявления угроз в отношении элементов сетевых ансамблей — узлов и связей — приводят к успешным атакам, т. е. к удалению узлов и связей.

Из известных определений в теории информационной безопасности следует, что атака — это всегда пара «источник угрозы — уязвимость», реализующая угрозу и приводящая к ущербу (см., например: [4]):

РИСК = $\rho_{\text{угрозы}}$ * $\rho_{\text{уязвимости}}$ * ЦЕНА ПОТЕРИ,

где $\rho_{\text{угрозы}}$ и $\rho_{\text{уязвимости}}$ — соответствующие вероятности угрозы и уязвимости.

Отличительной особенностью развиваемой сетевой модели является детализация атак через подробное описание составных частей этой пары — источника и уязвимостей.

Во-первых, модель позволяет путем составления описаний источников угроз, близких к реальным, изучать более сложные атаки на системы, нежели в их традиционной для сетевых моделей трактовке. В предлагаемой модели не только сетевые ансамбли рассматриваются как динамические объекты, но и угрозы описываются распределенными во времени.

Во-вторых, данный подход дает возможность для каждого из узлов ввести параметр уязвимости (или защищенности), в отличие от большинства известных, где следствием атаки всегда является уничтожение узла или связи. Элементам сети приписываются величины их уязвимости, в общем случае, с ρ_i уязвимости отличными от 1, и определяемыми объемом финансовых вложений F_i в безопасность i-го элемента:

ρ_i уязвимости $= f(F_i)$.

Цена потери — как реакции сети на атаку — определяется выбором элемента из множества метрик M — тех индикаторов работоспособности, которые определяют главные целевые характеристики сетевых ансамблей.

В данной модели используются традиционные множества M для неориентированных и ориентированных графов: центральности — степенная (связность), мостовая, близости, собственных векторов; максимальный размер кластера, кратчайшие пути, максимальные потоки, потоки минимальной стоимости и др., что позволяет применять модель для большинства социальных, биологических и технических объектов, причем в постановке задач, прежде не подвергавшихся анализу исследователей.

Этическая компонента модели изложена в [5], там же приведены результаты формирования сети с учетом этической составляющей.

Модель ***RT*** реализована в пакете Maple 12 в виде инструментального программного средства прогностического и описательного моделирования.

Основные результаты и выводы

В настоящей работе изучены и представлены два новых приближенных к реальности примера поведения комплексных сетей в поле угроз. Мы приняли в расчет то, что случайные сети являются в меньшей мере чувствительными к характеру атак, и то, что иерархические сети идеологически ориентированы на высокую защищенность узлов и связей. Поэтому для данного исследования мы остановили свой выбор в основном на безмасштабных сетях как наиболее характерных: выбор сетевой топологии определялся ее выразительностью для задач безопасности и современным звучанием. В каждом примере моделировались SF сети с показателем степенного закона $\gamma = 2$ и 1000 узлами.

Пример 1. Развитие данной модели позволяет провести имитацию атак в виде комбинированных угроз (R — случайной и I — целенаправленной) незащищенным узлам сети в прямой (R-угрозы + I-угрозы) и обратной (I-угрозы + R-угрозы) последовательности.

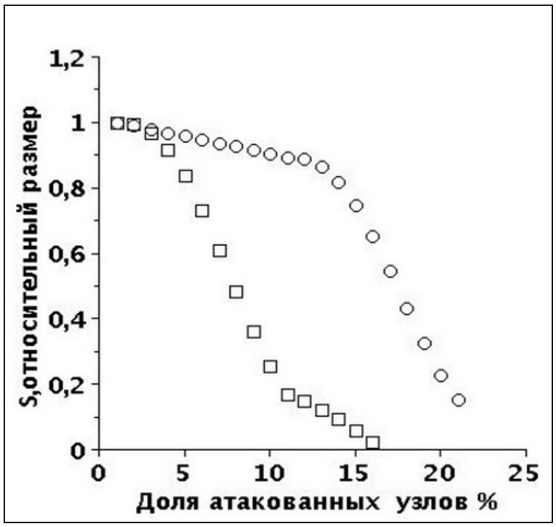


Рис. 3. Зависимость относительного размера максимального кластера в безмасштабных сетях, подвергнутых атакам в различной последовательности: I+R (□) и R+I(○)

На рис. 3 представлены результаты изменения такого показателя, как относительный размер максимального кластера, в зависимости от числа атакованных узлов безмасштабной сети. Видно, что атакующая комбинация I-R является более эффективной, нежели R-I.

