Научная статья
УДК 621.39
https://doi.org/10.31854/1813-324X-2026-12-2-92-101
EDN:LWPUOU

Анализ последствий атак на элементы системы синхронизации, функционирующие по алгоритму BTCA на основе протокола точного времени

Евгений Валерьевич Опарин[1], onapuh@mail.ru
Федор Алексеевич Прошин[2] ✉, fedorproshin@gmail.com

[1]ЗАО «Институт телекоммуникаций»,
Санкт-Петербург, 194100, Российская Федерация
[2]Петербургский государственный университет путей сообщения Императора Александра I,
Санкт-Петербург, 190031, Российская Федерация

Аннотация

Протокол точного времени получил широкое распространение во многих сферах, включая такие критически важные отрасли, как энергетический и промышленный комплексы, экономика и связь – где точность синхронизации является необходимым условием функционирования. Несвоевременность получения данных, вызванная возникновением отклонения шкалы времени, может привести к неисправности, что недопустимо. Общедоступность данного протокола делает его привлекательным для потенциального нарушителя, который может вмешаться в работу устройств. Следовательно, все большую актуальность приобретает задача выявления подобных воздействий на начальном этапе с целью недопущения дальнейшего рассогласования системы.

Цель: *исследовать вероятные стратегии атак на элементы системы синхронизации, функционирующие по алгоритму поиска лучшего источника; на основе сформированных стратегий атак разработать имитационные модели функционирования элементов системы синхронизации в условиях воздействия атак.*

Методы: *сбор, систематизация и анализ научно-технической информации, имитационное моделирование с применением агентного подхода.*

Результаты: *разработан комплекс имитационных моделей процесса функционирования элементов системы синхронизации, функционирующих по алгоритму поиска лучшего источника в условиях воздействия информационных атак.*

Теоретическая значимость: *на основе комплекса разработанных моделей возможно отслеживать состояния портов устройств протокола точного времени, определять время сходимости алгоритма поиска лучшего источника и в целом отслеживать процесс функционирования элементов системы синхронизации, исходя из атрибутов портов устройств, характеристик каналов связи и различных стратегий проведения атак.*

Практическая значимость. *Полученные результаты могут быть использованы на реальных сетях связи для выявления скомпрометированных устройств системы синхронизации при наличии информации о характеристиках узлов связи. Имея в наличии статистику оценки времени сходимости алгоритма поиска лучшего источника и сведения о состоянии портов устройств, можно сделать вывод о вероятных объектах атаки и предпринять шаги по ликвидации деструктивных воздействий.*

Ключевые слова: *сетевая синхронизация, BTCA, PTP, протокол точного времени, злоумышленник, атака*

Ссылка для цитирования: Опарин Е.В., Прошин Ф.А. Анализ последствий атак на элементы системы синхронизации, функционирующие по алгоритму BTCA на основе протокола точного времени // Труды учебных заведений связи. 2026. Т. 12. № 2. С. 92–101. DOI:10.31854/1813-324X-2026-12-2-92-101. EDN:LWPUOU

Original research
https://doi.org/10.31854/1813-324X-2026-12-2-92-101
EDN:LWPUOU

An Analysis of a Sequence to Attacks on Synchronization System Elements Operating According to BTCA Based on Precision Time Protocol

Evgeniy V. Oparin[1], onapuh@mail.ru
Fedor A. Proshin[2] ✉, fedorproshin@gmail.com

[1]Institute of Telecommunications JSC,
St. Petersburg, 194100, Russian Federation
[2]Emperor Alexander I St. Petersburg State Transport University,
St. Petersburg, 190031, Russian Federation

Annotation

Precision time protocol is widely common in different areas that include critically significant industries such as power generation, manufacturing, economics and communication where high accuracy is the necessary provision for its working. Time offset can causes delays in data receiving that potentially leads to faults. Precision time protocol is a quite attractive for malicious user to interfere in equipment functioning because of its accessibility. Therefore, preventable detecting of such actions is one of the actual goals for defending from faults.

The objective *is to research possible attack strategies on the elements of the synchronization system operating according to the best time transmitter clock algorithm, and to form simulation models of the functioning of the elements of the synchronization system under the influence of attacks based on the formed attack strategies.*

Methods include *collection, systematization and analysis of scientific and technical information, simulation using an agent-based approach.*

Results. *A complex of simulation models of the functioning of synchronization system elements operating according to the best time transmitter clock algorithm under the influence of information attacks are developed.*

The theoretical significance *is that a complex of developed models makes it possible to monitor the port status of precision time protocol's devices to determine the convergence time of the best time transmitter clock algorithm, and generally, to monitor the functioning of synchronization system elements based on the attributes of device ports, characteristics of communication channels, and various attack strategies.*

The practical significance *is that the obtained results can be used for real communication networks to identify anomaly synchronization system devices in the presence of information about the characteristics of communication nodes. When we have the statistics on the estimation of the convergence time of the best time transmitter clock algorithm and information on the status of device ports, it is possible to draw a conclusion about the objects for attacking and to take steps for eliminating destructive influences.*

Keywords: *network synchronization, BTCA, PTP, precision time protocol, attacker, attack*

For citation: Oparin E.V., Proshin F.A. An Analysis of a Sequence to Attacks on Synchronization System Elements Operating According to BTCA Based on Precision Time Protocol. *Proceedings of Telecommunication Universities.* 2026;12(2):92–101. (in Russ.) DOI:10.31854/1813-324X-2026-12-2-92-101. EDN:LWPUOU

Введение

Протокол точного времени (PTP, *аббр. от англ.* Precision Time Protocol) представляет собой пакетно-ориентированный протокол, спроектированный для точной синхронизации распределенных часов с разрешением менее микросекунды и работающий, в основном, по Ethernet или IP. Согласно стандарту IEEE Std 1588-2019 [1], протокол

PTP обеспечивает точность синхронизации в сети выше 1 мкс (до 10 нс). Процесс функционирования PTP основан на обмене сообщениями, передающими необходимую информацию в виде меток времени.

