ИССЛЕДОВАНИЕ СПОСОБА ПОСТРОЕНИЯ СЕТИ IP ДЛЯ ПЕРЕДАЧИ ТРАФИКА НА БАЗЕ АТС ASTERISK

Якубова Мубарак Захидовна[1], Мананкова Ольга[2], Якубов Баходыр[3], Садикова Гульнара[4], Ташев Комил[5]

[1,2,3,4] Алматинский университет энергетики и связи имени Гумарбека Даукеева

[5]Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми

https://doi.org/10.5281/zenodo.7857058

Abstract. *The article is devoted to the study of the method of organizing an IP network for secure data transmission based on the IP-PBX Asterisk, used as a switching station and gateway for traditional PBXs. The purpose of the study is to analyze and model the parameters of the studied IP network using Opnet Modeller for model time when changing codec types during voice traffic transmission. The results of the study show how the value of the transmitted total load changes when the type of codecs changes, the other parameters change insignificantly.*

Keywords: *IP network, Asterisk PBX, security, method, VoIP.*

ВВЕДЕНИЕ

При создании телекоммуникационной сети для функционирования малого или среднего бизнеса выбор часто падает в пользу IP-телефонии. Основным критерием выбора офисной IP-АТС является возможность масштабирования и интеграции в существующую компьютерную сеть компании с минимальными затратами. Основным компонентом сетевой инфраструктуры IP-сети является телефонная станция.

Среди доступных средств организации сети IP-телефонии на рынке телекоммуникаций выделяется программная IP АТС Asterisk, которая имеет открытый код и обладает широкими функциональными возможностями [1-2]. Архитектура IP-сети на базе Asterisk PBX полностью решает проблему организации множественного доступа из одной системы в другую [3-5]. Но, несмотря на множество преимуществ АТС Asterisk, проблема защищенной передачи данных в сети, особенно при ее масштабировании, когда АТС выступает в качестве самостоятельной сервисной системы, остается не до конца изученной.

Большинство исследований в настоящее время сосредоточено на протоколах и шифровании [6-10], но это не устраняет основные угрозы, поскольку в настоящее время у злоумышленников другая направленность. Доступность Asterisk из Интернета является одной из основных угроз сетевой безопасности. При проектировании IP-сети на основе программируемых АТС необходимо учитывать архитектуру сети и конфигурацию системы, чтобы обеспечить безопасную передачу данных. Для повышения уровня безопасности на первом этапе необходимо правильно спроектировать сеть, а затем необходимо защитить данные, передаваемые по открытым каналам связи, от перехвата и прослушивания.

В статье предлагается исследовать способ проектирования сети для защищенной передачи трафика при использовании IP АТС Asterisk в качестве шлюза в локальной сети с моделированием параметров сети в среде Opnet и оценкой защищенности передаваемых данных.

РАЗРАБОТКА СХЕМЫ IP PBX ASTERISK ДЛЯ ИСПОЛЬЗОВАНИЯ В ОФИСЕ

Имитационная модель офисной телефонной сети на базе Asterisk позволяет объединять разрозненные типы данных в общую телефонную сеть с бесплатными звонками и сообщениями внутри нее. Телефония Asterisk безотказно работает в линиях, состоящих из простейших аналоговых устройств и цифровых компонентов.

Для проектирования сети используется среда моделирования Opnet Modeler v.14.5. На рисунке 1 представлена схема, в которой АТС Asterisk используется в качестве шлюза. Эта архитектура позволяет при необходимости выводить пользователей за пределы офисной АТС или за АТС в качестве периферийного сервера приложений. Можно даже делать и то, и другое одновременно. Перед моделированием необходимо настроить устройства по требуемым параметрам. В нашем случае это передача трафика VoIP.

