ИССЛЕДОВАНИЕ ВЛИЯНИЯ АТАК НА СТРУКТУРНЫЕ И ПАРАМЕТРИЧЕСКИЕ МЕТРИКИ СЕТЕЙ С АДАПТИВНОЙ ТОПОЛОГИЕЙ

Павленко Е. Ю.[1]

Цель статьи: *анализ чувствительности структурных и параметрических метрик сетей с адаптивной топологией к компьютерным атакам различного типа.*

Методы исследований: *системный анализ существующих структурных метрик для оценки состояния компьютерных сетей, теоретическая формализация, проведение эксперимента.*

Результат: *предложенный подход позволил на практике получить оценку влияния различного рода компьютерных атак, специфичных для сетей с адаптивной топологией, в частности, атаки типа испытание бессонницей, атаки «воронка» и атаки Сивиллы. Практическое моделирование адаптивной сетевой инфраструктуры с использованием теории графов позволило получить уникальный набор данных, позволяющий вычислять как структурные, так и параметрические методы оценки состояния сети. Также предложенный подход, сочетающий единовременную оценку структурных и параметрических метрик для узлов сети, продемонстрировал гибкость в части распознавания различных сетевых атак, часть из которых нагляднее проявляется в сетевом трафике, а другая часть – в изменениях в топологии сети. Расширение предложенного подхода в части используемых метрик позволит оценивать безопасность текущего состояния сети на трех уровнях: на уровне всей сети или ее отдельных сегментов (структурные метрики), на уровне только критических узлов (структурные и параметрические метрики) и на уровне отдельных устройств (параметрические метрики).*

Научная новизна: *посредством имитационного моделирования с использованием теории графов создан новый набор данных, содержащий характеристики функционирования сетей с адаптивной сетевой топологией в нормальных условиях и под воздействием специфичных компьютерных атак. Ключевым отличием от известных имитационных моделей динамических сетей и сформированных на их основе наборов данных является возможность одновременного анализа сетевых данных, которыми обмениваются узлы, физических показателей работы узлов и структуры сети.*

Ключевые слова: *Компьютерные атаки, сети с адаптивной топологией, метрики центральности, уровень сигнала, интеллектуальные сети электроснабжения, атака «воронка», атака Сивиллы.*

DOI:10.21681/2311-3456-2023-4-65-71

Введение

С развитием технологической инфраструктуры усложняется и сетевая топология: сетевое взаимодействие носит динамический и адаптивный характер, узлы способны инициировать новые взаимодействия с учетом текущей ситуации в сети, кооперироваться для перераспределения нагрузки и выполнять различные функции в разные моменты времени (например, узел сети может быть как приемником, так и передатчиком, а в ряде случаев и агрегатором передаваемой информации).

В последние годы наблюдается не только увеличение числа атак, но и появление их новых типов, свойственных, в частности, сетям с адаптивной топологией (динамическим сетям). Целью настоящей статьи является исследование метрик, которые бы позволили выявить различные типы атак на сети с адаптивной топологией. Значительный интерес представляют как метрики, характеризующие структуру сети, так и метрики, связанные с параметрами отдельных узлов сети. Такими параметрами могут быть как информационные параметры – используемые сетевые порты, пропускная способность узла сети и т.п., так и физические параметры – уровень заряда батареи, уровень сигнала устройства и прочие аналогичные параме-

1 Павленко Евгений Юрьевич, кандидат технических наук, доцент Института кибербезопасности и защиты информации, Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия. E-mail: pavlenko_eyu@spbstu.ru, ORCID: 0000-0003-1345-1874

тры, значимые в силу киберфизической природы динамических сетей.

В работе освещен вопрос моделирования сетей с адаптивной топологией на примере интеллектуальной сети электроснабжения Smart Grid [1-3], сеть представляется в виде неориентированного графа и включает различные типы устройств. Также проведены три типа атак на сеть, исследованы различные метрики с точки зрения их чувствительности к атакам.

