

АНАЛИЗ СИНЕРГЕТИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗОВ В СЛОЖНЫХ СЕТЕВЫХ СТРУКТУРАХ

Гребенюк Г.Г., Лубков Н.В., Рошин А.А., Середа Л.А.

*Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65*

grebenuk@lab49.ru, lbknv@mail.ru, rochinaa@mail.ru, sereda@lab49.ru

Аннотация: Рассматриваются синергетические последствия множественных отказов объектов сложных сетевых структур в обратной задаче уязвимости. Последствия от таких отказов зависят от состава отказавших объектов, их положения в структуре. Предлагается метод поиска «опасных» объектов, основанный на частотном анализе сечений с максимальными синергетическими последствиями.

Ключевые слова: уязвимость, сетевая инфраструктура, надежность энергоснабжения, синергетические последствия.

Введение

Внедрение новых открытий и достижений науки и техники, средств автоматизации и информационно-телекоммуникационных технологий в сетевые системы обеспечения промышленности, торговли и населения электроэнергией, водой и топливом, наряду с положительными эффектами, породили новые уязвимости в этих системах, добавив немало угроз для жизни и деятельности людей. Этим можно объяснить пристальное внимание к исследованию уязвимости сложных систем [1-5].

Уязвимость – параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными средствами или факторами, который понимается как характеристика элемента структуры, либо дефекта структуры или её элементов [6]. При такой интерпретации элемент называется уязвимостью системы, если отказ этого элемента имеет для этой системы большие негативные последствия.

Все воздействующие на объект факторы можно представить двумя группами - внутренние факторы, и факторы, внешние по отношению к объекту. Состав внутренних факторов зависит от конструкции объекта, технологии изготовления, используемых конструкционных материалов. Внешние факторы присутствуют в виде условий окружающей среды, в которой происходит функционирование объекта, а также технологических связей. Поэтому особо выделяют внешние факторы, соответствующие нормальным (нормативным, проектным) условиям применения объекта, при которых все характеристики исправного объекта соответствуют техническим требованиям. При отклонении параметров внешней среды от нормативных, в том числе при возникновении дополнительных внешних воздействий, уже не может гарантироваться не только работоспособность объекта, но и его целостность.

Исходными событиями, приводящими к отклонению параметров внешней среды от нормативных, могут быть:

- 1) природные явления (наводнения, циклоны, лесные пожары, засуха, сейсмическая активность);
- 2) действия злоумышленников;
- 3) воздействия со стороны других объектов системы, связанных с данным объектом технологически или территориально.

Воздействия со стороны других объектов системы предопределяют возможность возникновения в системе цепных отказов.

Анализ последствий от отказов тех или иных объектов и их комбинаций позволяет обнаружить уязвимости в сложной системе и принять меры к повышению ее надежности. К таким мерам, в частности, относятся резервирование, частичное или полное обновление и др.

Причины уязвимости могут скрываться в топологии системы, которая, к примеру, может иметь низкий уровень резервирования ответственных объектов, в географическом расположении ее элементов, подверженных ураганам и наводнениям, неудачной логике работы системы управления и др.

В системах большой размерности количество объектов и их сочетаний, подлежащих исследованию последствий отказов, может достигать десятков тысяч. Так в [7] при анализе уязвимости распределительной сети 11 кВ исследовано более 300 тысяч двойных и более 80 тысяч тройных отказов.

Основные стратегии выбора отказывающихся объектов сети основаны на анализе достижимости оставшихся работоспособных объектов из источников ресурсов. Достижимость вершины графа из

вершины-источника понимается как существование пути между ними. При этом выбирается такая стратегия, в которой минимальное множество повреждаемых объектов обеспечивает изоляцию от источников максимального множества других объектов сети. При решении данной задачи широко применяются методы топологического анализа сетевых систем, представленных в виде графа.

Искомые отказавшие объекты определяются с учетом характеристик графа сети или случайным образом.

Указанным способом решается прямая задача поиска уязвимостей. В прямой задаче при оценке последствий важное значение имеет синергетический эффект от одновременного отказа (множественного отказа) нескольких объектов. Под синергетическим эффектом здесь понимается явление, возникающее при одновременном отказе нескольких объектов сети, следствие от которого превышает суммарные последствия от отказов каждого из этих объектов.

