ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www. esa-conference.ru

Применение Марковской цепи для моделирования функционирования мобильной операционной системы (ОС), типа Android с учетом воздействия вредоносных программ

Жернаков Сергей Владимирович, доктор технических наук, профессор;
Гаврилов Григорий Николаевич, аспирант
Уфимский государственный авиационный технический университет (г. Уфа)

В данной работе разработана модель работы мобильной ОС с учетом воздействия вредоносных программ на основе Марковской цепи, а также полученные количественные и качественные показатели. Согласно полученным результатам существует необходимость в исследованиях по направлению защиты информации в данной области.

Ключевые слова: *Android, мобильная операционная система, Марковская цепь, вредоносная программа, стационарное состояние.*

Мобильная ОС типа Android в настоящее время получила широкое применение, а также функциональные возможности, что сказалось на появление большого количества вредоносных программ. Вследствие большого темпа роста популярности разработчикам данной ОС необходимо в короткие строки расширять функциональные возможности путем добавления различных нововведений с выпуском новых версий ОС. С таким темпом работы уделить внимание сфере защиты информации мобильной ОС становится проблематично как финансово так с точки зрения временных затрат на проработку данного вопроса. Таким образом, одной из основных проблем является проблема безопасности мобильной ОС. Наличие множества типов и способов совершения вредоносных действий дает повод проводить исследования в данном направлении, касательное области защиты информации [6, 7, 8, 9].

В своем большинстве вредоносные программы выполняют действия в фоновом режиме, то есть пользователь данной ОС ничего не подразумевает. Следовательно, в процессе работы вредоносная программа расходует большое количество ресурсов системы, парализует ее или выводит из строя. Применение Марковской цепи позволит оценить воздействие вредоносных программ на работоспособность мобильной ОС, а также получить количественные показатели. Марковская цепь широко используется для прогнозирования и моделирования, а также она может быть включена в систему поддержки принятия решений с целью описания процесса функционирования. В данной работе опишем процесс работы мобильной ОС типа Android с учетом воздействия вредоносных программ [1].

Рассматриваемая мобильная ОС – S, имеет 13 возможных состояний. Опишем дискретные состояния, в которых она пребывает в процессе функционирования: S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13. В таблице 1 описаны все состояния, перечисленные выше.

Таблица 1. **Возможные состояния мобильной ОС типа Android.**

Состояние	Описание
S1	Стабильный рабочий режим системы.
S2	Загрузка программы из известного или неизвестного источника.
S3	Программа выполняет запрос разрешений согласно функционалу.
S4	Исполняется код программы.
S5	Программа выполняет вредоносные действия.
S6	Программа находится в состояние покоя (ожидания).
S7	Средства защиты (встроенные, антивирусная программа).
S8	База сигнатур антивирусной программы.
S9	Детектор вредоносных программ.
S10	Ремонт, восстановление.
S11	Отказ, нерабочее состояние мобильного устройства.
S12	Вредоносная программа активируется.
S13	Вредоносная программа пересылает смс, получает контроль и выполняет прочие вредоносные действия.

Марковские процессы с дискретными представляют собой изображенный схематично граф состояний, на котором кружками представлены состояния мобильной ОС, стрелки показывают возможные переходы из состояния в состояние, а задержки в каком-либо состоянии изображаются в виде петли, направленной из данного состояние в него же. На рисунке 1 описаны Марковские процессы в мобильной ОС [2].

Все интенсивности потоков событий, которые переводят мобильную ОС из состояния в состояние постоянные, то есть простейшие потоки.

$$\lambda_{ij} = const \quad (1)$$

Поскольку время перехода мобильной ОС из состояния в состояние, не фиксированное будем считать, что t→∞. В таком случае $p_n(t)$ будут стремиться к пределам, которые называются предельными вероятностями состояний.

