Методика выявления аномального поведения функционирования устройств сетевой инфраструктуры «Индустрии 4.0»

Technique for identifying anomalous behavior of functioning of devices of network inforastructure "Industry 4.0"

Сухопаров / Sukhoparov M.
Михаил Евгеньевич
(sukhoparovm@gmail.com)
кандидат технических наук.
Санкт-Петербургский филиал АО «НПК «ТРИСТАН»,
старший научный сотрудник.
г. Санкт-Петербург

Ключевые слова: информационная безопасность – information security; беспроводные сети, сетевая инфраструктура «Индустрии 4.0» – «Industry 4.0» network infrastructure; доступность устройств – device accessibility; модель информационной безопасности – information security model.

Рассмотрена сетевая инфраструктура «Индустрии 4.0», проведен анализ характеристик систем, базирующихся на беспроводных технологиях, получаемых в результате пассивного наблюдения и активного опроса устройств, которые составляют инфраструктуру сети. Предложена методика выявления внешних признаков попыток несанкционированного доступа к устройствам сетевой инфраструктуры со стороны потенциального нарушителя информационной безопасности.

A wireless network is considered, an analysis of the characteristics of systems based on wireless technologies obtained as a result of passive monitoring and active polling of the devices that make up the network infrastructure is carried out. A number of external signs of attempts of unauthorized access to a wireless network by a potential information security violator are considered.

Введение

Глобальные изменения, связанные с массовой компьютеризацией технологических процессов и быстрый рост различных информационных технологий, не оставили в стороне производственные системы.

Создание и повсеместное использование роботов, программируемых контроллеров и цифровых систем управления, интегрированных в вычислительные сети предприятий, повлекло за собой изменение самого подхода к управлению производством, что, в свою очередь, привело к созданию новых технологических процессов управления.

Но в то же время подобные системы становятся крайне уязвимы к различного рода деструктивным воздействиям со стороны потенциальных нарушителей в силу отсутствия стандартизированных подходов к организации сетевой инфраструктуры и недостаточного внимания к обеспечению информационной безопасности в процессе их функционирования [1–3].

Злоумышленник получает возможность осуществлять деструктивные воздействия за счет использования для организации сегментов сети стандартных технологий и возможной ограниченности вычислительных ресурсов. Ввиду отсутствия контролируемой зоны, недостаточного уровня криптографической защиты информации, возможности идентификации сетевых устройств и узлов при помощи служебных сообщений при несанкционированных попытках доступа к сети, возникает ряд предпосылок для реализации угроз информационной безопасности, связанных с осуществлением попыток управления такими устройствами извне [4, 5].

Необходимость анализа отклика устройств, подверженных атаке, со стороны нарушителя вызывает рост числа повторных типов команд и сообщений, несоответствующих установленной ситуации, что может служить источником информации для более пристального анализа параметров сетевого трафика [6, 7].

Таким образом, для идентификации состояния ИБ сетевой инфраструктуры «Индустрии 4.0» может служить анализ различных отклонений характеристик информационных потоков в процессе функционирования системы.

Постановка задачи

Физические, логические компоненты сетевой инфраструктуры обеспечивают управление, связь, маршрутизацию, безопасность, доступ и другие функциональные свойства. Совокупность устройств определяет инфраструктуру вычислительной системы [8, 9].

Прием, обработка и передача ограниченного типа сообщений, большое количество типов подключаемых

устройств, накладывает ряд проблемных вопросов, связанных, с одной стороны, с гибкостью изменений, дополнений, вносимых в архитектуру системы, а с другой – отслеживания, анализа и обработки возникающих неоднозначных ситуаций со стороны системы защиты информации в условиях ограничения вычислительных ресурсов. В связи с этим возникает потребность в использовании внешних систем мониторинга информационной безопасности.

