УДК 621.396

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ИССЛЕДОВАНИЯ ВРЕМЕННЫХ ХАРАКТЕРИСТИК БЕСПРОВОДНЫХ СЕТЕЙ ШИРОКОПОЛОСНОГО ДОСТУПА

© 2018 А. С. Стешковой, А. В. Туровский

ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина

В данной статье рассматривается задача, связанная с моделированием беспроводных сетей на основе широкополосного доступа. На основе созданного программного продукта показано, каким образом распределены паузы между передаваемыми пакетами для пакетов данных.

Ключевые слова: широкополосный доступ, моделирование, беспроводные сети.

Стремительность внедрения в системы широкополосной связи стандарта 802.11 Wi-Fi легко объяснить низкой стоимостью, простотой настройки и эксплуатации [1]. Разработанный в совместимости со стандартами 802.3 Ethernet, стандарт Wi-Fi позволяет организовать беспроводную локальную сеть, не меняя существующую архитектуру. Поэтому беспроводные сети стандарта 802.11 широко используются для организации канала связи [3, 4] и передачи мультимедийных данных в сетях общего пользования.

Однако, широкая распространенность и популярность технологии Wi-Fi, использование общей среды передачи, а также отсутствие четкого периметра сети ведут к росту рисков информационной безопасности. В связи с этим применение беспроводных сетей для передачи критически важных данных предъявляет дополнительные требования к обеспечению защиты информации. В статье [1] проведен анализ возможности реализации атаки на беспроводной канал связи с использованием уязвимости проверки целостности пакетов на MAC-уровне.

Схема атаки с использованием уязвимости проверки целостности пакетов представлена на рисунке 1. Злоумышленник ведет прослушивание эфира при помощи бытового (коммерческого) беспроводного адаптера. При получении заголовка физического уровня и заголовка MAC-уровня определяется длина передаваемых данных. По окончанию передачи данных легальным пользователем отправляется контрольная сумма переданного пакета CRC32. В тот же момент злоумышленник, используя этот же адаптер, отправляет в эфир случайные биты, искажая передаваемые значения. Помимо этого, по окончанию передачи злоумышленник может передать от имени точки доступа пакет ACK, подтверждающий успешную доставку отправленного пакета. Обрабатывая полученные данные, точка доступа вычисляет контрольную сумму переданного пакета и сверяет с контрольной суммой, отправленной клиентом. При их обнаружении их различия пакет отбрасывается. Таким образом пакет оказывается «вырезанным» из эфира [1, 6].

Проведенные в статье [6] расчеты проведены на выборке 400 000 пакетов. Для анализа частотно временных характеристик в режиме реального времени разработан программно-аппаратный комплекс, позволяющий производить вычисления длительности пакета, величины пауз между передаваемыми пакетами с учетом рабочего канала точки доступа.

Анализ захваченных пакетов осуществляется на уровне операционной системы при помощи библиотеки Scapy, в связи с чем пакет может быть обработан только после его получения сетевым адаптером и передачи драйвером.

В связи с этим время передачи пакета и величина паузы между пакетами могут быть вычислены на основании времени приема, а также скорости передачи по формулам:

$$\Delta t_i = \frac{l_i}{V_i}, \qquad (1)$$

$$\Delta p_i = t_{\kappa_i} - \frac{l_i}{V_i} - t_{\kappa_{i-1}} = t_{\kappa_i} - \Delta t_i - t_{\kappa_{i-1}}, \qquad (2)$$

Стешковой Анатолий Сергеевич – ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина, сотрудник, 9515431635@mail.ru.

Туровский Алексей Владимирович – ВУНЦ ВВС ВВА им. проф. Н. Е. Жуковского и Ю. А. Гагарина, сотрудник, a.tursk93@yandex.ru.

где Δt_i – время передачи *i*-го пакета,

Δp_i – величина паузы между *i* и *i-1* пакетами,

$t_{к_i}$ – время окончания передачи *i*-го, полученное от драйвера,

l_i – длина *i*-го пакета [бит],

V_i – скорость передачи *i*-го пакета [бит/с].