$$lim_{t\to\infty}\, p_i(t) = p_i(i = 1,2, \dots, n) \quad (2)$$

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www. esa-conference.ru

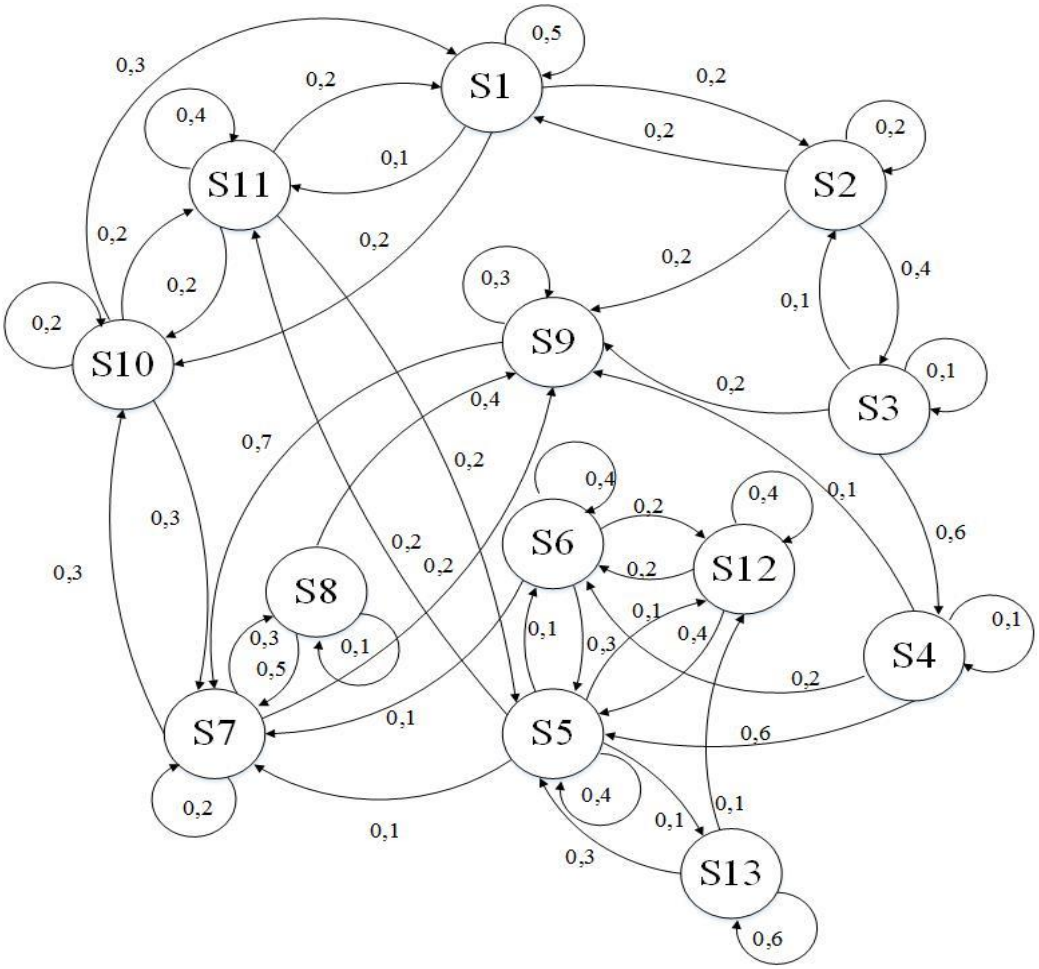

Рис. 1. **Граф состояний мобильной ОС**

Вероятностью перехода (переходной вероятностью) на k-ом шаге из состояния S_i в состояние S_j называется условная вероятность того, что система S после k-го шага окажется в состоянии S_j при условии, что непосредственно перед этим (после k-1 шага) она находилась в состоянии S_i [3].

Поскольку система может пребывать в одном из n состоянии, то для каждого момента времени t необходимо задать n^2 вероятностей перехода P_{ij}, которые удобной представить в виде матрицы.

Составим матрицу условных переходных вероятностей для полученной Марковской цепи.