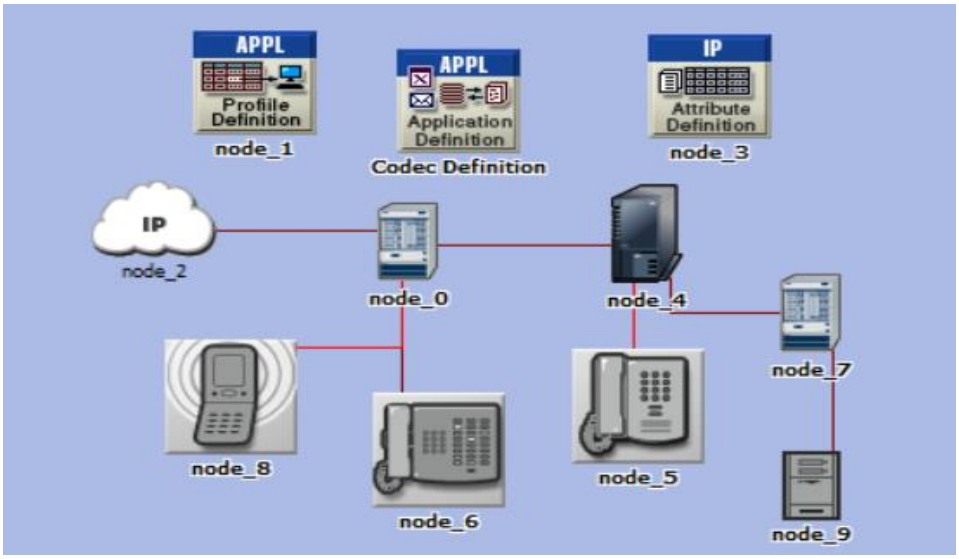
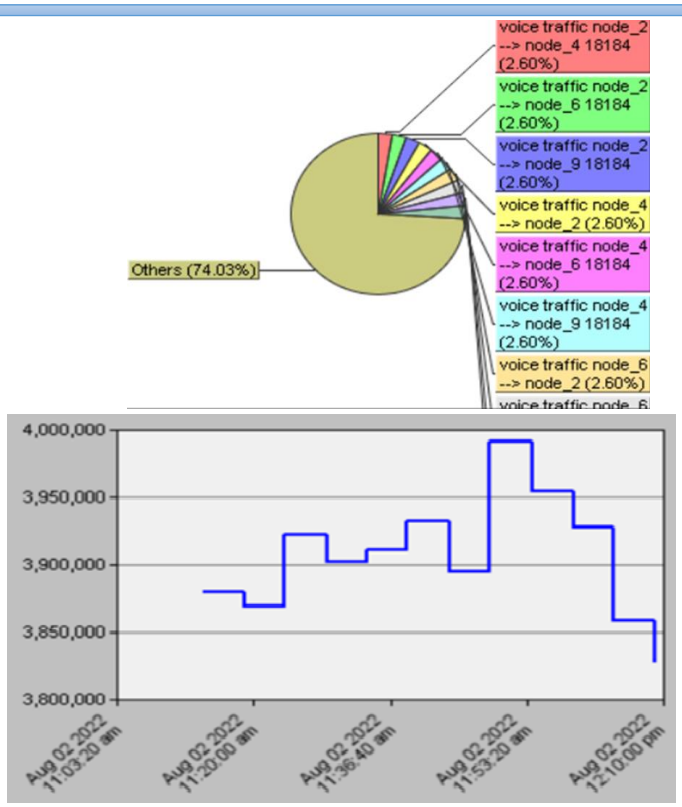


Рис. 1. Сеть IP, в которой АТС Asterisk выполняет роль коммутационной станции в локальной сети и шлюза для традиционной АТС

После настройки было проведено моделирование при выборе VOIP-трафика и получены результаты по прохождению всего трафика при работе кодека G711 в течение времени моделирования (рисунок 2).

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ СЕТИ

По результатам моделирования в среде Opnet Modeler v.14.5 на рисунке 2 а) представлена доля голосовой нагрузки на сеть от каждого устройства при использовании кодека G711, а 2 б) - общее количество пакетов в секунду G 721.



а) б)

Рис. 2. Результаты при моделировании на G 711

В статье исследовано несколько типов кодеков для передачи голосовой информации в рамках разработанной архитектуры. Среди этих кодеков G711, G723, G726, G729. В таблице 1 показаны данные после моделирования нагрузки для рекомендуемых кодеков.

Таблица 1

Величины голосового трафика

Кодеки	G 711	G 723	G 726	G 729
Общая передаваемая нагрузка в GB	147	117	129	126
Величина передаваемой нагрузки между двумя устройствами в GB	3,94	3,14	3,94	3,92
Значение голосового трафика между двумя оборудованиями в %	2,6	3,49	3,06	3,16

Из таблицы 1 видно, что при смене типа кодека изменяется общая нагрузка, передаваемая по сети, и большая нагрузка получается при использовании кодека G 711.

Также меняются и другие параметры, например величина передаваемой нагрузки между оборудованием и голосовой трафик, но незначительно, учитывая значение голосового трафика график передачи при различных типах кодеков приводится на рисунке 3 ниже.