В рамках проведенных исследований использованы методы теории графов для выделения репрезентативного набора метрик, чувствительных к изменениям в структуре графа, моделирующего сеть с адаптивной топологией.

1. Анализ существующих исследований

Обеспечение безопасности современных систем, построенных на базе одноранговых и децентрализованных сетей с адаптивной топологией, базируется, в первую очередь, на обнаружении атак, в том числе, на ранней стадии и с применением интеллектуальных технологий. Этому направлению посвящено значительное число работ [4-8]. Несмотря на большое число исследований, они не ориентированы на единовременное обнаружение аномалий информационной и физической составляющих сложных систем, в том числе, с адаптивной сетевой топологией.

Часть исследовательских работ сосредоточена на обнаружении киберугроз, характерных именно для систем, построенных на базе динамических сетей [9-11]. Эти исследования посвящены созданию подходов к обнаружению специфичных атак типа «черная дыра» и выделению вредоносных узлов сети, однако они не предоставляют информации о том, какие параметры адаптивных сетей могут отреагировать на различные типы атак.

Перспективным подходом видится анализ состояния сети в целом, а не только отдельных узлов: комплексное понимание того, как изменяется ситуация в сети, позволит распознавать как новые типы атак, так и деструктивные воздействия на ранней стадии. Для этого требуется исследовать, какие именно метрики, характеризующие структуру графа, моделирующего адаптивную сеть, способны реагировать на различные типы атак (в том числе, специфичные для ad hoc сетей).

Использование таких структурных метрик в сочетании с параметрическими метриками отдельных узлов (например, критических – через которые проходит наибольшее число потоков информации) и анализом сетевого трафика при подключении средств искусственного интеллекта способно существенно повысить уровень безопасности динамических сетей и сложных систем, построенных на их основе.

Следует отметить малое число наборов данных, содержащих информацию о состоянии динамических сетей, в частности, ad hoc. Еще меньше таких наборов данных содержат сведения об атаках на сеть и о поведении сети при реализации атак. Многие исследовательские работы, посвященные обеспечению безопасности сетей с адаптивной сетевой топологией, используют достаточно давно опубликованные наборы данных, такие как KDD-99 [12, 13].

Различные исследования по моделированию атак на динамические сети включают моделирование с использованием сетевых симуляторов ns-2 и ns-3, однако графы, построенные с использованием таких симуляторов, недостаточно репрезентативны с точки зрения структурных метрик всей сети или ее части, а также параметрических метрик отдельных узлов.

В связи с этим, данная работа состоит из двух основных частей: моделирования сети с адаптивной топологией и оценки структурных и параметрических метрик для смоделированной сети в различных состояниях (без атак и при атаках).

2. Проведение моделирования

2.1 Моделирование сети с адаптивной топологией

Сеть с адаптивной топологией смоделирована в виде неориентированного графа, имитирующего работу сетевой инфраструктуры энергетической системы Smart Grid, в соответствии с источником[2] (рисунок 1).

Сетевая топология представляет собой дерево, листьями которого являются простейшие устройства – сенсоры и умные счетчики, назначение которых в измерении параметров энергопотребления и передаче этих данных другим узлам – повторителям, для последующей агрегации на узлах-концентраторах [14].

Адаптивность сетевой топологии ограничена типами устройств, входящих в нее: возможно перераспределение данных от сенсоров, измерителей и повторителей между различными концентраторами, а также периодическая активация связи между повторителем и конечным измеряющим устройством в случае ухудшения сигнала. Число устройств в сети остается конечным, в рамках моделирования оно составляет

2 Hartmann, T. Generating realistic smart grid communication topologies based on real-data / T. Hartmann, F. Fouquet, J. Klein, Y. Le Traon, A. Pelov, L. outain, T. Ropitault //2014 IEEE International Conference on Smart Grid Communications (SmartGridComm). — 2014. — P. 428-433.