В исследованиях уязвимости сложных технико-экономических систем, наряду с прямой, рассматривается также обратная задача – поиск тех объектов сети, от которых зависит снабжение ресурсами не всех, а некоторой группы потребителей. [8]. В обратной задаче задано множество потребителей, как правило, важных объектов промышленности, транспорта, пунктов управления, гражданской инфраструктуры и других, так называемых целевых объектов (далее ЦО). Фактически, в обратной задаче рассматривается уязвимость целевых объектов в смысле снижения их работоспособности теми или иными способами [6], в том числе включая отказы сетевых объектов.

В данной работе при решении обратной задачи уязвимости рассматривается синергетика отказов и роль сетевых элементов в надежности и безопасности снабжения ресурсами целевых объектов.

Решение обратной задачи сводится к построению минимальных сечений, каждое из которых отключает указанное множество целевых объектов от источников ресурса, их ранжированию по воздействию на ЦО и поиску значимых для уязвимости ЦО объектов сечений.

1 Постановка задачи

Рассматривается сетевая система, граф которой содержит множество вершин:

$$W = R \cup P \cup C, \quad (1)$$

где R – источники ресурса, P – объекты потребления ресурса и C – объекты сети, передающие или преобразующие ресурсы (трансформаторные, насосные и другие подстанции, электрические линии, трубопроводы, распределительные устройства, отпайки), образующие технологическую сеть.

Обозначим через P_z подмножество потребителей P , представляющее собой заданный набор ЦО, $P_z \subseteq P$.

Необходимо отделить множество источников R от множества целевых объектов P_z , что достигается построением минимальных сечений. Множество минимальных сечений обозначим как

$$F = \{F^1, \dots, F^N\}, \text{ где } N \text{ – число сечений, а } F^k = \{c_1^k, \dots, c_l^k\} \text{ – } k \text{-ое минимальное сечение.}$$

Требуется определить «опасные» объекты, входящие в состав минимальных сечений с высокими синергетическими последствиями, но не создающие значительных последствий при собственном отказе. В дальнейшем будем предполагать, что последствия отказов измеряются количеством объектов, отключенных от сети.

В дальнейшем, для простоты будем говорить «полный отказ сечения» при отказе всех его объектов и «частичный отказ сечения» при отказе части его объектов.

2 Схема решения задачи

Схема решения задачи состоит из следующих основных этапов:

- 1) поиск минимальных сечений с ограничением по их мощности;
- 2) расчет синергетических последствий и выбор сечений с высокой их долей
- 3) отбор объектов с учетом синергетических последствий сечений п.2.

2.1 Поиск минимальных сечений

Поиск минимальных сечений для сетей высокой размерности (сотни и тысячи вершин) требует больших вычислительных ресурсов, в том числе для хранения и анализа сечений, число которых измеряется миллионами. Существует несколько методов расчета сечений [9-10]. Как правило, все они требуют предварительного определения безызбыточных путей между источниками ресурсов и объектами их потребления, для получения сечений затем используется алгоритм Петрика или метод совпадающих множеств, основанный на построении HS-дерева [10] и др.

В данной работе использовался метод поиска минимальных сечений, основанный на специальной разметке графа, принципы работы которого изложены в [11] и развиваемый ниже.

Для оценки суммарных последствий частичного отказа сечения необходимо подсчитать количество потребителей, лишившихся питания необходимыми им ресурсами в результате удаления из графа сети вершин, соответствующих отказавшим объектам.

Если сеть однородная, т. е. от источников к потребителям в ней передается единственный ресурс (например, если это электрическая передающая сеть), то все подходящие к вершине графа сети ребра можно считать равноправными: вершина может получать ресурс по любому из них. В этом случае для выяснения, питается ли какой-либо потребитель, достаточно проверить наличие хотя бы одного пути к этому потребителю от любого источника после удаления из графа заданного набора вершин. Проще всего это сделать, итеративно разметив граф от источников в направлении ребер. В первой итерации во все вершины-источники помещается метка, после чего эти вершины добавляются в обрабатываемый в следующей итерации список. В каждой следующей итерации все еще не помеченные вершины, смежные с вершинами из текущего списка в направлении ребер, тоже помечаются и добавляются в список для следующей итерации. Итерации заканчиваются, когда список для следующей итерации становится пустым. После этого подсчитывается количество не помеченных ЦО, т. е. тех вершин, к которым не оказалось ни одного пути от какого-либо источника.