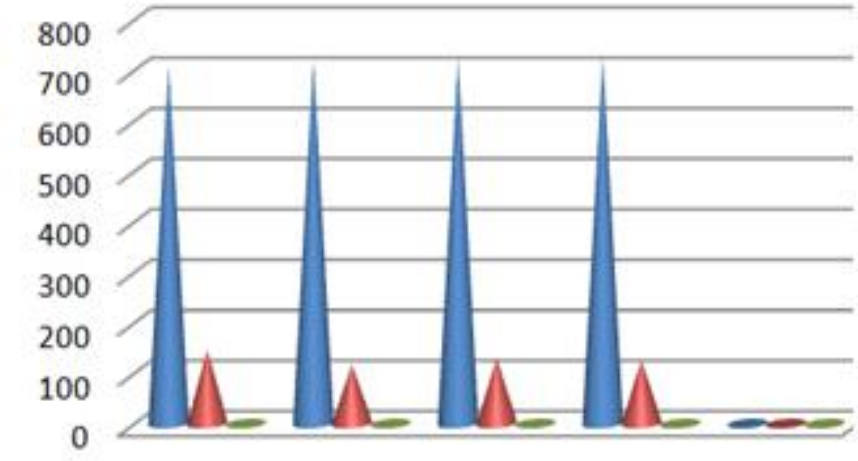


Рис. 3. График распределения голосовой нагрузки в процентах между двумя устройствами

Как видно из рисунка 3, где синим цветом отмечены кодеки, а красным – процентное значение голосового трафика, разница между значениями незначительна.

Разным кодекам требуется разная пропускная способность для передачи аудио- или видеоданных. Некоторые кодеки, например G.711, потребляют больше пропускной способности, чем другие, например G.729. Использование кодеков, потребляющих больше пропускной способности, может привести к перегрузке сети и снижению качества связи.

Кодеки, использующие более высокие коэффициенты сжатия, могут создавать дополнительную задержку, что может привести к задержке или эху во время вызова. Это может повлиять на качество звонка и затруднить естественный разговор.

Не все кодеки совместимы со всеми устройствами и системами. Использование кодека, который не поддерживается конкретным устройством или системой, может привести к передаче аудио- или видеоданных в нестандартном формате, что может вызвать проблемы с качеством связи.

ЗАКЛЮЧЕНИЕ

Таким образом можно сделать выводы по результатам имитационного моделирования разработанной схемы ЛВС, в которой IP PBX Asterisk играет роль коммутации пакетов и шлюза для соединения с традиционными коммутационными станциями, что при использовании разных типов кодеков при передаче информации величина проходящей общей информации за модельное время изменяется, только голосовой трафик изменяется незначительно.

Данное исследование позволяет выявить лучший вариант кодека для использования в сети IP при организации защищенной передачи данных.

БЛАГОДАРНОСТЬ

Данное исследование выполнено/финансируется Комитетом науки Министерства образования и науки Республики Казахстан AP14871745 «Разработка метода повышения безопасности телекоммуникационной сети на базе IP-АТС Asterisk».

REFERENCES

1. Tim Green. Asterisk helps you save money. Seti/Network world, 2011, No. 01 https://www.osp.ru/nets/2011/01/13007192

2. Comparison of Asterisk IP-PBX with traditional PBX using Panasonic KX-TDA200 as an example. http://it.aleksandrid.ru/asterisk-vs-panasonic-KX-TDA200.html.
3. S.V. Konshin, M.Z.Yakubova, T.N. Nishanbayev, O.A. Manankova. Research and development of an IP network model based on PBX asterisk on the opnet modeler simulation package. International Conference on Information Science and Communications Technologies (ICISCT 2020), Article no. 20486746, doi: 10.1109/ICISCT50599.2020.9351405.
4. Khaled Salah, A Alkhoraidly, An Opnet based simulation approach for deploying VoIP. International Journal of Network Management. V.16, No. 3. - John Wiley & Sons, Ltd 2006. 159-183 pp.
5. Salah Khan, N. Sadiq. Design and configuration of VoIP based PBX using asterisk server and OPNET platform. IEECON 2017.
6. Hossain, M.A., Hossain, M.B. Uddin, M.S. and Imitiaz, S.M., "Performance analysis of different cryptographic algorithms", International Journal of Advanced Research in Computer Science and Software Engineering V.6, No.3, 2016, pp. 659-665.
7. O.A. Manankova, B.M. Yakubov, T.G. Serikov, M.Z. Yakubova, A.K. Mukasheva. Analysis and research of the security of a wireless telecommunications network based on the IP PBX Asterisk in an Opnet environment. Journal of Theoretical and Applied Information Technology, Vol.99, No.14, 2021, pp. 3617-3630.
8. Voznak, M.; Rezac, F. Threats to Voice over IP communications systems. WSEAS Transact. Comput. V. 9, No. 11, 2010, pp. 1348–1358.
9. Muntaka, S.A.; Hussein, F.; Sarfo, P. Implementation of an IP Telephony System Based on Asterisk PBX. Int. J. Comput. Appl., V. 177, No.28. Doi: 10.5120/ijca2019919743.
10. Zhang, L.; Hu, X.; Rasheed, W.; Huang, T.; Zhao, C. An Enhanced Steganographic Code and its Application in Voice-Over-IP Steganography. IEEE Access, V.7, 2019, pp. 97187–97195. Doi: 10.1109/access.2019.2930133.