50 узлов. Число связей между узлами (ребер) варьируется, однако в тех случаях, когда длительность связи между узлами составляет менее 30 секунд, они не отображаются в графе и не используются для дальнейшего анализа.

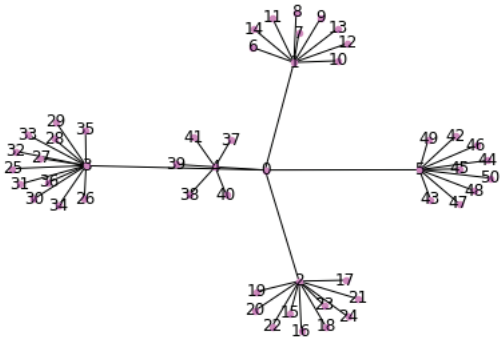

Рис. 1. Смоделированная сеть в виде графа

На рисунке 1 заметны узлы с повышенной центральностью, характеризующие собой концентраторы, собирающие данные от более простых по функционалу узлов. Рисунок 1 характеризует сеть в ее начальном состоянии, в дальнейшем структура сети менялась – как в связи с изменениями в энергопотреблении, так и в связи с атаками.

2.1 Моделирование атак на сеть

На сеть были смоделированы следующие типы кибератак:

1. Испытание бессонницей – атака состоит в повышении мощности работы целевого узла путём вынуждения его производить дополнительные действия. Цель атаки – израсходовать энергию целевого узла, запасённую в его источнике питания.

2. Атака «воронка», Sinkhole, состоящая в изменении поведения скомпрометированного узла в сети таким образом, чтобы он стал перенаправлять на себя весь трафик сети [15]. Цель атаки – получить весь трафик на узел, подконтрольный злоумышленнику.

3. Атака Сивиллы – атака, заключающаяся в использовании скомпрометированным узлом нескольких лжеидентификаторов, чтобы выдавать себя за несколько узлов сети [15]. Цель атаки – нарушить процессы маршрутизации, агрегации данных в сети.

Возможные признаки атак, как структурные, так и параметрические, описаны в таблице 1.

4. Эксперимент

На рисунках представлены графы, характеризующие изменения, происходящие в сети, во время реализации каждой атаки. Следует отметить, что атаки происходили в различные моменты времени, и сетевая топология в силу своей динамичности не всегда соответствовала изначальной, представленной на рисунке 1.

На рисунках 2.а и 2.б представлены графы, моделирующие сеть до атаки испытанием бессонницей и при атаке испытанием бессонницей.

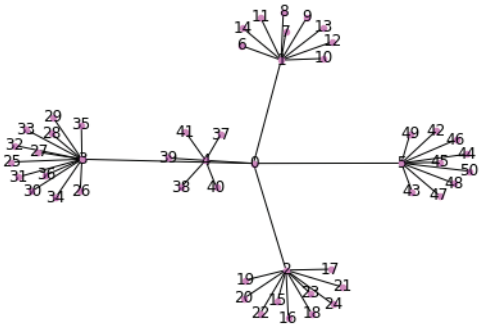

Рис. 2.а – Граф сети до атаки «испытание бессонницей»

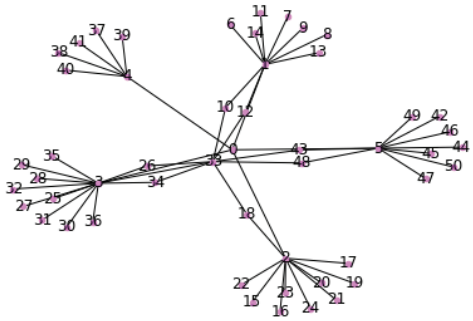

Рис. 2.б – Граф сети при реализации атаки «испытание бессонницей»

На рисунке 3.а показана динамика значения метрики центральности PageRank для атакуемого узла №33 («pagerank_two_normal», «pagerank_two_anomaly») и узла №31, аналогичного по функциям атакуемому узлу («pagerank_one_normal», «pagerank_one_anomaly»). Виден нестабильный рост значения метрики для узла №33 при одновременном снижении диапазона значений метрики для узла №31.