В случае надежного опознавания целенаправленной атаки защитной стороне выгодна перестройка топологии сети с SF на E (размер дополнительно моделируемой экспоненциальной сети составлял также 1000 узлов) и с обратным переходом от экспоненциальной к безмасштабной с изменением характера атаки (Рис. 4).

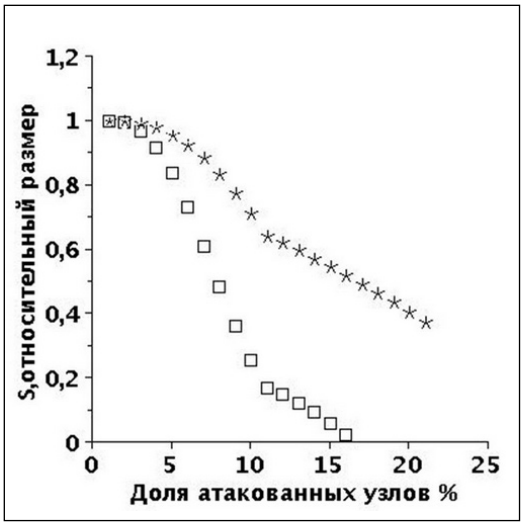


Рис. 4. Зависимость относительного размера максимального кластера в безмасштабной сети (□) и сети с перестройкой топологии: экспоненциальной + безмасштабной ( ), подвергнутой атакам в последовательности: I+R*

Примером уязвимой топологии может служить пример сети продовольственного снабжения Ленинграда в 1941 г. Тогда немецкая авиация произвела целенаправленную атаку — бомбовый удар по Бадаевским складам, что в значительной степени осложнило продовольственную ситуацию и оборону города в целом. В сознании ленинградцев пожар на Бадаевских складах стал символом начала голода 1941–1942 г. Рассредоточение запасов продовольствия — переход к топологии экспоненциальной сети — мог бы повысить стойкость сети снабжения.

Пример 2.

В данном примере исследовалась реакция безмасштабной сети на целенаправленные угрозы защищаемым элементам — узлам. Полагали, что вероятность успешной атаки на узел меняется только с изменением ρ уязвимости $_i$, которая уменьшается экспоненциально с увеличением «толщины» защитного барьера d_i, определяемого традиционным комплексом мер безопасности: морально-этическими, правовыми, организационными, техническими, физическими и математическими, и выражаемого величиной затрат, т. е. $d_i \sim F_i$, и в этом случае:

ρ уязвимости $_i \sim exp(-\mu F_i)$,

где μ — некий коэффициент, задающий эффективность использования финансовых средств.

На рис. 5 представлены зависимости относительного размера максимального кластера в безмасштабной сети при различных объемах равномерно распределенного по узлам финансирования защитных мероприятий ($F0_i = 0; F1_i = 1/\mu; F2_i = 2/\mu$).

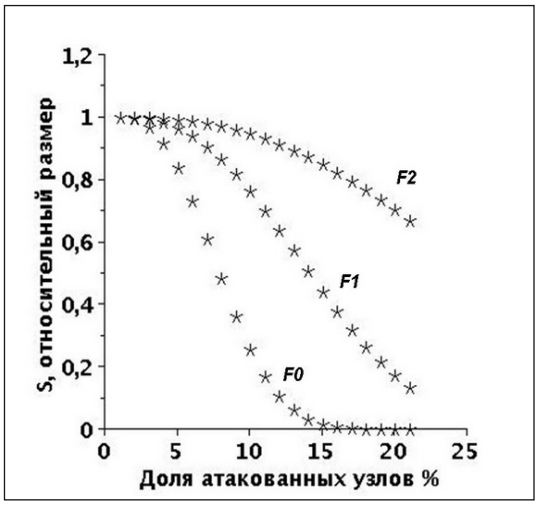


Рис. 5. Зависимость относительного размера максимального кластера в безмасштабной сети при различных объемах финансирования защитных мероприятий: $F0_i = 0; F1_i = 1/\mu; F2_i = 2/\mu$

На практике различные элементы сети — узлы и связи — защищены (финансируются) в разной степени. Так, обычно наиболее важные (в любом смысле) агенты сети защищаются в большей степени. Полагая, что стратегия безопасности определяет распределение средств между узлами, мы исследовали реакцию сети на угрозы для случаев:

а) отсутствия инвестиций: $F0_i = 0$;

б) трех возможных стратегий распределения инвестиций в защиту, которые зависят от степени узла (при одинаковом суммарном объеме):

$F1_i = Const\ (k_i) = 1/\mu; F2k_i = 1.9k_i/\mu; F2k2_i = 35\,k_i^2/\mu$

$$\sum_{i=1}^{1000} F1_i = \sum_{i=1}^{1000} F2k_i = \sum_{i=1}^{1000} F2k2_i$$

Предполагалось, что противоборствующей стороной использовалась классическая стратегия целенаправленных атак с последовательными атаками на узлы максимальной связности. Результаты расчетов изменения относительного размера максимального кластера для этих четырех вариантов защитной стратегии приведены на рис. 6.