Функционирование протокола PTP может быть концептуально разделено на два этапа. На первом этапе устройства PTP логически самоорганизуются в иерархическое дерево синхронизации с использованием алгоритма поиска лучшего источника (BTCA, *аббр. от англ.* Best Time Transmitter Clock Algorithm). В сети связи устройства PTP постоянно обмениваются друг с другом качественными характеристиками своих внутренних часов. Устройство PTP с часами самого высокого качества в системе в конечном итоге берет на себя роль Грандмастера (GM, *аббр. от англ.* Grandmaster) и выполняет функции источника времени для всей сети связи. На втором этапе осуществляется непрерывная передача меток времени от GM вниз по иерархии устройств сети связи [1–3].

Полная иерархия дерева синхронизации целиком формируется отдельными узлами PTP, которые решают, в каком состоянии должен находиться каждый порт, просматривая сообщения Announce, которые узел получает от других портов PTP, находящихся в состоянии «Master».

Алгоритм BTCA состоит из двух независимых алгоритмов [1, 4]:

– алгоритм сравнения набора данных (*от англ.* data set comparison algorithm);

– алгоритм определения состояния (*от англ.* the state decision algorithm).

Алгоритм сравнения набора данных основывается на попарном сравнении атрибутов портов узлов со следующими приоритетами [1, 4]:

– *priority1*: атрибут, задаваемый пользователем, который описывает, что генератор находится в перечне генераторов, из которых выбирается ведущий (Master);

– *clockClass*: атрибут, определяющий отслеживание часами международного атомного времени (TAI, *аббр. от англ.* International Atomic Time);

– *clockAccuracy*: атрибут, определяющий точность часов;

– *offsetScaledLogVariance*: атрибут, определяющий стабильность часов;

– *priority2*: атрибут, задаваемый пользователем, который описывает более тонкое упорядочивание среди одинаковых часов;

– *clockIdentity*: дополнительный параметр.

Алгоритм определения состояния вычисляет, будет ли следующее состояние порта установлено как «Master», «Slave», или «Passive», основываясь на результатах алгоритма сравнения набора данных. Цель BTCA – определить состояние каждого порта системы PTP. Это определение основано на информации, содержащейся в сообщениях синхронизации, полученных портами, и на заданных по умолчанию значениях данных для узлов системы PTP.

Алгоритм BTCA работает независимо для каждых часов в системе PTP, то есть часы не согласовывают, какие из них должны быть ведущими, а какие ведомыми. Вместо этого каждый вычисляет только свое собственное состояние, при этом BTCA избегает конфигураций с двумя ведущими, или без них [1, 4, 5].

Результат работы BTCA существенно зависит от информации, находящейся в сообщениях Announce, и отсутствие координации между узлами во время выбора ведущих устройств делают участников PTP уязвимыми для атак, связанных с процессом функционирования данного алгоритма.

При атаке на элементы системы синхронизации, функционирующие по BTCA на основе протокола PTP, злоумышленник, завладев отдельным узлом PTP, может вмешаться в процесс выбора ведущего устройства, заявляя преувеличенные и неверные характеристики скомпрометированного узла, и, став ведущим, манипулировать синхронизацией всех ведомых устройств [6–8].

Манипулирование содержимым сообщения Announce при организации процесса функционирования алгоритма BTCA

Полная иерархия дерева синхронизации полностью формируется отдельными узлами PTP, которые решают, в каком состоянии должен находиться каждый порт, просматривая сообщения Announce, которые узел получает от других портов PTP, находящихся в состоянии «Master».

Для моделирования атаки на элементы системы синхронизации, функционирующие по BTCA на основе протокола PTP, рассмотрим простую топологию, где исходные данные для моделирования представлены в виде сети связи (рисунок 1).

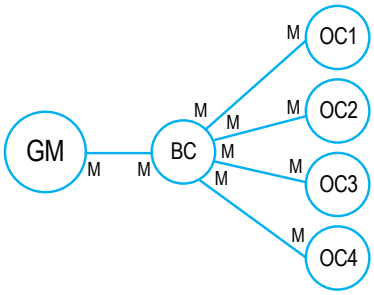

Рис. 1. Сеть PTP, находящаяся в исходном состоянии

Fig. 1. PTP Network in the Initial State

Сеть связи на рисунке 1 содержит одно устройство уровня GM. Дополнительно она состоит из граничных часов (BC, *аббр. от англ.* Boundary Clock), а также из обычных часов (OC, *аббр. от англ.* Ordinary

Clock), которые выступают потребителями сигналов точного времени. В качестве исходных данных для моделирования также выступают состояния портов устройств. Условно считаем, что изначально порты всех устройств находятся в состоянии «Master» и осуществляют рассылку сообщений Announce [1, 9, 10].

Главным итогом работы BTCA должно быть такое состояние портов устройств, чтобы обеспечить создание дерева синхронизации и передачу меток времени потребителям. Любой порт PTP в состоянии «Master» периодически отправляет сообщения Announce на общий адрес групповой рассылки PTP. Поля в этом сообщении содержат атрибуты портов и устройств, используемые алгоритмом BTCA для определения состояния портов. Указанные атрибуты портов и устройств представлены в таблице 1 [1, 11].