Таблица 2. **Матрица условных переходных вероятностей**

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13
S1	S1.1	S1.2	0	0	0	0	0	0	0	S1.10	S1.11	0	0
S2	S2.1	S2.2	S2.3	0	0	0	0	0	S2.9	0	0	0	0
S3	0	S3.2	S3.3	S3.4	0	0	0	0	S3.9	0	0	0	0
S4	0	0	0	S4.4	S4.5	S4.6	0	0	S4.9	0	0	0	0
S5	0	0	0	0	S5.5	S5.6	S5.7	0	0	0	S5.11	S5.12	S5.13
S6	0	0	0	0	S6.5	S6.6	S6.7	0	0	0	0	S6.12	0
S7	0	0	0	0	0	0	S7.7	S7.8	S7.9	S7.10	0	0	0
S8	0	0	0	0	0	0	S8.7	S8.8	S8.9	0	0	0	0
S9	0	0	0	0	0	0	0	S9.7	S9.9	0	0	0	0
S10	S10.1	0	0	0	0	0	S10.7	0	0	S10.10	S10.11	0	0
S11	S11.1	0	0	0	S11.5	0	0	0	0	S11.10	S11.11	0	0
S12	0	0	0	0	S12.5	S12.6	0	0	0	0	0	S12.12	0
S13	0	0	0	0	S13.5	0	0	0	0	0	0	S13.12	S13.13

Для Марковской цепи при достаточно большом времени функционирования при t→∞ наступает стационарный режим, при котором вероятности P_i состояний системы не зависят от времени и не зависят от распределения вероятностей в начальный момент времени, т.е. P_i =const.

Каждая компонента P_i вектора таких стационарных вероятностей характеризует среднюю долю времени, в течение которого система находится в рассматриваемом состоянии S_i за время наблюдения, измеряемое k шагами.

Для определения стационарных вероятностей P_i нахождения системы в состоянии S_i (i=1,...,n) нужно составить систе-

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www. esa-conference.ru

му n линейных однородных алгебраических уравнений с n неизвестными.

$$P_i = \sum_{j=1}^{n} P_j P_{ji}, (i = 1, \dots, n) \quad (3)$$

Причем, искомые вероятности должны удовлетворять нормировочному условию.

$$\sum_{i=1}^{n} P_i = 1 \quad (4)$$

Таким образом, при t→∞ в мобильной ОС S устанавливается предельный стационарный режим, то есть мобильная ОС случайным образом изменяет состояния, но вероятность каждого состояния не зависит от времени: каждые состояния выполняются с определенной постоянной вероятностью. Данная вероятность представляет собой среднее относительное время пребывания системы в каком-либо определенном состоянии [4, 5].

Систему линейных алгебраических уравнение удобно составлять по размеченному графу состояний. При этом в левой части уравнения записывается вероятность состояний, соответствующего рассматриваемой вершине графа, а в правой части – сумма произведений. Число слагаемых соответствует числу дуг графа, входящих в рассматриваемое состояние. Каждое слагаемое представляет произведение вероятности того состояния, из которого выходит дуга графа, на переходную вероятность, которой помечена соответствующая дуга графа.

На основании матрицы переходных состояний и графа состояний, а также нормировочным условием составим для стационарного режима систему линейных алгебраических уравнений и решим уравнения методом Крамера.

$$\begin{cases} p_1 = 0.5p_1 + 0.2p_2 + 0.3p_{10} + 0.2p_{11} \\ p_2 = 0.2p_1 + 0.2p_2 + 0.1p_3 \\ p_3 = 0.4p_2 + 0.1p_3 \\ p_4 = 0.6p_3 + 0.1p_4 \\ p_5 = 0.6p_4 + 0.4p_5 + 0.3p_6 + 0.2p_{11} + 0.4p_{12} + 0.3p_{13} \\ p_6 = 0.2p_4 + 0.1p_5 + 0.4p_6 + 0.2p_{12} \\ p_7 = 0.1p_5 + 0.1p_6 + 0.2p_7 + 0.5p_8 + 0.3p_{10} \\ p_8 = 0.3p_7 + 0.1p_8 + 0.7p_9 \\ p_9 = 0.2p_2 + 0.3p_3 + 0.1p_4 + 0.2p_7 + 0.4p_8 + 0.3p_9 \\ p_{10} = 0.2p_1 + 0.3p_7 + 0.2p_{10} + 0.4p_{11} \\ p_{11} = 0.1p_1 + 0.3p_5 + 0.2p_{10} + 0.4p_{11} \\ p_{12} = 0.1p_5 + 0.2p_6 + 0.4p_{12} + 0.1p_{13} \\ p_{13} = 0.1p_5 + 0.6p_{13} \end{cases}$$

Путем математических преобразований упростим систему алгебраических уравнений. В результате чего в левой части останутся нули и единицы, а в правой неизвестные. Решим полученные уравнения методом Крамера.