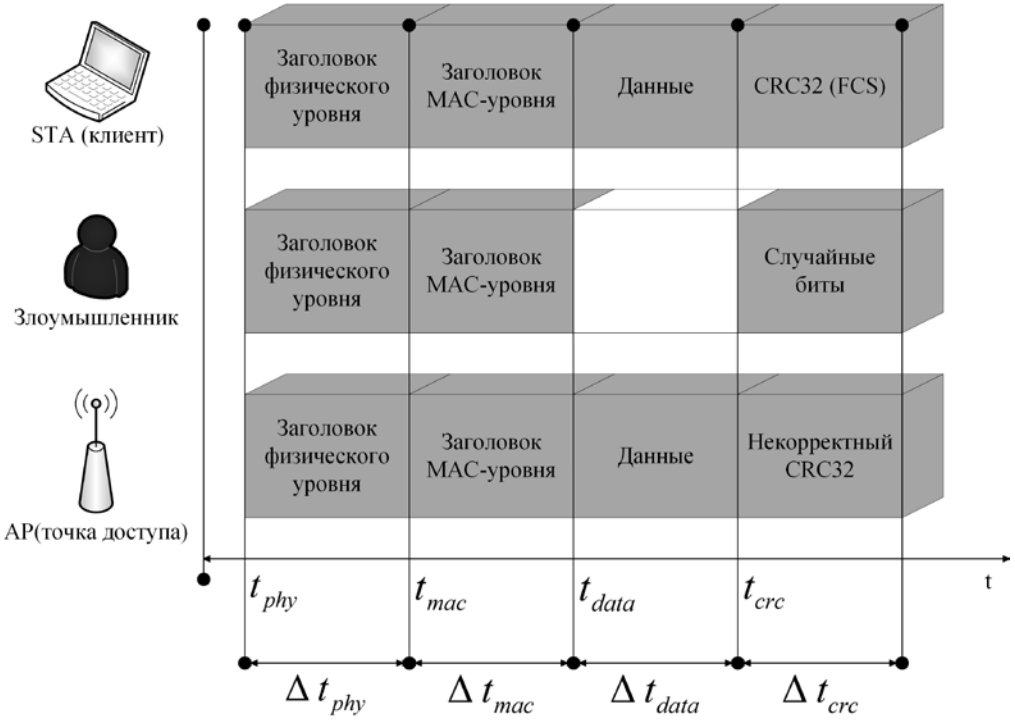


Рисунок 1. Схема искажения контрольной суммы пакета CRC32.

Программная часть комплекса для определения временных характеристик беспроводной сети реализована в виде консольного приложения на языке программирования Python. В качестве аргументов для запуска используются три параметра: режим работы, интервал, в пределах которого будут производиться расчеты, и рабочий канал. Пример работы программы для расчета величин длительности пакетов и паузы между пакетами представлен на рисунке 4.