ТАБЛИЦА 1. Атрибуты портов и устройств, используемые алгоритмом BTCA для определения состояния портов

TABLE 1. Per-Port and Per-System Attributes That are Used in BTCA for Port Initialization

Поле	Значение
priority1	0–255
clockClass	6–255
clockAccuracy	17–31
clockVariance	000016–FFFE16
priority2	0–255
clockIdentity	глобально уникальный номер в 8 октетах
portNumber	1–255
stepsRemoved	0–255

Определение состояния портов осуществляется путем поэтапного сравнения атрибутов. Проведем моделирование процесса функционирования реализации BTCA для примера сети связи, показанного на рисунке 1, при нормативных условиях, а также в условиях атаки манипулирования содержимым сообщения Announce.

Для проведения имитационного моделирования зададим изначально значения атрибутов портов устройств (таблица 2). Отметим в качестве замечания, что значения атрибутов «*clockVariance*» и «*clockIdentity*» приведены к десятичному виду. В качестве критерия функционирования BTCA примем время сходимости. Под временем сходимости BTCA будем понимать время, когда определено состояние последнего порта рассматриваемой сети. В итоге имитационная модель для оценки процесса функционирования алгоритма BTCA примет вид, показанный на рисунке 2 [1, 11–15]. Дополнительно заданы переменные «Port_N_N», в которых будет отражено значение порта по окончании процесса функционирования BTCA.

ТАБЛИЦА 2. Значения атрибутов портов устройств рассматриваемой сети

TABLE. 2. Per-Port Attribute Values for the Given Network

Поле	GM	BC	OC1	OC2	OC3	OC4
priority1	3	16	32	32	32	32
clockClass	6	20	32	40	44	44
clockAccuracy	17	25	50	53	56	56
clockVariance	0	25	50	58	62	62
priority2	0	25	50	64	70	70
clockIdentity	0	16	50	52	54	54
portNumber	1	1	1	1	1	1
stepsRemoved	0	1	2	2	2	2

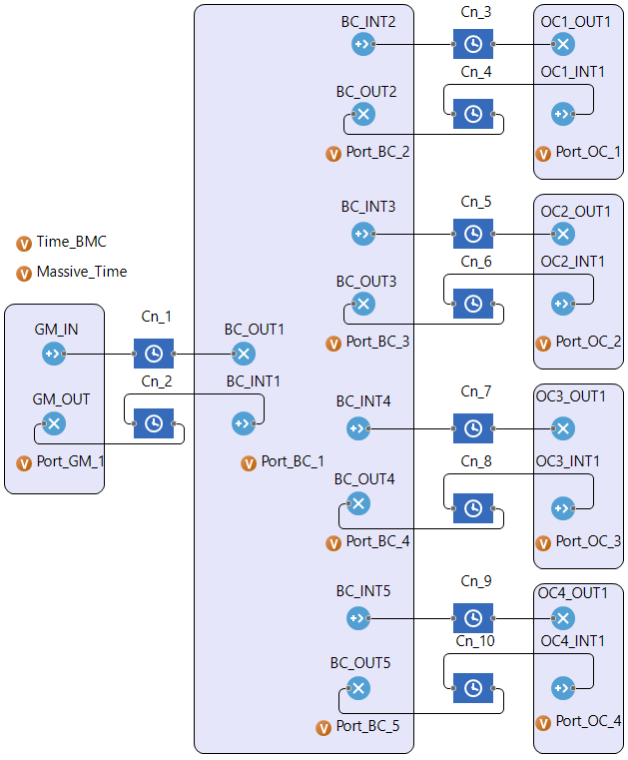

Рис. 2. Сетевая модель работы домена сети PTP при выполнении алгоритма BTCA

Fig. 2. The Network Model of PTP Domain Functioning in Accordance with BTCA

Построенная модель также позволяет производить оценку процесса функционирования BTCA в зависимости от характеристик каналов передачи данных, которые заданы соответствующими блоками задержек. Переменная *Massive_Time* содержит массив времен определения состояния портов по каждому каналу, переменная *Time_BMC* представляет собой время сходимости алгоритма BTCA. Атрибуты портов устройств рассматриваемой сети заданы как параметры агентов и при проведении процесса моделирования записываются в соответствующие переменные [1, 12, 15]. При передаче сообщения Announce, т. е. при прохождении агента по

каналу происходит отработка алгоритма сравнения атрибутов портов устройств. После отработки алгоритма сравнения атрибутов портов устройств происходит определение состояния каждого порта. Время определения состояния соответствующего порта записывается в массив *Massive_Time*, после обработки которого происходит определение времени сходимости алгоритма BTCA. При отсутствии атаки на элементы системы синхронизации и корректном функционировании алгоритма BTCA состояния портов устройств примут вид, как показано на рисунке 3. По результатам моделирования определены состояния портов устройств в соответствии с заданными атрибутами устройств, а также определено время сходимости алгоритма BTCA, которое составило 6,807 мкс.

В случае, если злоумышленник контролирует какое-либо из устройств PTP, он в состоянии подменить содержимое сообщений Announce, а значит вмешаться в процесс работы BTCA. Рассмотрим случай, когда злоумышленник контролирует узел ОС4. В данном случае он в состоянии подменить значения атрибутов портов устройства ОС4, например, присвоить атрибуту «*priority1*» значение 2, которое станет минимальным из всех устройств. Результат моделирования указанного случая показан на рисунке 4, из которого видно, что изменились состояния портов устройств PTP, а значит изменились маршруты доставки сигналов точного времени. Также следует отметить, что увеличилось время сходимости алгоритма BTCA (12,998 мкс), данный факт связан с тем, что потребовалась дополнительная отправка сообщения Announce в направлении устройства GM.