Таким образом, рассчитаны предельные вероятности, они равны: P1 = 0.108; P2 = 0.028; P3 = 0.013; P4 = 0.008; P5 = 0.067; P6 = 0.021; P7 = 0.17; P8 = 0.19; P9 = 0.17; P10 = 0.11; P11 = 0.077; P12 = 0.021; P13 = 0.017.

Каждая компонента P_i вектора стационарных вероятностей характеризует среднюю долю времени, в течение которого мобильная ОС находится в рассматриваемом состоянии S_i. Можно посчитать сколько, в общем, наша система находится в рабочем и нерабочем состояниях. Анализируя каждое состояние, выделим из множества состояний те, которые относятся к рабочему состоянию мобильной ОС: $S_р$ =S1, S2, S3, S4, S7, S8, S9.

$$(1 - S_н) \times 100 = S_р, (5)$$

где $S_н$ – множество нерабочих состояний мобильной ОС,

$S_р$ – множество рабочих состояний мобильной ОС.

Состояния $□_н$ =S5, S6, S10, S11, S12, S13 относятся к нерабочему состоянию.

$$(1 - S_р) \times 100 = S_н \quad (6)$$

Таким образом, можно сделать вывод, что система находится в рабочем состоянии 68,7% времени, остальное время находится под воздействием вредоносных программ. Достаточно большой процент времени система находится в нерабочем состоянии, что свидетельствует о том, что 31,3% ресурсов мобильная ОС расходует на пребывание не в рабочем состоянии. Большое количество ресурсов расходуется на пребывание в нерабочем состоянии, что оказывает значительное влияние на производительность, качество работы и безопасность мобильной ОС. Проделанный эксперимент свидетельствует о необходимости исследований по разработке системы обнаружения вредоносных программ в области защиты информации, так как данное решение поможет сократить время пребывания ОС в нерабочем состоянии и увеличить производительность, освободить дополнительные ресурсы, что в целом положительно повлияет на безопасность устройства в целом.

Литература:

1. Кельберт М.Я., Сухов Ю.М. Вероятность и статистика в примерах и задачах. Т. II: Марковские цепи как отправная точка теории случайных процессов и их приложения. – М.: МЦНМО, 2009. – 209 с.
2. Портенко Н.И., Скороход А.В., Шуренков В.М. Марковские процессы. – ВИНИТИ, 1989. – 178 с.
3. Стратонович Р.Л. Условные марковские процессы и их применение к теории оптимального управления. – М.: МГУ,

1966. – 25 с.

4. Таганов К.В., Овчаров Л.А., Тырышкин А.Н. Аналитические методы исследования систем. – М.: Советское радио, 1974. – 32 с.

5. Трахтенгерц Э.А. Компьютерная поддержка принятия решений: научно-практич. издание. Серия: Информатизация Россия на пороге XXI века. – М.: СИНТЕГ, 1998. – 376 с.

6. Уязвимости платформы Android. Настоящее и будущее [Электронный ресурс]. Режим доступа: http://habrahabr.ru/company/drweb/blog/142993/ (дата обращения: 28.11.2014).

7. Android. (n.d.). *Introduction to Android*. Retrieved 1 23, 2014, from Android Developers [Электронный ресурс]. Режим доступа: http://developer.android.com/guide/index.html (дата обращения: 23.01.2015)

8. Sheran Gunasekera. Android Apps Security. Apress, 2012. 3 p.

9. Arp D., Spreitzenbarth M., Hubner M., Gascon H., Rieck K. DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. NDSS Symposium 2014, Switzerland, 2014, vol. 4, no. 1 Available at: https://user.informatik.unigoettingen.de/~krieck/docs/2014-ndss.pdf