Если сеть – гетерогенная, т. е. в ней передается несколько ресурсов, то ребра, входящие в вершины графа сети, нельзя считать равноправными. В зависимости от внутреннего устройства объектов сети, которым соответствуют вершины, может оказаться, что для работы объекта одновременно нужно несколько ресурсов (например, для работы электрического насоса необходимы вода и электричество). Могут быть и более сложные ситуации: часть необходимых объекту ресурсов могут иметь альтернативы (например, котел может успешно работать как на газе, так и на мазуте), а часть – таких альтернатив не иметь (в котел обязательно должна поступать вода, и заменить ее ничем). В этом случае простая проверка наличия путей от источников к потребителям не может служить признаком работоспособности потребителя: не всем потребителям нужно соединение со всеми источниками, и некоторым из них необходимо соединение сразу с несколькими источниками.

Для вершины графа гетерогенной сети необходимость различных ресурсов можно описать логической функцией работоспособности: одновременно необходимые ресурсы или группы ресурсов объединяются оператором «И», а альтернативные – оператором «ИЛИ». В этом случае для выяснения наличия необходимого питания у объектов-потребителей также можно использовать разметку графа, но процедура разметки будет более сложной.

Каждой вершине графа приписывается набор логических признаков обеспеченности каждым из передающихся в сети ресурсов, и исходно все эти признаки считаются истинными, т. е. все вершины считаются обеспеченными всеми необходимыми ресурсами. Из графа удаляются вершины исследуемого сечения, после чего проводится разметка в двух вложенных циклах итераций. Во внешнем цикле перебираются все ресурсы сети с переходом к первому после рассмотрения последнего, а во внутреннем цикле граф размечается только по выбранному ресурсу.

Для каждого рассматриваемого во внешнем цикле ресурса во все вершины-источники этого ресурса помещается метка, которая затем во внутреннем цикле распространяется по графу так же, как было описано выше для однородной сети, но при этом рассматриваются только ребра, передающие выбранный ресурс. После того, как разметка по ресурсу окончена, во всех вершинах, не получивших метки, сбрасываются признаки обеспеченности данным ресурсом и вычисляются логические функции работоспособности. Все вершины, для которых функция дает ложное значение, удаляются из графа – для них уже известно, что необходимого питания они не получают. Далее для разметки выбирается следующий ресурс, и внешний цикл продолжается.

Внешний цикл необходимо остановить в том случае, если в очередной раз были перебраны все ресурсы сети, но ни одна вершина из графа удалена не была. Это значит, что питание всех вершин графа всеми ресурсами уже определено, и дальнейшие итерации уже ничего не изменят. Условие остановки рано или поздно будет выполнено: удаление вершин может привести только к лишению питания других вершин, т. е. к новым удалениям вершин из графа, и общее число рассматриваемых вершин может только уменьшаться. Таким образом, оно либо уменьшится до нуля, либо стабилизируется на некотором значении в течение нескольких итераций, что и приведет к остановке цикла. После этого суммарными последствиями частичного отказа объектов из выбранного сечения будет общее количество ЦО, удаленных из графа в процессе разметки.

2.2 Расчет синергетических последствий и выбор сечений с высокой их долей

Почему важны исследования синергетики в сетевых структурах?

Во-первых, синергетические последствия определяют реальную роль сетевого объекта в структуре сети, его влияние на ее уязвимость. Это влияние в отсутствие оценки синергетических последствий равно последствиям отказа самого сетевого объекта, что чаще всего нетрудно определить и поэтому используется на практике для принятия мер по повышению надежности к объектам с повышенными последствиями одиночного отказа. При этом упускаются из рассмотрения объекты с незначительными последствиями отказа, как малозначимые для сохранения эффективности сетевой структуры, предназначенной для передачи ресурсов от их источников к потребителям.

Исследования, выполненные в [7], говорят о том, что большинство множественных отказов не обладает синергетическим эффектом и последствия индивидуальных отказов не увеличиваются при действии в компании с другими отказами.

При множественных отказах роль сетевого объекта может измениться ввиду того, что часть множественных отказов может создавать синергетический эффект. В таких отказах сетевой объект с незначительными последствиями индивидуального отказа в компании с другими отказавшими сетевыми объектами вызовет значительные негативные последствия. В этом случае влияние отказа указанного объекта на эффективность структуры сети может резко увеличиться, и, в таком случае, он должен рассматриваться в качестве приоритетного для принятия мер по повышению надежности сетевой структуры. Собственно, такие выводы следуют из анализа сетевой системы, выполненного в [7].

Во-вторых, выявление синергетических последствий является важным для построения системы защиты от преднамеренных негативных действий, поскольку дает знания о влиянии сетевого объекта на уязвимость сетевой системы.