Построенная модель позволяет отслеживать состояния портов устройств PTP, определять время сходимости алгоритма BTCA и в целом отслеживать процесс его функционирования, исходя из атрибутов портов устройств и характеристик каналов связи, что может являться основой для фиксации и выявления возможных атак на домены PTP.

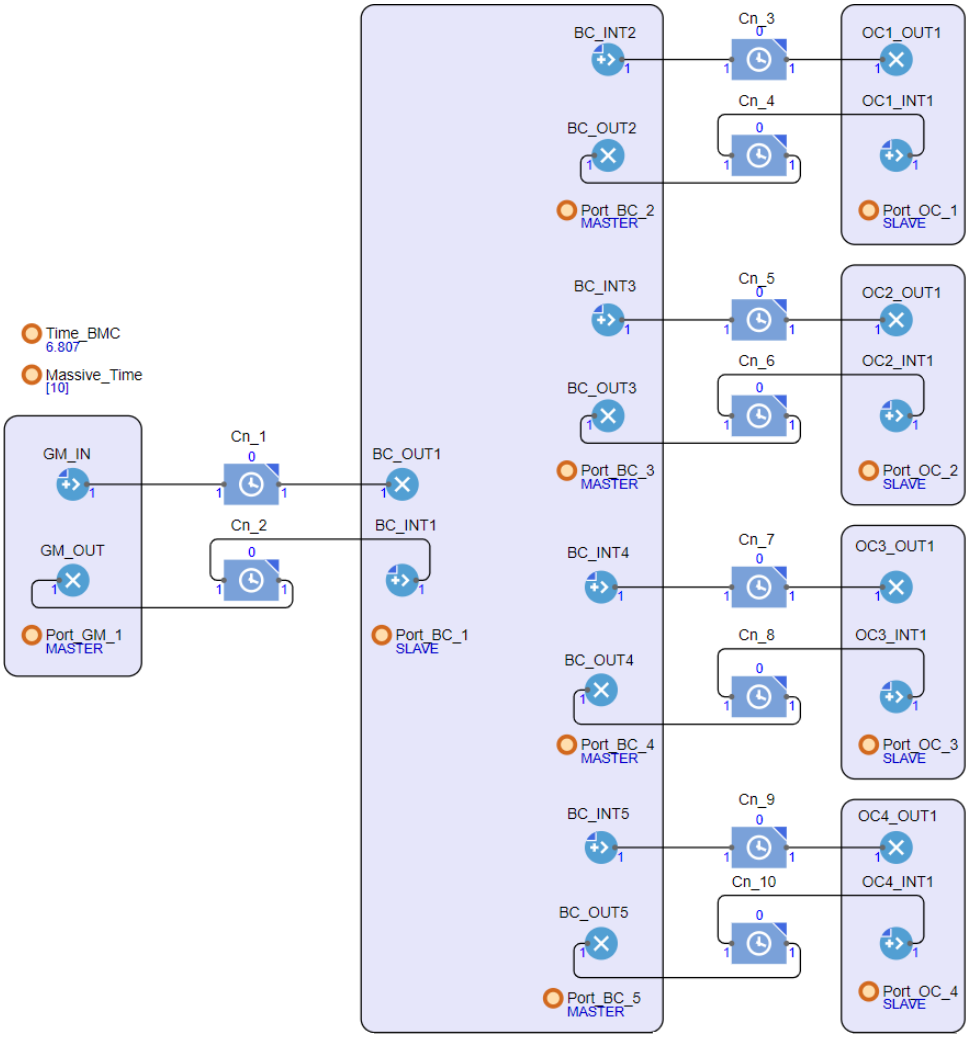

Рис. 3. Результат моделирования процесса функционирования алгоритма BTCA при отсутствии атаки на элементы системы синхронизации