Аналогичное исследование метрики центральности по степени узла было еще более наглядным (рисунок 3.б), здесь видно увеличение числа соединений с узлом №33 («degree_cent_two_normal», «degree_cent_two_anomaly») по сравнению с узлом №16. Он находился в другом сегменте сети, поэтому атака его никак не затронула, что видно из рисунка 3.б – его

Таблица 1

Атаки и их возможные признаки

Атака	Возможные структурные и параметрические признаки атаки
Испытание бессонницей	• увеличение степени вершины; • уменьшение заряда батареи устройства; • ухудшение качества сигнала от устройства.
Атака «воронка»	• повышение качества сигнала устройства; • увеличение степени вершины, соответствующей скомпрометированному узлу; • снижение степени вершин, соседних со скомпрометированным узлом и обладающих хорошими характеристиками (сигналом и зарядом) и ранее высокой степенью.
Атака Сивиллы	• появление и сохранение на протяжении некоторого времени новых ребер в графе; • увеличение диаметра графа за счет неоптимальной маршрутизации в сети.

показатели центральности по степени («degree_cent_one_normal», «degree_cent_one_anomaly») не изменились.

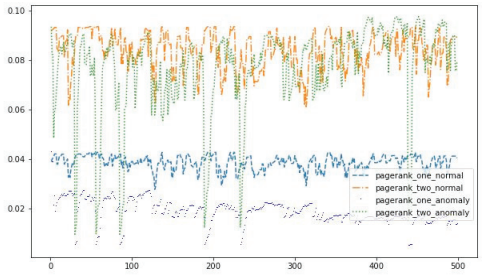

Рис. 3.а – Динамика метрики центральности PageRank

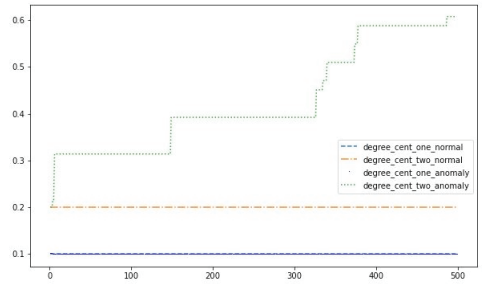

Рис. 3.б – Динамика метрики центральности по степени вершин

При анализе параметрических метрик атакуемого устройства №33 (рисунок 4) было заметно уменьшение заряда батареи, причем, попытки системы восстановить уровень заряда устройства нивелировались атакой, чем и объясняются скачки на графике.

На рисунках 5.а и 5.б представлены графы, моделирующие сеть до атаки «воронки» и при атаке «воронки».

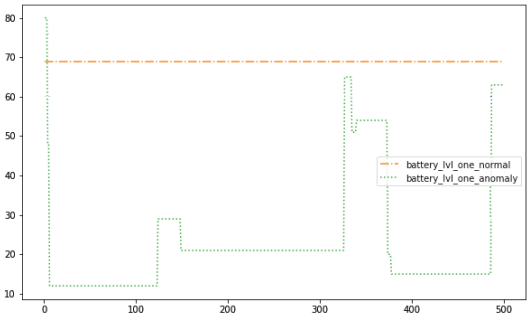

Рис. 4 – Динамика параметра «уровень заряда батареи»

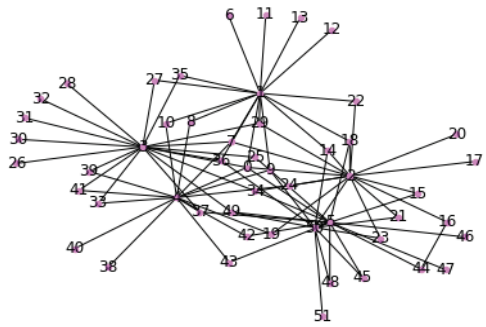

Рис. 5.а –Граф сети до атаки «воронка»