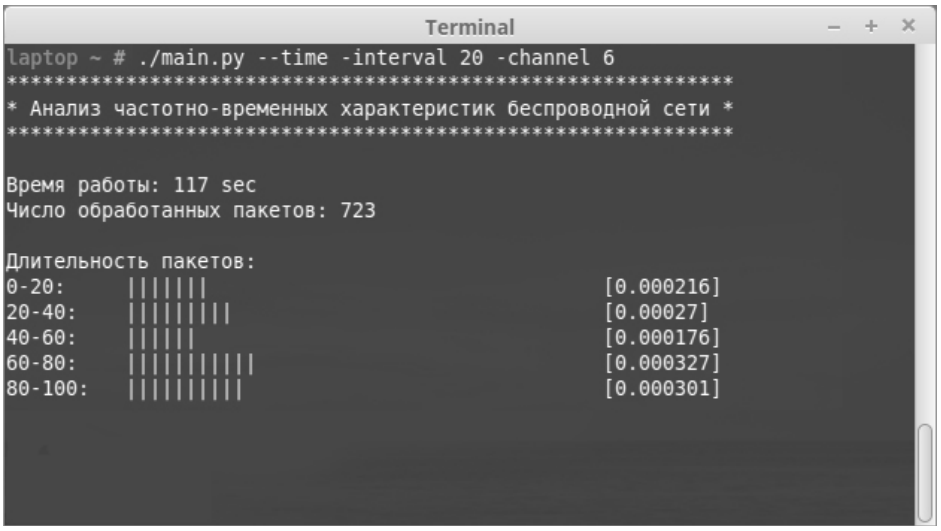


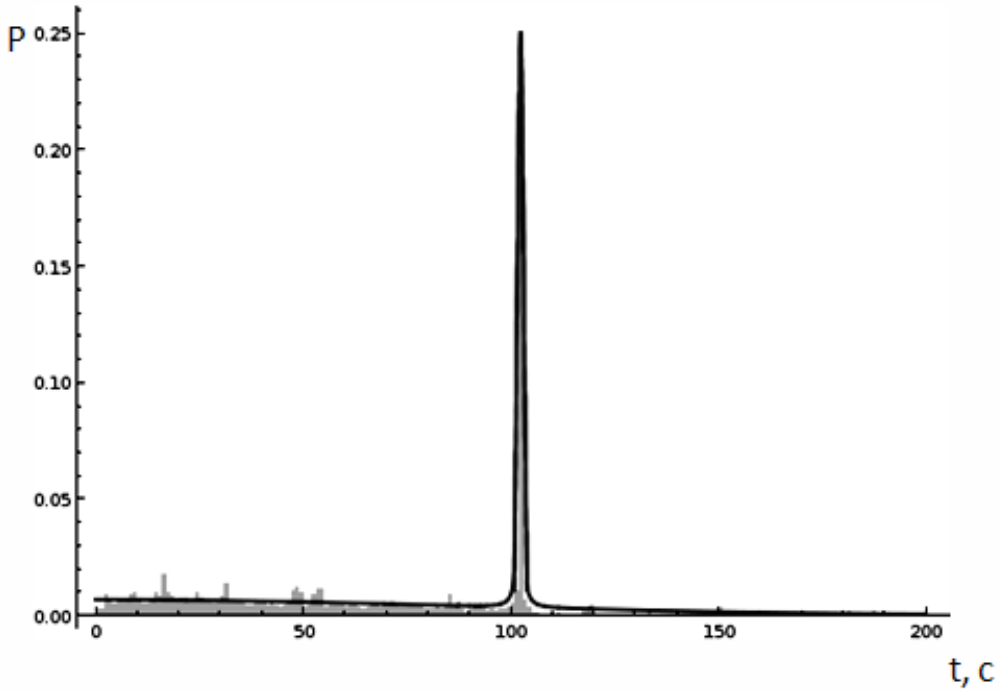
Рисунок 2. Вывод результата работы программы при расчете длительности передаваемых за время анализа пакетов на шестом канале

Также, в предложенном программно-аппаратном комплексе присутствует возможность сортировки по типу передаваемых пакетов. Всего существует три типа пакетов при передаче данных по сети Wi-Fi – пакеты контроля, управления и данных. Каждый из этих основных типов пакетов делится на несколько подтипов. Так, например, пакеты управления подразделяются на пакеты типов Beacon, ProbeReqest, ProbeResponse. В результате собранных с помощью программно-аппаратного комплекса статистических данных были исследованы распределения величин пауз и длительностей для пакетов с данными, контроля и управления [1, 2, 4]. Распределения пауз между пакетами различных типов представлены на рисунках 3, 4, 5. Параметры распределений пауз между пакетами приведены в таблице 1.