Fig. 3. The Results of BTCA Functioning Model without Attack on Network Elements

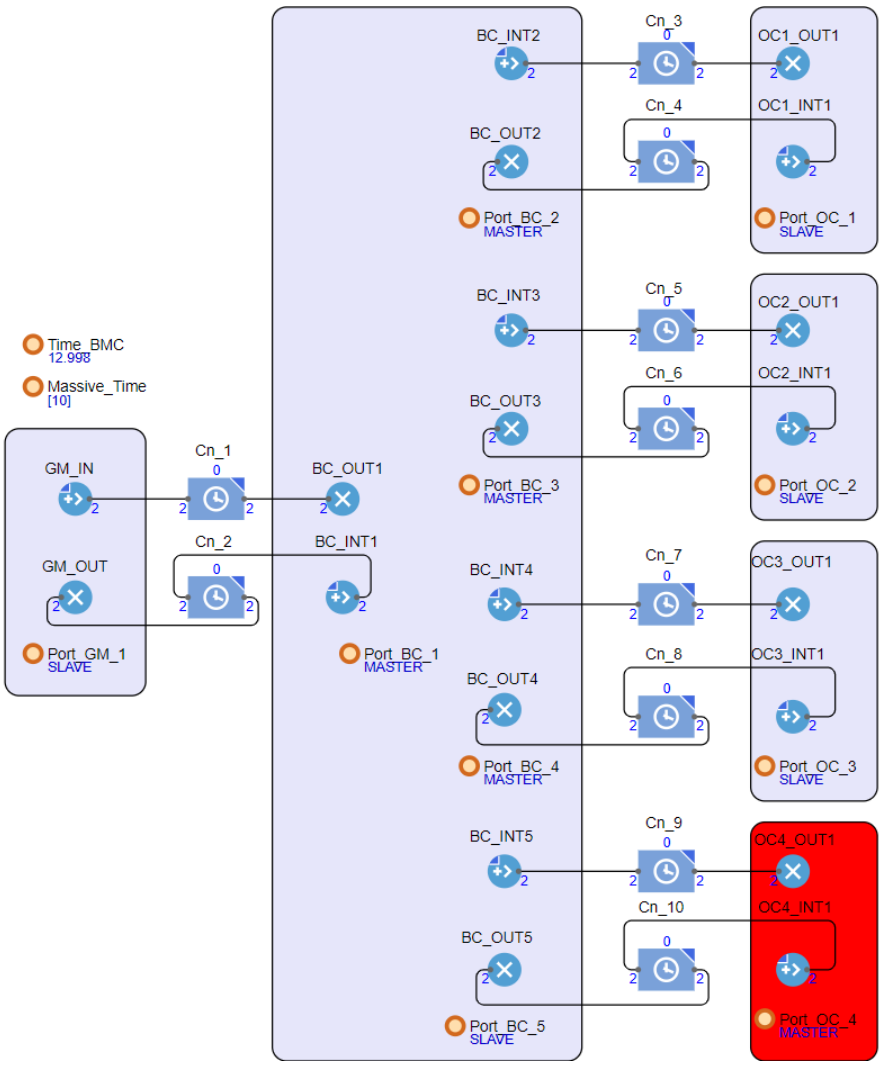

Рис. 4. Результат моделирования процесса функционирования алгоритма BTCA в случае контроля злоумышленником узла ОС4

Fig. 4. The Results of BTCA Functioning Model with Node OC4 Controlled by Attacker

Манипулирование задержкой сообщения Announce при организации процесса функционирования алгоритма BTCA

Сообщение Announce является общим сообщением при функционировании протокола PTP и используется для распространения информации о характеристиках и состоянии портов устройств PTP, а также данных о качестве синхронизации и приоритетах. Злоумышленник в случае контроля отдельных устройств PTP способен вносить задержки в процесс обработки сообщений Announce, влияя таким образом на работу алгоритма BTCA, повышая его время сходимости, в результате чего могут видоизменяться маршруты доставки сигналов единого времени в отдельные моменты времени.

Рассмотрим случай, когда злоумышленник контролирует узел BC. Для этого добавлены дополнительные элементы задержки «*Delay*», которые имитируют воздействие на пакеты PTP при контроле злоумышленником узла BC на каждый канал передачи сообщения Announce, в результате чего имитационная модель для оценки процесса функционирования BTCA примет вид, показанный на рисунке 5 [1, 11, 15].

Построенная модель позволяет оценивать время сходимости BTCA при различных видах внесения задержек на каждый канал (как постоянных, так и блуждающих). Для примера оценим время сходимости алгоритма при дополнительной задержке 2 мкс на каждый канал передачи и обработки сообщения Announce при исходных данных согласно таблице 2. В результате проведенного моделирования получены следующие результаты. Алгоритм отработал корректно, однако наблюдается значительное увеличение времени сходимости, равное 13,117 мкс. В случае сетей связи значительного размера и масштаба увеличение времени сходимости алгоритма из-за внесения дополнительных задержек в передачу сообщения Announce может повлиять на точность доставки сигналов единого времени и маршруты их передачи.