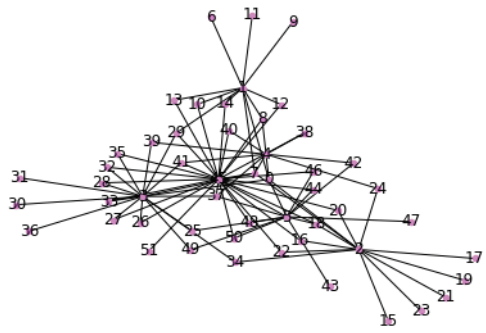

Рис. 5.б – Граф сети при реализации атаки «воронка»

Из рисунков 5.а и 5.б видно, что если до атаки в графе было несколько вершин с высокой степенью, через которые передавались данные, то при реализации атаки увеличилась степень узла №3, уменьшилась степень узла №2 и значительно выросла степень узла №37, фактически, он стал центром графа.

Исследован показатель центральности по степени близости (рисунок 6) для узла №31, который атака не затронула, и для узла №37, скомпрометированного в результате атаки «воронки». На рисунке 6 линии, соответствующие устройству «one», характеризуют центральности узла №31 до (degree_cent_one_normal) и после атаки (degree_cent_one_anomaly) и узла №37 до (degree_cent_two_normal) и после атаки (degree_cent_two_anomaly). Видно, что центральность узла 31 практически не менялась, в то время как изменения для узла №37 значительные.

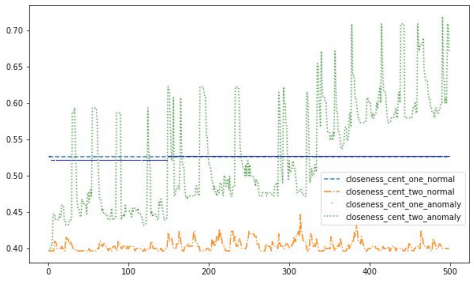

Рис. 6 – Динамика показателей центральности по степени близости

Показатель «качество сигнала» также отреагировал на атаку, однако его динамика на графике получилась нерепрезентативной, поскольку в сравнении с другими узлами, у которых также менялся уровень сигнала, изменения были не столь значительными.

На рисунках 7.а и 7.б представлены графы, моделирующие сеть до атаки Сивиллы и после атаки.

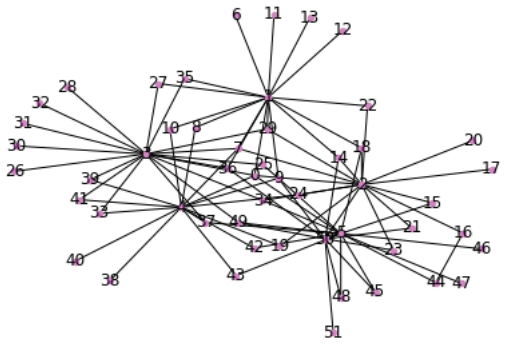

Рис.7.а – Граф сети до атаки Сивиллы

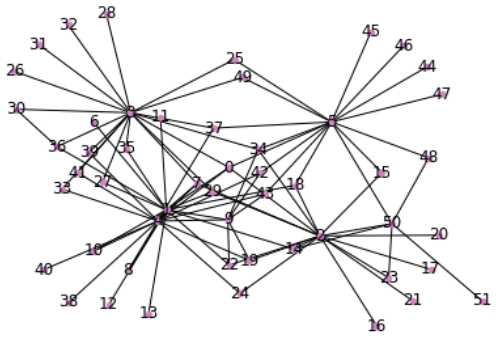

Рис. 7.б – Граф сети при реализации атаки Сивиллы

Для атаки Сивиллы различие в графах, представленных на рисунках 7.а и 7.б, не такое явное, как в случаях с другими атаками. Однако в графе на рисунке 7.б появились небольшие циклы, описываемые последовательностью вершин: 3-30-36-3, 2-50-23-2, что свидетельствует о нарушениях в процессе маршрутизации.