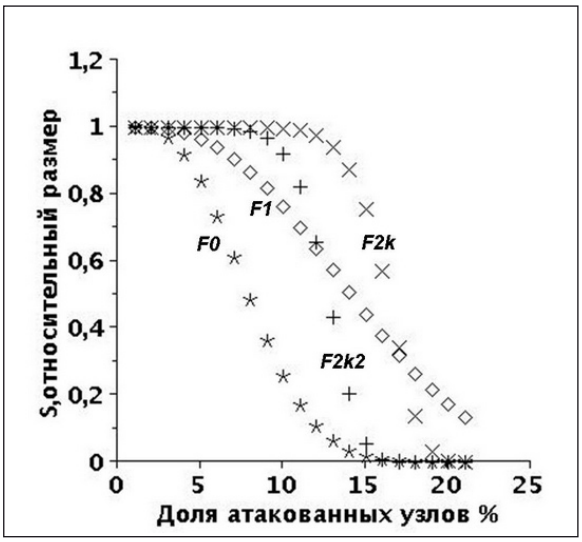


Рис. 6. Зависимость относительного размера максимального кластера в безмасштабной сети при различных защитных стратегиях мероприятий: $F0_i = 0; F1_i = 1/\mu; F2k_i = 1.9k_i/\mu; F2k2_i = 35\,k_i^2/\mu$

Видно, что стратегия с чрезмерной защитой узлов максимальной связности (т. е. $F_i \sim k_i^2$) не является оптимальной, такое поведение можно объяснить тем, что на защиту элементов меньшей степени попросту не хватает средств.

Выстраивая оптимальную стратегию защиты сети, обусловленную как выбором ее топологии, так и распределением ресурсов на защиту сетевых элементов, необходимо в максимальной степени верно оценивать стратегию и действия атакующей стороны. Практическое применение данного подхода нашло и находит свое отражение в функционирующих и проектируемых сетях [6, 7, 8].

В целом модель RT представляется мощным универсальным инструментом в области современных проблем безопасности разнообразных сетей — природного, социального и технического характера, инструментом, который позволяет эффективно подойти к решению широкого спектра задач стойкости практически значимых сетевых конструкций.

СПИСОК ЛИТЕРАТУРЫ:

1. *Erdos P., Renyi A.* Publ. Math. Inst. Hung. Acad. Sci. 5, 1960. P. 17–25.
2. *Barabási A.-L., Albert R., Jeong H.* Mean-field Theory for Scale-free Random Networks // Physica. 1999. A 272. P. 173–187.
3. *Albert R., Jeong H., Barabási A.-L.* Error and Attack Tolerance of Complex Networks // Nature. 2000. 406. P. 378–482.
4. *Петренко С. А., Симонов С. В.* Управление информационными рисками: Экономически оправданная безопасность. М.: АйТи-Пресс, 2004. – 381 с.
5. *Гурски Э., Галиндо Ф., Лапорт Р., Линкова Ф., Михайлов Н., Труфанов А., Журавлев Д., Россодивита А., Шубников Е., Николаева Н., Арефьева Е.* Роль этики в противодействии химическим, биологическим, радиационным и ядерным угрозам // Актуальные проблемы формирования культуры безопасности жизнедеятельности населения. Материалы XIII Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. 14–15 мая 2008 г. Москва, Россия. М.: ИПП «КУНА», 2008. С. 106–111.
6. *Тихомиров А. А.* Организация межотраслевого управления / Отв. ред. Н. Я. Петраков; АН СССР, Центр. экон.-мат. ин-т, Науч. совет по комплекс. пробл. «Оптимальное планирование и управление народным хозяйством». М.: Наука, 1986. – 112 с.
7. URL: http://www.pitt.edu/~super1/.
8. *Rossodivita A., Galindo F., Gursky E., LaPorte R., Linkov F., Shubnikov E., Stikova E., Trufanov A., Vinograd N.* Interagency Collaboration Topology for Counteracting Global Threats International Preparedness & Response to Emergencies & Disasters // Program and book of abstracts (11–14 January 2010, Tel Aviv, Israel). 2010. P. 78.