Обработка внешних статистических данных, характеризующих состояние системы, может служить одним из подходов при реализации подобных систем. В различных режимах эксплуатации возможно произвести оценку интенсивности появления служебных сообщений, информационных пакетов (в том числе и нераспознанных), задержки отклика на запросы, количественные показатели коллизий, частоту идентификации пропущенных сообщений [9, 10].

Осуществлять накопление данных для последующего статистического анализа можно при помощи пассивного «прослушивания» сети, опроса устройств сетевой инфраструктуры системой мониторинга, или путем применения комбинированного режима.

За счет анализа полученных статистических данных оказывается возможным идентификация появления различных аномалий в процессе штатного режима функционирования вычислительной системы.

Предлагаемый подход

Для обнаружения попыток несанкционированного доступа необходимо производить анализ пакетов сообщений, в которых присутствуют поля, содержащие неправильные адреса, флаги, команды на подключение, конфигурацию, доступ к ресурсам. В то же время для анализа состояния информационной безопасности, выявления инцидентов на низком уровне взаимодействия устройств необходимы знания узкоспециализированных алгоритмов функционирования устройств конкретных производителей, сетевых протоколов.

В связи с этим для упрощения построения системы мониторинга статистические данные можно рассматривать на прикладном уровне протоколов. Узел анализа сетевых событий может быть реализован в виде устройства, работающего только на прием всех сообщений вычислительной сети, либо блока, рассылающего команды и обрабатывающего принимаемые сообщения, данные, задержки, настройки, идентификационную информацию узлов. Таким образом, при помощи полученной информации можно строить частотные портреты функционирования как всей сети, так и для отдельных устройств, а также проводить их сравнение и анализ.

На рис. 1 представлена схема системы с выделенным узлом анализа.

На специально выделенном узле происходит обработка и анализ сообщений, передаваемых и принимаемых датчиками и сенсорами.

Частотные показатели нераспознанных, повторных сообщений, сбоев и отказов отдельных устройств, изменение временных показателей задержек различных идентифицируемых типов сообщений позволяют по каждому устройству создать модель функционирования системы M для дальнейшего анализа состояния информационной безопасности (1):

$$M = < h_1^{out}, ..., h_N^{out} > \quad (1)$$

На рис. 2 представлен частотный портрет функционирования отдельного устройства сетевой инфраструктуры.

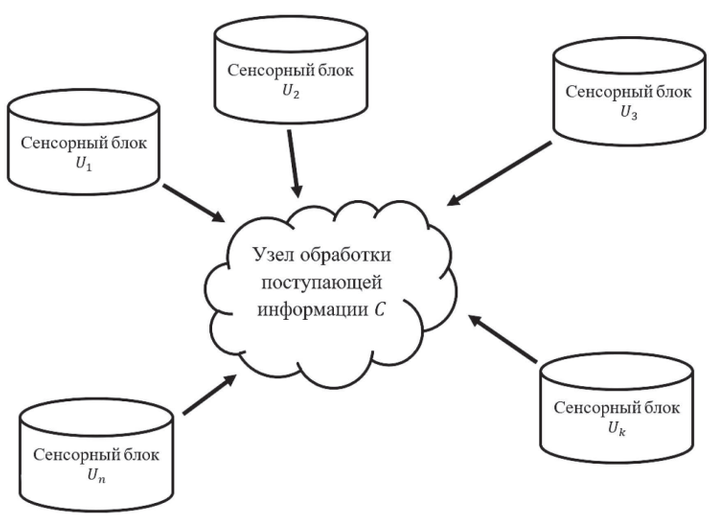

Рис. 1. Взаимодействие узлов сети

Тогда функционирование конечного множества m устройств может быть представлено в виде матрицы:

$$M = \begin{bmatrix} h_{10}^{out} & \cdots & h_{1n}^{out} \\ \vdots & \ddots & \vdots \\ h_{m0}^{out} & \cdots & h_{m0}^{out} \end{bmatrix} \quad (2)$$

Приведенная выше совокупность частот событий позволяет рассмотреть частотный портрет функционирования персональной сети в целом.