При этом параметрический анализ графовых метрик не позволил получить каких-либо явных отклонений, выбивающихся из общей картины.

Выводы

Таким образом, авторами статьи достигнут положительный эффект в области исследования подходов к распознаванию специфичных атак на сети с адаптивной топологией, достигаемый за счет экспериментальной оценки и моделирования.

Результаты проведенной работы, состоящей в моделировании сети с адаптивной сетевой топологией в нормальном состоянии и при реализации на нее атак, позволили выделить структурные и параметрические метрики, чувствительные к атакам. К ним отнесены структурные метрики центральности (по степени вершин, по степени близости и PageRank) и параметрическая метрика «уровень заряда батареи».

В статью не вошли результаты, связанные с метриками, которые не оказались показательными для обнаружения атак на сеть. В частности, это метрики радиуса и диаметра графа, а также метрика «уровень сигнала» устройств.

Исходя из того, что изменения в структуре графа при атаке можно заметить визуально, дальнейшим направлением исследования является подключение нейронных сетей для обработки визуального представления графов и попытки с их помощью классифицировать изображения графа на те, которые соответствуют сети в нормальном состоянии и сети под атакой.

Исследование выполнено за счет гранта Российского научного фонда № 22-21-20008, https://rscf.ru/project/22-21-20008/.

Исследование выполнено за счет гранта Санкт-Петербургского научного фонда в соответствии с соглашением от «15» апреля 2022 г. № 61/220

Литература

1. Macana C. Cyber Physical Energy Systems Modules for Power Sharing Controllers in Inverter Based Microgrids / C. Macana, A. Abdou, H. Pota, J. Guerrero, J. Vasquez // Inventions. – 2018. – Vol. 3. – № 3. – P. 1-21.
2. Liang Y. Smart Grid Project Benefit Evaluation Based on a Hybrid Intelligent Model / Y. Liang, Y. Fan, Y. Peng, H. An // Sustainability. – 2022. – Т. 14. – №. 17. – P. 10991.
3. Mohanty S. Demand side management of electric vehicles in smart grids: A survey on strategies, challenges, modelling, modeling, and optimization / S. Mohanty, S. Panda, S. M. Parida, P. K. Rout, B. K. Sahu, M. Bajaj, H. M. Zawbaa, N. M. Kumar, S. Kamel //Energy Reports. – 2022. – Т. 8. – С. 12466-12490.
4. Павленко Е.Ю. Распознавание киберугроз на адаптивную сетевую топологию крупномасштабных систем на основе рекуррентной нейронной сети / Е.Ю. Павленко, Н.В. Гололобов, Д.С. Лаврова, А.В. Козачок // Вопросы кибербезопасности. – 2022. - №6(52). – С. 93-99.
5. Петренко А. С. Система обнаружения аномалий функционирования технологических платформ цифровой экономики / А. С. Петренко, С. А. Петренко // Информационные системы и технологии в моделировании и управлении: Сборник материалов III Всероссийской научно-практической конференции с международным участием, посвященной 100-летию Крымского федерального университета имени В.И. Вернадского, Ялта, 21–23 мая 2018 года / Ялта: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2018. – С. 199-204. – EDN UVTHBC.
6. Branitskiy A. Applying artificial intelligence methods to network attack detection / A. Branitskiy, I. Kotenko // Intelligent Systems Reference Library. – 2019. – Vol. 151. – P. 115-149. – DOI 10.1007/978-3-319-98842-9_5. – EDN MAYKTJ.
7. Шелухин О. И. Модификация алгоритма обнаружения сетевых атак методом фиксации скачков фрактальной размерности в режиме Online / О. И. Шелухин, С. Ю. Рыбаков, А. В. Ванюшина // Труды учебных заведений связи. – 2022. – Т. 8. – №. 3. – С. 117-126.
8. Кононов Р. В. Многоклассовая классификация сетевых атак методами интеллектуального анализа / Р. В. Кононов, О. И. Шелухин // Телекоммуникации и информационные технологии. – 2022. – Т. 9, № 1. – С. 11-16. – EDN AMBLME.
9. Abdelhamid A., Elsayed M. S., Jurcut A. D., & Azer M. A. A Lightweight Anomaly Detection System for Black Hole Attack. Electronics. – 2023. – 12(6), 1294.
10. Tangade S., Kumaar R. A., Malavika S., Monisha S., & Azam F. Detection of Malicious Nodes in Flying Ad-hoc Network with Supervised Machine Learning. In 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE). – 2022. – Pp. 1-5. IEEE.
11. Gupta C., Singh L., & Tiwari R. Wormhole attack detection techniques in ad-hoc network: A systematic review. Open Computer Science. – 2022. – 12(1), 260-288.
12. Feng F., Liu X., Yong B., Zhou R., & Zhou Q. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks. – 2019. – 84, 82-89.
13. Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. Anomaly-based behavioral detection in mobile Ad-Hoc networks. Procedia Computer Science. – 2019. – 159, P. 77-86.
14. Srinivas, V. L., Wu, J. Topology and parameter identification of distribution network using smart meter and μPMU measurements / V. L. Srinivas, J. Wu // IEEE Transactions on Instrumentation and Measurement. – 2022. – №71. – P. 1-14.
15. Свинцов Ю.А. Проблемы безопасности в беспроводной сенсорной сети-обзор. Проблемы науки 4 (52). – 2020 – С. 28-31.