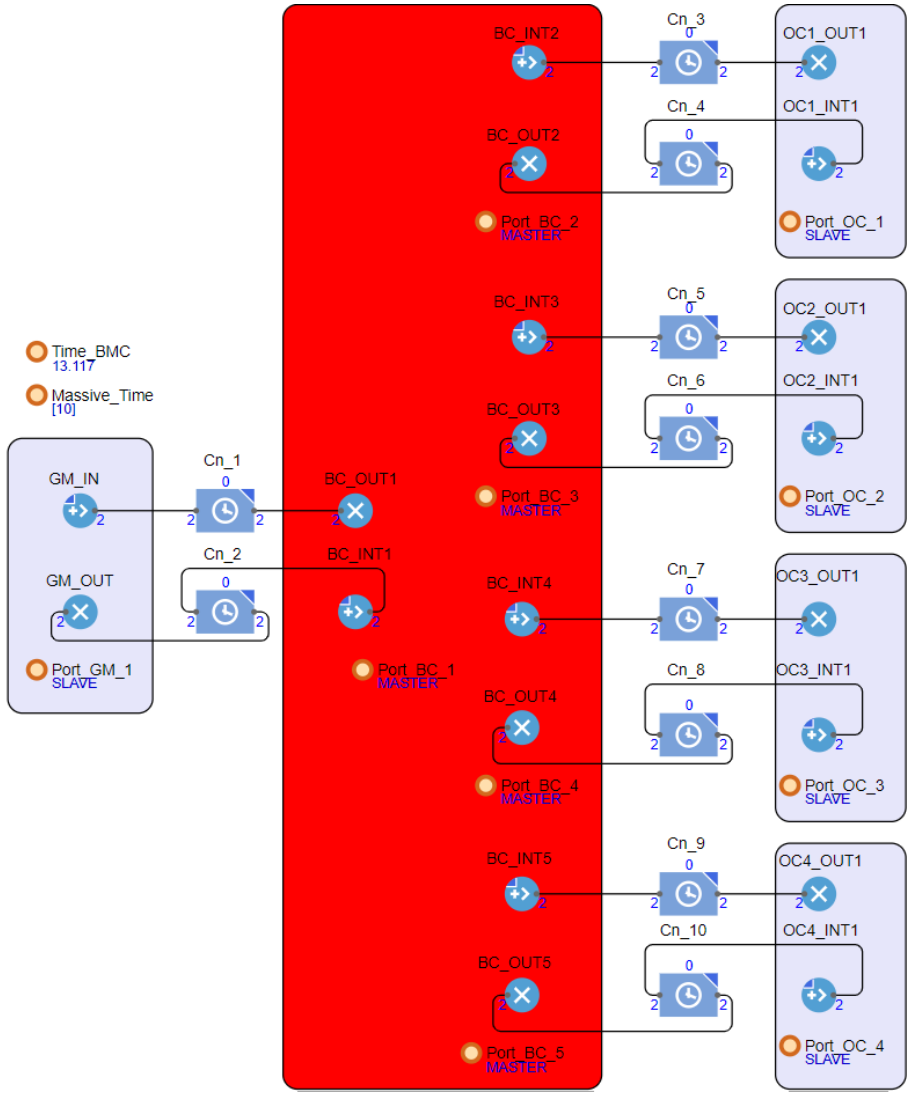

Рис. 5. Результат моделирования процесса функционирования алгоритма BTCA при атаке манипулирования задержкой сообщения Announce в случае контроля злоумышленником узла BC

Fig. 5. The Results of BTCA Functioning Model When Attacker is Manipulating on Announce Messages from Controlled Node BC

С помощью построенной модели возможно производить оценку времени сходимости BTCA с учетом возможных атак на различные устройства PTP и в зависимости от величины возможных задержек. Имея в наличии сведения по оценке времени сходимости алгоритма, можно сделать вывод о вероятных атаках на различные устройства PTP и принять меры по их устранению.

Удаление сообщений Announce при организации процесса функционирования алгоритма BTCA

При атаке с удалением сообщений Announce замедляется процесс построения дерева синхронизации устройств PTP в результате снижения времени сходимости BTCA за счет повторной отправки сообщений. Подобные виды атак являются труднообнаруживаемыми и труднофиксируемыми, так как зачастую на потерю сообщений в сетях связи влияет значительное число дестабилизирующих факторов, таких как качество каналов связи, электромагнитная совместимость, качество электропитания устройств и т. д. Тем не менее, замедление процесса функционирования алгоритма влияет на качество синхронизации, а значит – на качество предоставляемых услуг связи и сервисов реального времени конечным потребителям.

Рассмотрим случай, когда злоумышленник также контролирует узел BC и способен удалять сообщения Announce, в результате имитационная модель для оценки процесса функционирования BTCA примет вид, показанный на рисунке 6 [1, 7, 15]. Исходная модель процесса функционирования алгоритма дополнена блоком «*SelectOutput*», позволяющим задавать вероятность возникновения ошибок

при передаче сообщения Announce. При возникновении ошибки осуществляется повторная передача сообщения.

Для примера оценим время его сходимости при вероятности удаления сообщения, равной 0,3 на каждый канал передачи и обработки сообщения Announce при исходных данных согласно таблице 2. В результате проведенного моделирования получены следующие результаты. Алгоритм корректно определил состояния портов устройств исходя из их атрибутов, однако с учетом удаления отдельных сообщений Announce значительно возросло время сходимости алгоритма, которое в данном случае составляет 15,126 мкс в результате дополнительной отправки сообщений.

При помощи разработанной модели возможно производить оценку времени сходимости BTCA с учетом вероятных атак на сетевые узлы протокола точного времени, когда злоумышленник, завладев узлом PTP, осуществляет умышленное удаление сообщений Announce. Имея в наличии статистику оценки времени сходимости алгоритма, можно сделать вывод о вероятных объектах атаки и предпринять шаги по ликвидации атаки.