В [7] рассматривалась прямая задача уязвимости, для которой множество отказов системы F , состоит из n элементов ($n > 1$): $F = \{c_1, \dots, c_n\}$. Множество F разделяется на подмножества S , представляющие собой отказы различной кратности. Это разбиение выполняется p разными способами, каждый из которых обозначен V_i . Каждое разбиение V_i представлено следующим образом:

$$V_i = \{S_1^i, \dots, S_m^i\}, \quad \text{где } m \text{ количество подмножеств в } i\text{-ом разбиении.}$$

Множественный отказ F имеет синергетические последствия тогда и только тогда, когда общие последствия $C(F)$ больше, чем сумма последствий всех подмножеств каждого из разбиений V_i ($i=1..p$):

$$C(F) > \sum_{j=1}^m C(S_j^i) \forall V_i. \quad (2)$$

Синергетические последствия $C_{syn}(F)$ множественного отказа F вычисляются как разница между последствиями отказа F и наибольшей суммой последствий отказов отдельных подмножеств S_1^i, \dots, S_m^i среди всех разбиений V_i :

$$C_{syn}(F) = C(F) - \max_{V_i} \left(\sum_{j=1}^m C(S_j^i) \right), \quad (3)$$

где $C(S_j^i)$ – последствия отказа подмножества S_j^i разбиения V_i сечения множества отказов F .

Доля синергетических последствий множественного отказа F определяется как отношения синергетических последствий к общим последствиям:

$$f_{syn}(F) = \frac{C_{syn}(F)}{C(F)}. \quad (4)$$

В обратной задаче в качестве множества отказов рассматриваются сечения, отделяющие ЦО от источников ресурса.

Нарушение работоспособности объектов сети приводит к снижению выходного эффекта объектов потребления, который определяется суммарным объемом ресурсов, получаемых этими объектами. При этом предполагается, что объекты получают ресурс, если существует технологическая цепочка, соединяющая их с источниками ресурса.

Сетевые объекты, также как и объекты потребления, могут находиться в двух состояниях – работоспособном или не работоспособном. Для объектов потребления работоспособность определяется получением или неполучением ресурса. В обратной задаче негативные последствия отказа всех объектов любого сечения одинаковы и равны числу ЦО.

Для обеспечения безопасности целевых объектов решается задача поиска минимальных сечений в графе сети. Такие сечения включают два типа объектов: объекты, одиночный отказ которых вносит существенный вклад в последствия отказа сечения, и объекты сечения, потеря работоспособности которых сама по себе не вызывает заметных последствий, но приводит к серьезным последствиям при потере работоспособности объектов всего сечения.

Очевидно, что обнаружение объектов первого типа является тривиальной задачей, и надежности их функционирования и так уделяется повышенное внимание. Поиск объектов второго типа, напротив, является проблемой, и необходимо уделить особое внимание именно этой задаче.

Для обнаружения объектов второго типа предлагается ранжировать все найденные минимальные сечения по доле синергетических последствий.

Необходимо доказать утверждение: сечение с большими долями синергетических последствий содержит хотя бы одну вершину c_1, \dots, c_n , которая представляет собой объект второго типа.

Будем считать большими синергетические последствия множественного отказа F в случаях, когда их доля не ниже некоторого порога A , т.е.:

$$\frac{C_{syn}(F)}{C(F)} \geq A. \quad (5)$$

Подставив в формулу (5) выражение (3) для расчета синергетических последствий, получим:

$$C(F)(1 - A) \geq \max_{V_i} \left(\sum_{j=1}^m C(S_j^i) \right). \quad (6)$$

Найдется такое разбиение V_i , при котором $\sum_{j=1}^m C(S_j^i)$ будет максимальной, тогда

$$C(F)(1 - A) \geq \sum_{j=1}^m C(S_j^k). \quad (7)$$

Рассмотрим одно из подмножеств k -го разбиения (с номером t), тогда:

$$C(S_t^k) \leq C(F)(1 - A) - \sum_{j=1, j \neq t}^m C(S_j^k). \quad (8)$$

Таким образом, было найдено ограничение сверху на величину последствий отказа t -го подмножества k -го разбиения сечения F . Из полученного выражения видно, что с ростом порога A максимально возможное значение величины последствий t -го подмножества k -го разбиения уменьшается. Одиночный отказ объектов, входящих в состав подмножества S_t^k , не превышает последствий самого подмножества, поэтому также ограничен сверху значением (8).