STUDY OF THE EFFECT OF ATTACKS ON STRUCTURAL AND PARAMETRIC METRICS OF NETWORKS WITH ADAPTIVE TOPOLOGY

***Pavlenko E.Y.*[3]**

The purpose of the article: *analysis of sensitivity of structural and parametric metrics of networks with adaptive topology to computer attacks of different types.*

Main research methods: *system analysis of existing structural metrics to assess the state of computer networks, theoretical formalization, conducting an experiment.*

3 Evgeniy Yu. Pavlenko, Ph.D., Associate Professor, Institute of Cyber Security and Information Protection, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: pavlenko_eyu@spbstu.ru, ORCID: 0000-0003-1345-1874

Result: *the proposed approach allowed us to estimate in practice the impact of various types of computer attacks, specific to networks with adaptive topology, in particular, insomnia type attacks, sinkhole and Sybil attacks. Practical modeling of adaptive network infrastructure using graph theory has yielded a unique dataset that allows us to compute both structural and parametric methods for assessing network state. Also, the proposed approach, which combines the simultaneous estimation of structural and parametric metrics for network nodes, demonstrated flexibility in terms of recognizing various network attacks, some of which are more clearly manifested in network traffic, and another part in changes in the network topology. Extension of the proposed approach in terms of used metrics will allow to evaluate the security of the current state of the network at three levels: at the level of the entire network or its individual segments (structural metrics), at the level of critical nodes (structural and parametric metrics) and at the level of devices (parametric metrics).*

Scientific novelty: *by means of simulation using graph theory a new data set has been created, which contains the characteristics of networks with adaptive network topology functioning in normal conditions and under the influence of specific computer attacks. The key difference from the known simulation models of dynamic networks and the data sets formed on their basis is the ability to simultaneously analyze the network data exchanged by nodes, the physical performance of the nodes and the structure of the network.*

Keywords: Computer attacks, networks with adaptive topology, centrality metrics, signal level, Smart Grid networks, sinkhole attack, Sybil attack