Изменение статистического портрета функционирования сети и устройств наблюдается в зависимости от режима работы. На основе частотных данных возникновения сетевых событий отдельного устройства и сети в целом можно создавать базу данных функционирования системы, информацию которой в дальнейшем обрабатывать статистическими методами.

Накопление признаков, их представление в виде вектора числовых значений, изменяемых в течение времени, позволяет использовать различный математический аппарат для идентификации состояния информационной безопасности на основе решения задач классификации.

Одним из подходов является применение наивного байесовского классификатора, для обучения которого требуется малое количество данных:

$$C = \arg\max_{h \in H} \frac{p(X/h)p(h)}{p(X)} \quad (3)$$

где h, X – предсказываемое и предшествующее события;

p – вероятности этих событий ($p = m/n$, где m – количество произошедших событий, n – количество всех событий).

Предлагаемый подход позволяет определить состояние информационной безопасности сетевой инфраструктуры. В то же время полученные на его основе результаты решения могут носить рекомендательный характер и требовать дальнейшего изучения.

В различных режимах работы системы могут наблюдаться аномалии, возникающие по причине технических и технологических факторов. Построение на основе количественных, частотных данных о сбоях отказах пропусках сообщений классификатора изначально предполагает наличие ошибок первого и второго рода, которые могут возникать по причине конфликтов с соседними сетями, либо наличия помех [9].

Информационные и служебные сообщения циркулируют между узлами $U_1,\ldots,U_n$, устройство C предназначено для сбора информации (рис. 1). В первом случае устройство C прослушивает сеть и формирует выборку статистических данных, во втором – дополнительно осуществляет рассылку запросов на устройства и измеряет различные характеристики.

Методика

Архитектура модельной сети состоит из модуля сбора и обработки данных, передающих и принимающих модулей.

Модуль сбора и обработки, осуществляющий сетевое взаимодействие с установленным на нем программным обеспечением, анализирует частотные показатели принимаемых и отправляемых сообщений в сети, что позволяет собирать статистические данные взаимодействия узлов.

Методика выявления аномального поведения функционирования устройств сетевой инфраструктуры состоит в следующем. Выдается последовательность информационных сообщений на узлы сети. Отправляемые и получаемые данные сравниваются на узлах сети, в результате анализа получаются количественные и частотные характеристики работы. В ходе работы выполняется следующая последовательность действий.

1. Каждое устройство независимо от других сетевых узлов последовательно выдает информационные сообщения по адресам узлов сети.

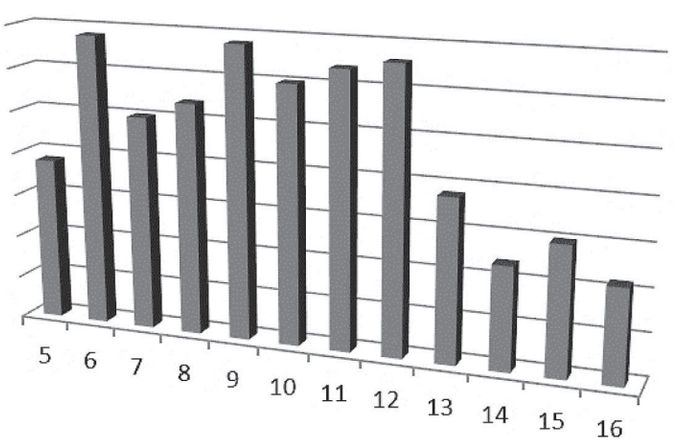

Рис. 2. Частотный портрет функционирования отдельного устройства персональной сети