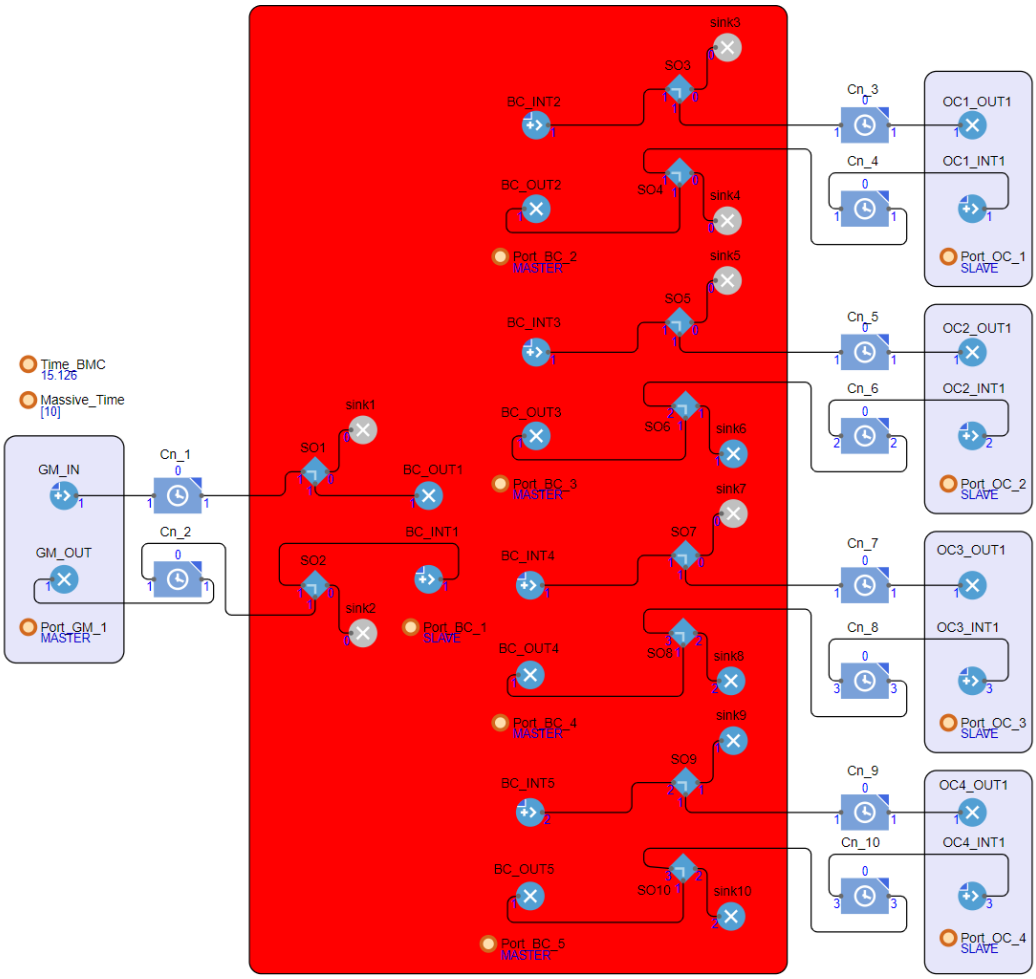

Рис. 6. Результат моделирования процесса функционирования алгоритма BTCA при атаке удаления сообщений Announce в случае контроля злоумышленником узла BC

Fig. 6. The Results of BTCA Functioning When Attacker is Deleting Announce Messages from Controlled Node BC

Заключение

Алгоритм BTCA является ключевым компонентом протокола PTP, который обеспечивает синхронизацию времени в пакетно-ориентированных сетях связи. Реализация BTCA обеспечивает определение устройств PTP с наилучшим качеством, исходя из значений атрибутов портов устройств и характеристик самих устройств. От оперативности и корректности его работы зависит оперативность, точность и стабильность синхронизации всех узлов в сети связи, а значит и качество предоставляемых услуг, поэтому атаки на элементы системы синхронизации, функционирующие по данному алгоритму, являются одними из вероятных сценариев атак. В статье исследованы наиболее возможные стратегии атак на элементы системы синхронизации, функционирующие по BTCA, такие как манипулирование содержимым сообщения Announce,

манипулирование задержкой сообщения Announce и удаление сообщение Announce. Разработанный комплекс моделей позволяет отслеживать процесс функционирования алгоритма BTCA при указанных стратегиях атак, отслеживать состояния портов устройств, оценить качество и достоверность построения дерева синхронизации и время сходимости алгоритма, что может являться основой для выявления возможных атак. Построенные модели могут быть применены на реальных сетях связи для выявления скомпрометированных устройств при наличии информации о характеристиках узлов связи.

Список источников

1. IEEE 1588-2019 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. DOI:10.1109/IEEESTD.2020.9120376

2. Рыжков А.В. Частотно-временное обеспечение в сетях электросвязи: учебное пособие для вузов. М.: Горячая линия – Телеком, 2021. 270 с.

3. Лоховин В.А., Шварц М.Л., Рыжков А.В. Перспективные направления развития систем связи и синхронизации сложных инфраструктурных объектов // T-Comm: Телекоммуникации и транспорт. 2024. Т. 18. № 11. С. 30–37. DOI:10.36724/2072-8735-2024-18-11-30-37. EDN:UZQBNC

4. Мазуренко Д.К. Аспекты построения системы частотно-временной сетевой синхронизации сигналов // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 8. С. 4–8. EDN:ZGFBST

5. Прошин Ф.А., Сторожук М.Н., Сторожук Н.Л. Методы синхронизации в сетях связи // Первая миля. 2024. № 2(118). С. 62–69. DOI:10.22184/2070-8963.2024.118.2.62.69. EDN:BQBPFX

6. Alghamdi W., Schukat M. Cyber Attacks on Precision Time Protocol Networks – A Case Study // Electronics. 2020. Vol. 9(9). P. 1398. DOI:10.3390/electronics9091398. EDN:BVQULX

7. Alghamdi W., Schukat M. Precision time protocol attack strategies and their resistance to existing security extensions // Cybersecurity. 2021. Vol. 4(1). P. 12. DOI:10.1186/s42400-021-00080-y. EDN:WBOCZY

8. Moradi M., Jahangir A.H. A Petri net model for Time-Delay Attack detection in Precision Time Protocol-based networks // IET Cyber-Physical Systems: Theory & Applications. 2024. Vol. 9. Iss. 4. PP. 407–423. DOI:10.1049/cps2.12088

9. Moussa B., Kassouf M., Hadjidj R., Debbabi M., Assi C. An Extension to the Precision Time Protocol (PTP) to Enable the Detection of Cyber Attacks // IEEE Transactions on Industrial Informatics. 2019. Vol. 16. Iss. 1. PP. 18–27. DOI:10.1109/TII.2019.2943913

10. Мазуренко Д.К., Пальцин Д.А., Фень А.С., Федоров А.В., Шварц М.Л. Угрозы безопасности для протоколов сетевого времени в сетях с коммутацией пакетов // Электросвязь. 2024. № 10. С. 69–74. DOI:10.34832/ELSV.2024.59.10.010. EDN:LOHBJL