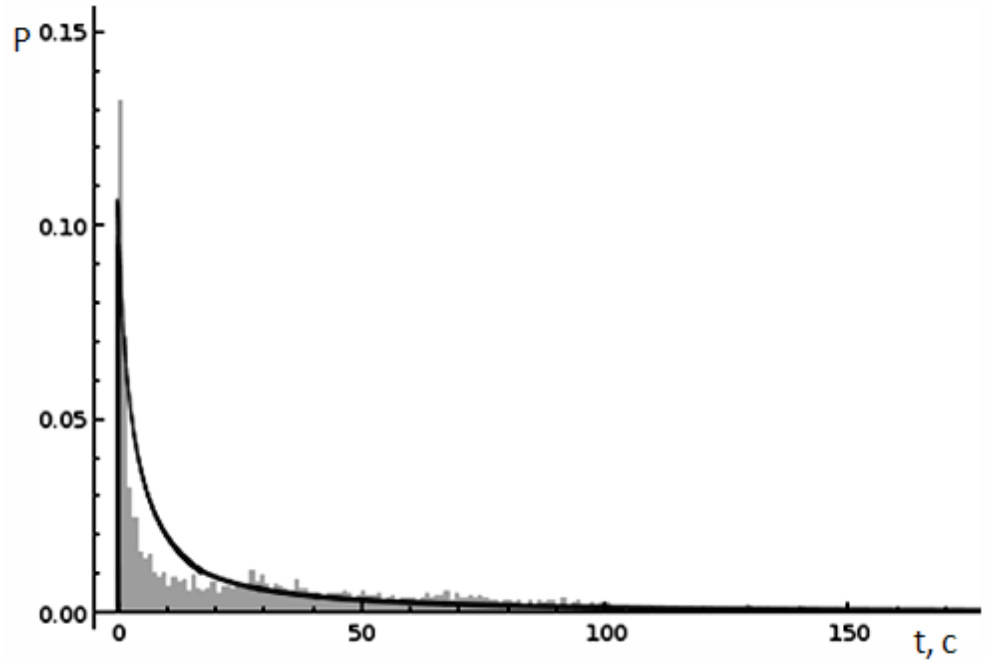
Таблица 1

Параметры распределений пауз между пакетами

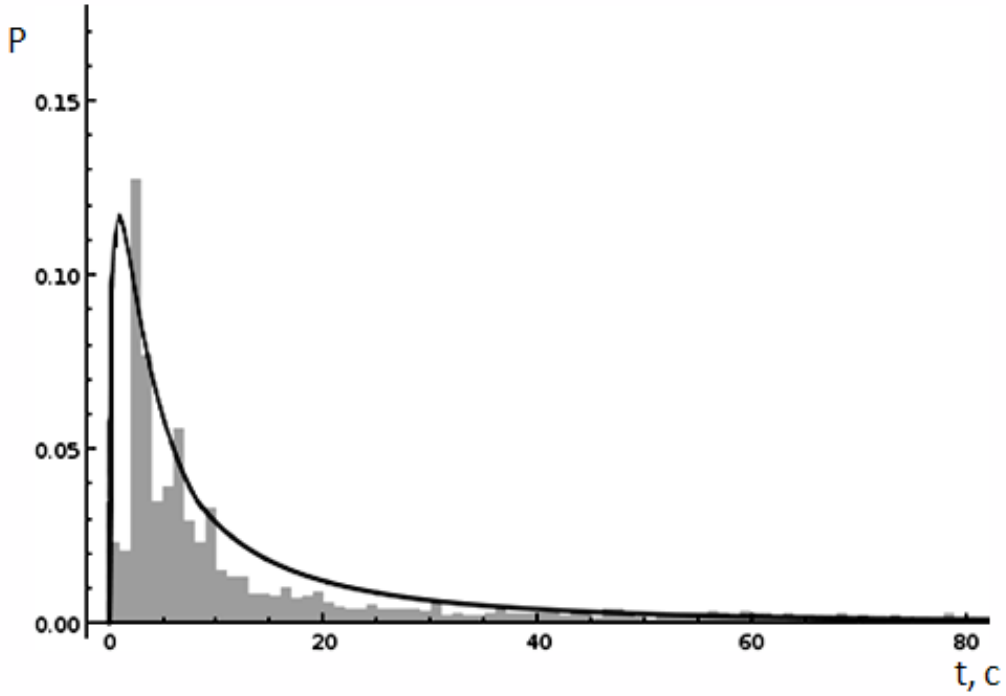
Тип передаваемых пакетов	Beacon	Probe Reqest	Probe Response	ACK	CTS	RTS
Параметры распределений	a = 102.2 b = 0.3	μ=2.7 σ=2.1	μ= 2.1 σ= 1.3	μ = 3.8 σ = 1.5	μ = 2.7 σ = 1.8	μ = 2.4 σ = 2.2



а)