Полученный результат является доказательством утверждения, т.к. при больших синергетических последствиях (см. выше) и при значительных последствиях отказов остальных объектов (больших $\sum_{j=1, j \neq t}^m C(S_j^k)$) разность (8) уменьшается, что означает, что в сечении существует объект с незначительными последствиями отказа. А при незначительных последствиях отказов остальных объектов (малых $\sum_{j=1, j \neq t}^m C(S_j^k)$) объект с незначительными последствиями находится среди этих остальных объектов.

Ниже предлагается подход к отбору наиболее «опасных» объектов в составе сечений.

2.3 Отбор объектов с учетом синергетических последствий

Выбор значимых объектов в сети осуществляется с использованием частотного анализа объектов сечений. В составе отобранных минимальных сечений осуществляется поиск наиболее часто встречающегося объекта. Затем из списка отобранных сечений удаляются все сечения, содержащие найденный объект, и процедура поиска повторяется.

Таким образом, получается ранжированный список «опасных» объектов, рекомендованных для защиты от воздействий.

3 Пример

Рассмотрим граф электрической сети, состоящей из 20 вершин (см. рис. 1), включающий 2 источника (вершины 16,18), 3 целевых объекта (вершины 12, 19, 20) и 15 промежуточных объектов.

Заключение

Выполнен анализ проблемы уязвимости в сетевых технологических структурах, даны два варианта постановки задач – прямой и обратной задачи оценки уязвимости.

Показаны особенности расчета последствий отказов в сложных сетевых структурах для прямой и обратной задач оценки уязвимости.

Обоснована целесообразность и показана возможность учета синергетических последствий отказов сетевых объектов для выявления среди них наиболее уязвимых, представляющих в случае отказа опасность для снабжения ресурсами целевых потребителей и нуждающихся в принятии мер по их защите.

На фрагменте электрической сети иллюстрируются все этапы схемы решения обратной задачи уязвимости, определяются сетевые объекты, представляющие опасность для функционирования целевых потребителей.

Литература

1. *Eusgeld I., Kröger W., Sansavini G., et al.* The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures // *Reliability Engineering and System Safety*. – 2009. – Vol. 94. – P. 954–963. – URL: <http://www.sciencedirect.com/science/article/pii/S0951832008002639>
2. *Rosas-Casals M.* Topological Complexity of the Electricity Transmission Network. Implications in the Sustainability Paradigm / PhD Thesis Universitat Politècnica de Catalunya. – Autumn, 2009. – URL: <http://www.tesisenred.net/bitstream/handle/10803/5824/TMRC1de1.pdf>
3. *Wang W.* Defending against multifaceted attacks in wireless networks and power grid networks / University of Rhode Island, 2011 URL: http://dfcsc.uri.edu/docs/Wenkai_Dissertation.pdf
4. *Rosas-Casals M., Valverde S., Solé R.V.* Topological vulnerability of the European power grid under errors and attacks. – URL: http://upcommons.upc.edu/e-prints/bitstream/2117/6179/6/vulnerabilitat_xarxa_DEF_revisat.pdf
5. *Кондратьев А.* Современные тенденции в исследовании критической инфраструктуры в зарубежных странах // *Зарубежное военное обозрение*. – 2012. – № 1. – С. 19–30.
6. *Johansson J., Hassel H.* An approach for modelling interdependent infrastructures in the context of vulnerability analysis // *Reliability Engineering and System Safety* - 2010. - Vol. 95, No 12. - P. 1335-1344.
7. *Jönsson H., Johansson J., Johansson H.* Identifying critical components in technical infrastructure networks // *Proceedings of the Institution of Mechanical Engineers. Part O: Journal of Risk and Reliability*. - 2008. Vol. 222, No. 2 - P. 235-243.
8. *Grebenyuk G. G. Nikishov S. M.* Block of energy and resources supplies targets in the network infrastructure // *Control Issues*. – 2016.- №4.-p.52-57.
9. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. – СПб.: Изд-во СПб. гос. ун-та, 2007. – 276 с.
10. *Haenni R.* Generating Diagnoses from Conflict Sets. – URL: www.aai.org/Papers/FLAIRS/1998/FLAIRS98-081.pdf
11. *Grebenyuk G.G., Dorri M, Kh., Roshchin A.A., Nikishov S.M.* A study of influence of the structure of Heterogeneous Engineering Networks on the Reliable Operation of Large Consumes // *Proceedings of the 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017, Moscow)*. М.: IEEE, 2017. Vol. 2. - P. 57-61.