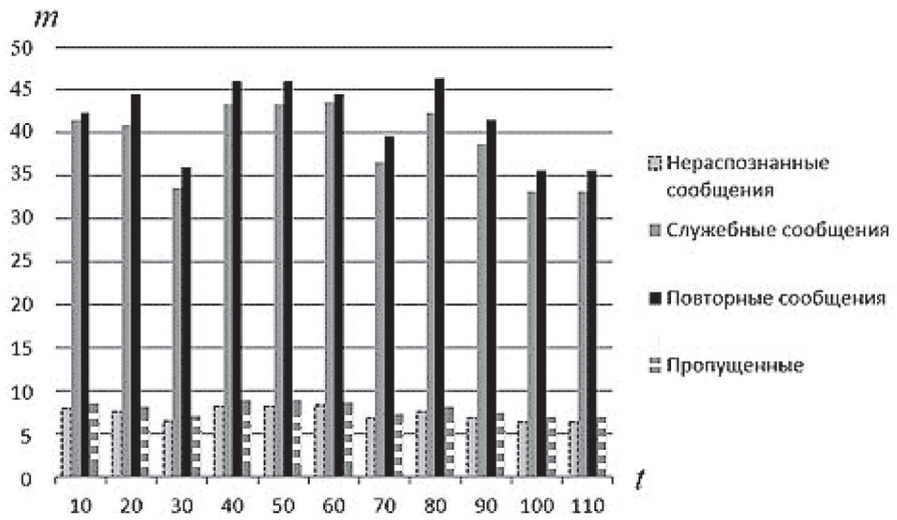

Рис. 3. Изменения количественных значений по видам сообщений

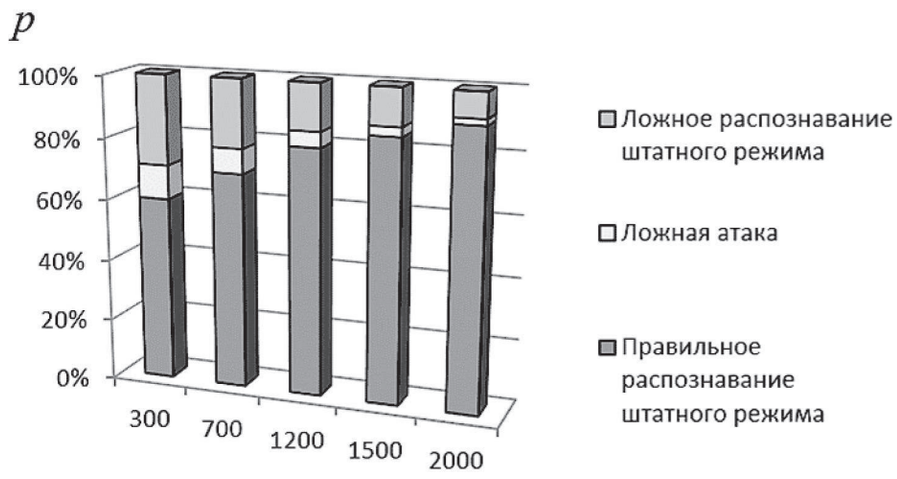

Рис. 4. Вероятностная оценка работы классификатора состояний системы на основе байесовского классификатора для различных объемов обучающей выборки

2. Каждое устройство принимает сообщения, анализирует их корректность. Периодически выдает информацию о своем состоянии.

3. Модуль *C* в пассивном режиме слушает сеть. Распознает типы переданных сообщений, анализирует внешние признаки, накапливает информацию на определенном интервале времени.

4. В активном режиме модулем *C* осуществляется опрос состояния устройств, определяется задержка на переданную команду.

Имитация действий нарушителя происходит после обучения в модуле *C* наивного байесовского классификатора в течении интервала времени. Для этого передающее устройство модуля *C* посылает команды конфигурирования и управления модулями во время работы сети.

Накопление данных происходило путем сравнения статистической информации служебных сообщений оконечных узлов в пассивном и активном режимах модуля *C*.

Ниже приведены результаты работы методики на сети, состоящей из 12 элементов. Изменения количественных значений по видам сообщений кортежа параметров приведены на рис. 3.