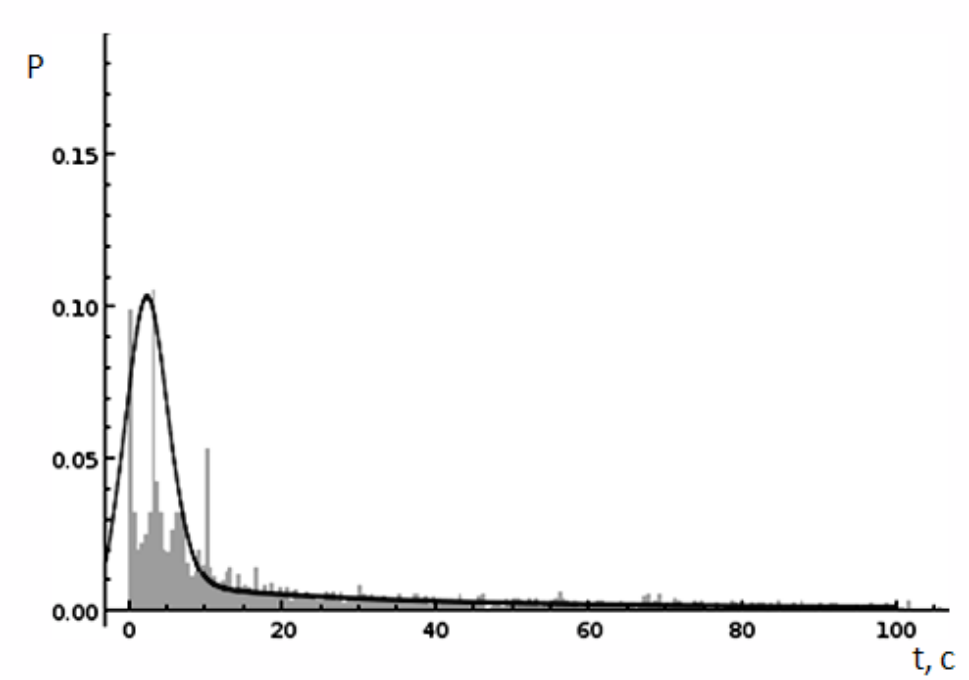


б)

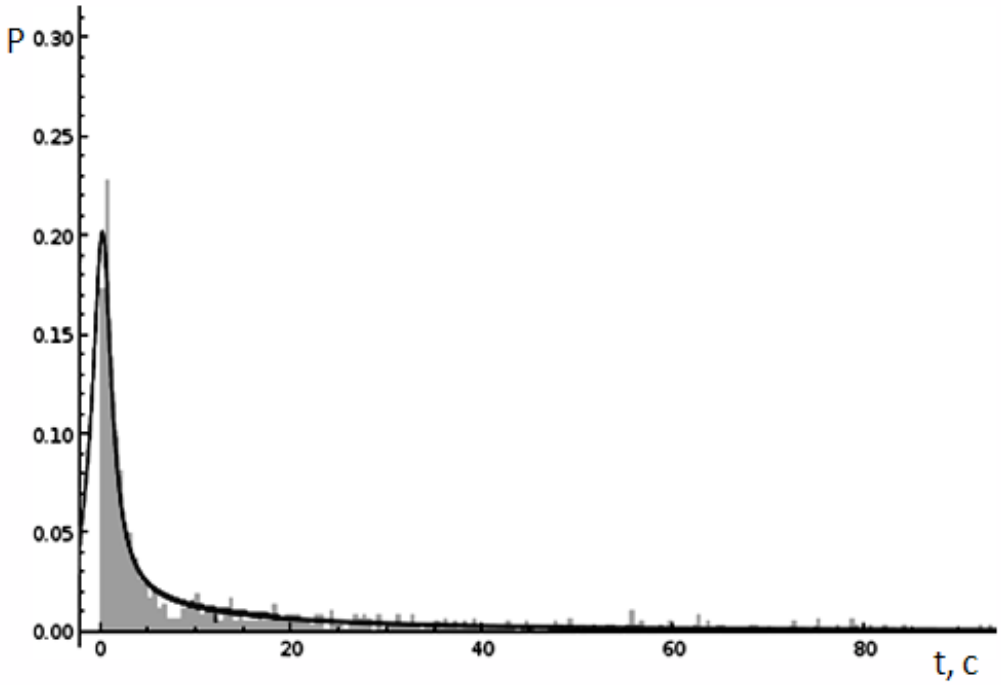


в)