11. Опарин Е.В. Функционирование системы частотно-временного обеспечения железнодорожного транспорта в условиях воздействия дестабилизирующих факторов. М.: ООО «Издательский центр РИОР», 2025. 248 с. DOI:10.29039/02173-6. EDN:VVRPWS

12. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. С. 36–44. DOI:10.34832/ELSV.2021.14.1.004. EDN:OYYZGF

13. Карпов М.А., Митрофанов М.В., Лаута О.С., Пальцин Д.А. Методика управления защитой информационно-телекоммуникационной сети // Электросвязь. 2021. № 12. С. 49–57. DOI:10.34832/ELSV.2021.25.12.007 EDN:CYNHOX

14. Канаев А.К., Опарин Е.В., Горбач А.Н. Моделирование атаки на систему управления сетью синхронизации // Вестник Рязанского государственного радиотехнического университета. 2020. № 72. С. 35–47. DOI:10.21667/1995-4565-2020-72-35-47. EDN:HYKAKY

15. Бунцев И.А. Создание и реализация имитационных моделей в программной среде AnyLogic. М.: Горячая Линия – Телеком, 2016. 154 с.

References

1. *IEEE 1588-2019 Standard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. DOI:10.1109/IEEESTD.2020.9120376

2. Ryzhkov A.V. *Frequency-Time Support in Telecommunication Networks*. Moscow: Hotline – Telecom Publ.; 2021. 270 p. (in Russ.)

3. Lokhovin V.A., Schwartz M.L., Ryzhkov A.V. Development trends regarding communication and synchronization systems of comxlex infrustructure facilities. *T-Comm*. 2024;18(11):30–37. (in Russ.) DOI:10.36724/2072-8735-2024-18-11-30-37. EDN:UZQBNC

4. Mazurenko D.K. Aspects of the building a system of network synchronization signals in frequency, phase shift and time. *T-Comm*. 2017;11(8):4–8. (in Russ.) EDN:ZGFBST

5. Proshin F.A., Storozhuk M.N., Storozhuk N.L. Methods of synchronization communication networks. *Last Mile*. 2024;2(118):62–69. (in Russ.) DOI:10.22184/2070-8963.2024.118.2.62.69. EDN:BQBPFX

6. Alghamdi W., Schukat M. Cyber Attacks on Precision Time Protocol Networks – A Case Study. *Electronics*. 2020;9(9):1398. DOI:10.3390/electronics9091398. EDN:BVQULX

7. Alghamdi W., Schukat M. Precision time protocol attack strategies and their resistance to existing security extensions. *Cybersecurity*. 2021;4(1):12. DOI:10.1186/s42400-021-00080-y. EDN:WBOCZY
8. Moradi M., Jahangir A.H. A Petri net model for Time-Delay Attack detection in Precision Time Protocol-based networks. *IET Cyber-Physical Systems: Theory & Applications*. 2024;9(4):407–423. DOI:10.1049/cps2.12088
9. Moussa B., Kassouf M., Hadjidj R., Debbabi M., Assi C. An Extension to the Precision Time Protocol (PTP) to Enable the Detection of Cyber Attacks. *IEEE Transactions on Industrial Informatics*. 2019;16(1):18–27. DOI:10.1109/TII.2019.2943913
10. Mazurenko D.K., Paltsin D.A., Fen A.S., Fedorov A.V., Schwartz M.L. Security threats of time protocols in packet switched networks. *Electrosvyaz*. 2024;10:69–74. (in Russ.) DOI:10.34832/ELSV.2024.59.10.010. EDN:LOHBJL
11. Oparin E. *Functioning of the frequency-time support system for railway transport under the influence of destabilizing factors*. Moscow: RIOR Publ.; 2025. 248 p. (in Russ.) DOI:10.29039/02173-6. EDN:VVRPWS
12. Sayenko I.B., Lauta O.S., Karpov M.A., Kribel A.M. Model of threats to information and telecommunication network resources as a key asset of critical infrastructure. *Electrosvyaz*. 2021;1:36–44. (in Russ.) DOI:10.34832/ELSV.2021.14.1.004. EDN:OYYZGF
13. Lauta O.S., Karpov M.A., Mitrofanov M.V., Paltsin D.A. Information and telecommunication network security management methodology. *Electrosvyaz*. 2021;12:49–57. (in Russ.) DOI:10.34832/ELSV.2021.25.12.007. EDN:CYNHOX
14. Kanaev A.K., Oparin E.V., Gorbach A.N. Simulation of attack on synchronization network control system. *Vestnik of Ryazan State Radio Engineering University*. 2020;72:35–47. (in Russ.) DOI:10.21667/1995-4565-2020-72-35-47. EDN:HYKAKY
15. Buntsev I.A. *Creation and Implementation of Simulation Models in the AnyLogic Software Environment*. Moscow: Hotline – Telecom Publ.; 2016. 154 p. (in Russ.)

Статья поступила в редакцию 22.12.2025; одобрена после рецензирования 15.01.2026; принята к публикации 26.01.2026
The article was submitted 22.12.2025; approved after reviewing 15.01.2026; accepted for publication 26.01.2026

Информация об авторах:

ОПАРИН Евгений Валерьевич
кандидат технических наук, доцент, ведущий специалист отдела разработки систем связи ЗАО «Институт телекоммуникаций»
https://orcid.org/0000-0003-4622-9161

ПРОШИН Федор Алексеевич
кандидат технических наук, ассистент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I
https://orcid.org/0009-0009-5513-9302

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.