Имитация атаки осуществлялась путем интенсивности поступления команд управления на модули сети.

Последовательность команд, отправляемых на функционирующие устройства, выбиралась случайным образом.

Кортеж признаков, полученный через постоянные заданные промежутки времени, обрабатывались наивным байесовским классификатором. В результате работы классификатора производилось обнаружение аномальных состояний системы, на которые следует обратить более пристальное внимание.

В приводимом эксперименте для систем пассивного и активного мониторинга рассмотрены состояния:

– правильного распознавания штатного режима функционирования и атаки на сеть;

– ложного распознаваний атаки (при ее отсутствии);

– ложного распознавания нормального состояния (при проведении атаки).

Объем обучающей выборки *k* изменялся от 500 до 2500 кортежей. Результаты работы классификатора (где правильное распознавание состояний объединено) представлены на рис. 4.

Предлагаемое решение достаточно легко реализуемо и может применяться для обнаружения аномальных параметров функционирования вычислительной сети. Особенностью наивного байесовского классификатора является отсутствие больших вычислительных затрат и быстрое обучение.

Заключение

Предложенное решение может применяться для поиска аномалий при функционировании устройств сетевой инфраструктуры «Индустрии 4.0».

Для повышения точности обнаружения несанкционированного доступа возможен дополнительный анализ взаимосвязи анализируемых событий.

Предложенная методика выявления аномального поведения функционирования устройств сетевой инфраструктуры «Индустрии 4.0» на основе статистических данных функционирования узлов позволяет оценивать состояния информационной безопасности с помощью вероятностных характеристик. Основная особенность, обусловливающая преимущество методики, заключается в быстрой адаптации к локальным сетям маломощных устройств.

Литература

1. Зикратов, И. А. Доверительная модель управления безопасностью мультиагентных робототехнических систем с децентрализованным управлением / И.А. Зикратов, Т.В. Зикратова, И.С. Лебедев // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 2 (90). – С. 47–52.

2. Zikratov, I. Trust and Reputation Mechanisms for Multi-agent Robotic Systems / I. Zikratov, I. Lebedev, A. Gurtov // Lecture Notes in Computer Science. – 2014. – Vol. 8638. – P. 106–120.

3. Security of autonomous systems employing embedded computing and sensors / A.M. Wyglinski [et al.] // IEEE Micro. – 2013. – Vol. 33, No. 1. – P. 80–86.

4. Lebedev, I. S. The Monitoring of Information Security of Remote Devices of Wireless Networks / I.S. Lebedev, V.M. Korzhuk // Lecture Notes in Computer Science. – 2015. – Vol. 9247. – P. 3–10.

5. The analysis of abnormal behavior of the system local segment on the basis of statistical data obtained from the network infrastructure monitoring / I. Lebedev [et al.] // Lecture Notes in Computer Science. – 2016. – Vol. 9870. – P. 503–511.

6. Monitoring of the Information Security of Wireless remote devices / N. Bazhayev [et al.] // Source of the Document 9th International Conference on Application of Information and Communication Technologies, AICT 2015 – Proceedings. – 2015. – P. 233–236.

7. isBF: Scalable In-Packet Bloom Filter Based Multicast / I. Nikolaevskiy [et al.] // Computer Communications. – 2015. – Vol. 70. – P. 79–85.

8. Implementing a broadcast storm attack on a mission-critical wireless sensor network / I. Krivtsova [et al.] // Lecture Notes in Computer Science, 2016. – Vol. 9674. – P. 297–308.

9. Бажаев, Н. А. Исследование доступности удаленных устройств беспроводных сетей / Н.А. Бажаев, И.Е. Кривцова, И.С. Лебедев / Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16, № 3. – С. 467–473.

10. Оценка безопасного состояния мультиагентной робототехнической системы при информационном воздействии на отдельный элемент / Д.Г. Исакеев [и др.] // Вестник компьютерных и информационных технологий. – 2015. – № 1 (127). – С. 43–49.