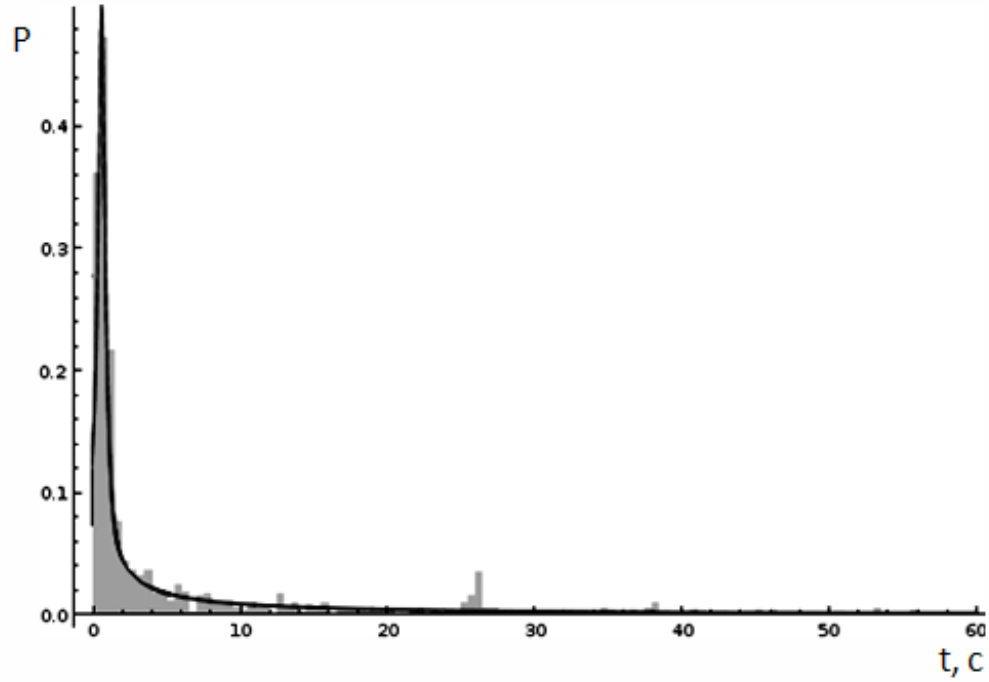
Рисунок 3. Гистограммы распределения паузы между передаваемыми пакетами управления типа:
а) Beacon (Распределение Коши)
б) ProbeReqest (Логнормальное распределение)
в) ProbeResponse (Логнормальное распределение)


P
0.15
0.10
0.05
0.00
0
20
40
60
80
100
t, c

а)


P 0.30
0.25
0.20
0.15
0.10
0.05
0.00
0
20
40
60
80
t, c

б)



в)

Рисунок 4. Гистограммы распределения паузы между передаваемыми пакетами контроля типа:
а) ACK (Логнормальное распределение)
б) CTS (Логнормальное распределение)
в) RTS (Логнормальное распределение)