References

1. Macana C. Cyber Physical Energy Systems Modules for Power Sharing Controllers in Inverter Based Microgrids / C. Macana, A. Abdou, H. Pota, J. Guerrero, J. Vasquez // Inventions. – 2018. – Vol. 3. – № 3. – P. 1-21.
2. Liang Y. Smart Grid Project Benefit Evaluation Based on a Hybrid Intelligent Model / Y. Liang, Y. Fan, Y. Peng, H. An // Sustainability. – 2022. – T. 14. – №. 17. – P. 10991.
3. Mohanty S. Demand side management of electric vehicles in smart grids: A survey on strategies, challenges, modelling, modeling, and optimization / S. Mohanty, S. Panda, S. M. Parida, P. K. Rout, B. K. Sahu, M. Bajaj, H. M. Zawbaa, N. M. Kumar, S. Kamel //Energy Reports. – 2022. – T. 8. – C. 12466-12490.
4. Pavlenko E.YU. Raspoznavanie kiberugroz na adaptivnuyu setevuyu topologiyu krupnomasshtabnyh sistem na osnove rekurrentnoj nejronnoj seti / E.YU. Pavlenko, N.V. Gololobov, D.S. Lavrova, A.V. Kozachok // Voprosy kiberbezopasnosti. – 2022. - №6(52). – S. 93-99.
5. Petrenko A. S. Sistema obnaruzheniya anomalij funkcionirovaniya tekhnologicheskih platform cifrovoj ekonomiki / A. S. Petrenko, S. A. Petrenko // Informacionnye sistemy i tekhnologii v modelirovanii i upravlenii: Sbornik materialov III Vserossijskoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem, posvyashchennoj 100-letiyu Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo, YAlta, 21–23 maya 2018 goda / YAlta: Obshchestvo s ogranichennoj otvetstvennost'yu «Izdatel'stvo Tipografiya «Arial», 2018. – S. 199-204. – EDN UVTHBC.
6. Branitskiy A. Applying artificial intelligence methods to network attack detection / A. Branitskiy, I. Kotenko // Intelligent Systems Reference Library. – 2019. – Vol. 151. – P. 115-149. – DOI 10.1007/978-3-319-98842-9_5. – EDN MAYKTJ.
7. Sheluhin O. I. Modifikaciya algoritma obnaruzheniya setevyh atak metodom fiksacii skachkov fraktal'noj razmernosti v rezhime Online / O. I. SHeluhin, C. YU. Rybakov, A. V. Vanyushina // Trudy uchebnyh zavedenij svyazi. – 2022. – T. 8. – №. 3. – S. 117-126.
8. Kononov R. V. Mnogoklassovaya klassifikaciya setevyh atak metodami intellektual'nogo analiza / R. V. Kononov, O. I. SHeluhin // Telekommunikacii i informacionnye tekhnologii. – 2022. – T. 9, № 1. – S. 11-16. – EDN AMBLME.
9. Abdelhamid A., Elsayed M. S., Jurcut A. D., & Azer M. A. A Lightweight Anomaly Detection System for Black Hole Attack. Electronics. – 2023. – 12(6), 1294.
10. Tangade S., Kumaar R. A., Malavika S., Monisha S., & Azam F. Detection of Malicious Nodes in Flying Ad-hoc Network with Supervised Machine Learning. In 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE). – 2022. – Pp. 1-5. IEEE.
11. Gupta C., Singh L., & Tiwari R. Wormhole attack detection techniques in ad-hoc network: A systematic review. Open Computer Science. – 2022. – 12(1), 260-288.
12. Feng F., Liu X., Yong B., Zhou R., & Zhou Q. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks. – 2019. – 84, 82-89.
13. Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. Anomaly-based behavioral detection in mobile Ad-Hoc networks. Procedia Computer Science. – 2019. – 159, P. 77-86.
14. Srinivas, V. L., Wu, J. Topology and parameter identification of distribution network using smart meter and μPMU measurements / V. L. Srinivas, J. Wu // IEEE Transactions on Instrumentation and Measurement. – 2022. – №71. – P. 1-14.
15. Svincov YU.A. Problemy bezopasnosti v besprovodnoj sensornoj seti-obzor. Problemy nauki 4 (52). – 2020 – C. 28-31.