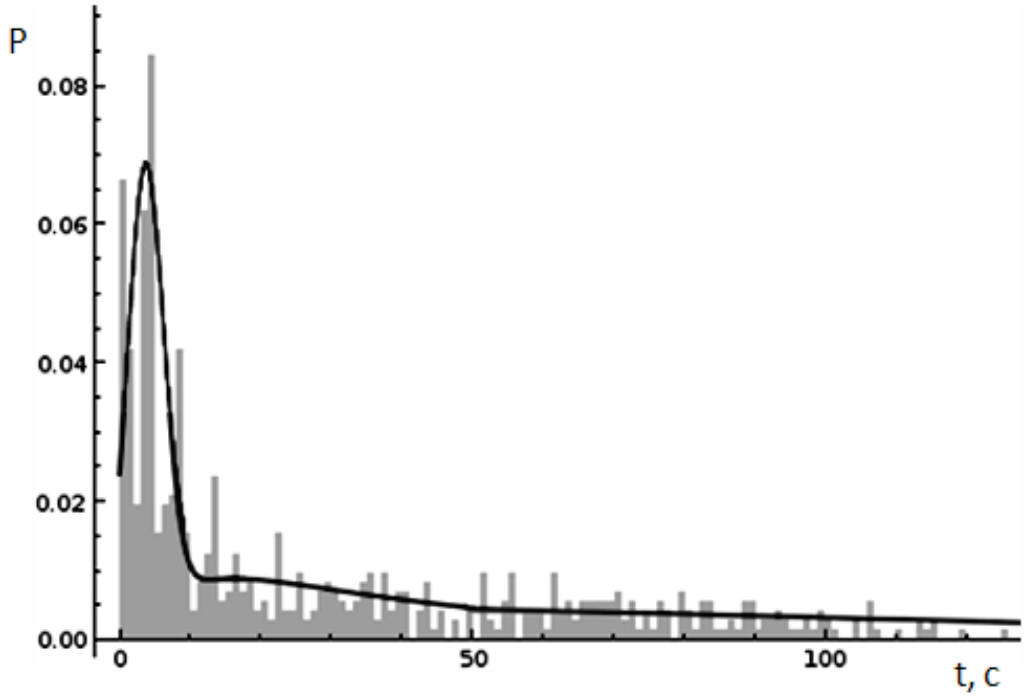


Рисунок 5. Гистограмма распределения паузы между передаваемыми пакетами для пакетов данных (Логнормальное распределение, параметры: $\mu = 2.4$, $\sigma = 2.2$).

Результаты, полученные в ходе работы комплекса, могут быть использованы при анализе скорости и стабильности работы сети, а также при оценке возможности реализации атаки на канал связи с использованием уязвимости проверки целостности пакетов.

ЛИТЕРАТУРА

1. Будников С. А. Модель атаки на беспроводной канал связи с использованием уязвимости проверки целостности пакетов на MAC-уровне / С. А. Будников, И. С. Алехин, Д. К Мухамбетов, К. С. Крючков // Радиоэлектронная борьба и информационная безопасность [текст]: сб. ст. по материалам II Межвузовской НПК курсантов и слушателей «Молодежные чтения, памяти Ю. А. Гагарина» (20 мая 2015 г.): в 2-х ч. – Воронеж: ВУНЦ ВВС «ВВА». – 2015. – Ч. 1. – С. 70-75.

2. Будников С. А. Анализ возможности реализации атаки на беспроводной канал связи с использованием уязвимости проверки целостности пакетов / С. А. Будников, К. С. Крючков, А. Д. Соколов // IV научные чтения имени А. С. Попова. Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией: сб. ст. по материалам Всероссийской НТК слушателей, курсантов и молодых ученых, посвященной Дню образования войск связи (15 октября 2015 г.). – Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 234-236.

3. Львович Я. Е. Исследование методов оптимизации при проектировании систем радиосвязи / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, С. О. Головинов // Теория и техника радиосвязи. – 2011. – № 1. – С. 5-9.

4. Милошенко О. В. Методы оценки характеристик распространения радиоволн в системах подвижной радиосвязи / О. В. Милошенко // Вестник Воронежского института высоких технологий. – 2012. – № 9. – С. 60-62.

5. Рошан П. Основы построения беспроводных сетей стандарта 802.11 / П. Рошан, Д. Лиэри // Пер. с англ. М.: Издательский дом «Вильямс», 2004. – 304 с.

6. Щербаков В. Б. Безопасность беспроводных сетей: стандарт 802.11. / В. Б. Щербаков, С. А. Ермаков // М.: РадиоСофр, 2010. 255 с.

PROGRAM-HARDWARE COMPLEX FOR RESEARCH TIME CHARACTERISTICS OF WIRELESS NETWORKS BROADBAND ACCESS

© 2018 A. S. Steshkovoy, A. V. Turovsky

VUNTS VVS VVA it. prof. N. Ye. Zhukovsky and A. A. Gagarin (Voronezh, Russia)

In this paper, we consider the problem associated with the modeling of wireless networks based on broadband access. On the basis of the created software product, it is shown how the pauses between the transmitted packets for the data packets are distributed.

Key words: broadband access, modeling, wireless networks.