клиентов, работающих в соответствии с координационно-ориентированной вредоносной программой [3]. Когда BotHunter создает профиль заражения, профиль передается в BHResponder, который реализует простой алгоритм сопоставления политики, чтобы решить, должен ли локальный ресурс быть помещен на карантин. Если это так, BHResponder передает директиву безопасности карантина, которая определяет IP-адрес локального беспроводного клиента в SDN Security Actuator. SDN Security Actuator – это приложение OpenFlow, работающее с ролью SEC, и использующее API SE-Floodlight Northbound для взаимодействия с SE-Floodlight. При активации он регистрирует обратный вызов для получения уведомлений обо всех потоковых запросах к зараженному клиенту и от него. Все подключения к клиенту и от него затем запрещаются.

Таким образом, была рассмотрена проблема безопасности, связанная с набором функций, которые позволят сети OpenFlow для нескольких приложений работать в чувствительной сетевой вычислительной среде, которая в свою очередь должна отвечать строгим требованиям безопасности [4]. А именно рассмотрено согласование динамического производства логики правил потока с необходимостью сохранения последовательных ограничений политики безопасности, которые в сетях OpenFlow, по существу, являются правилами потока, создаваемыми администратором или динамически вставляемыми приложениями безопасности в ответ на воспринимаемые угрозы. Следовательно, для уязвимых вычислительных сред существует достаточная мотивация, чтобы рассмотреть SDN как потенциальный источник инновационного устранения угроз.

Литература

1. FloodLight [Electronic resource] “Open SDN controller,” http://floodlight.openflowhub.org/.

2. N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, “NOX: Towards an Operating System for Networks,” in Proceedings of ACM Computer Communications Review, July 2008.

3. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection Through IDS-driven Dialog Correlation,” in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, 2007.

4. Sukhov A. M., Sagatov E. S., Baskakov A. V. Rank distribution for determining the threshold values of network variables and the analysis of DDoS attacks //Procedia Engineering. – 2017. – Т. 201. – С. 417-427.

В.П. Цветов

О ВЛОЖЕНИИ ИЗМЕРИТЕЛЬНЫХ ШКАЛ

(Самарский университет)

В современной теории измерений выделяют пять основных видов шкал измеряемых величин [1].

Шкалы наименований (номинальные шкалы). Подобные шкалы применяется исключительно для классификации объектов, путем их отнесения к одному из непересекающихся классов, т.е. задают на множестве объектов с оцениваемыми свойствами некоторое отношение эквивалентности. Классическим примером такой шкалы является шкала классификации цвета объектов по наименованиям в соответствии с атласами цветов.

Шкалы порядка (ранговые шкалы). Эти шкалы позволяют установить на множестве объектов отношение эквивалентности и отношение порядка на классах эквивалентности. В порядковых шкалах устанавливается иерархия объектов относительно оцениваемого свойства. Типичными представителями порядковых шкал являются шкалы измерения силы землетрясений, твердости минералов и т.п.

Шкалы интервалов (шкалы разностей). Интервальные шкалы сопоставляют измеряемому свойству вещественное число в соответствии с принятой условной единицей измерения и относительной нулевой точкой шкалы. Такими шкалами являются температурные шкалы Цельсия, Фаренгейта и т.п.

Шкалы отношений отличаются от интервальных шкал только наличием абсолютной естественной нулевой точки. К таким шкалам относятся температурная шкала Кельвина, шкалы измерения массы, длины и т.п.

Абсолютные шкалы являются частным случаем шкал отношений, в которых зафиксирована естественная единица измерения. В подобных шкалах выражают, например, молярные доли содержания веществ, коэффициенты трения, теплопроводности и т.п.

Первые две шкалы являются содержательно бедными и обычно не считаются метризуемыми, хотя, формально, для измерений в номинальных шкалах можно использовать дискретную метрику, а в качестве значений порядковых шкал принимать натуральные числа.

Отсутствие интерпретируемых метрик существенно ограничивает возможности применения методов кластерного или факторного анализа при обработке результатов измерений в номинальных и порядковых шкалах. Тем не менее, такая необходимость возникает при моделировании информационных процессов, идентификаторам которых приписываются, как правило, номинальные значения. В таких значениях выражаются, в частности сигнатуры сетевых атак или кодов вредоносных программ.

Ниже будет приведена формальная процедура отображения номинальной шкалы в декартово произведение интервальных шкал с естественной евклидовой метрикой.

Рассмотрим номинальную шкалу, соответствующую n различным классам объектов и фактор-множество $\Pi = \{\pi_1, \pi_2, .., \pi_n\}$. Определим расстояние между классами π_k и π_s в соответствии с дискретной метрикой

$$\rho_{\Pi}(\pi_k, \pi_s) = \begin{cases} \alpha, \pi_k \neq \pi_s \\ 0, \pi_k = \pi_s \end{cases},$$

где $\alpha > 0$ будет определено позднее. Понятно, что дискретная метрика фактически является индикатором класса и адекватно моделирует измерения в номинальной шкале.

Рассмотрим булеан $B = 2^C$ над n-элементным множеством $C = \{1,2,..,n\}$ с метрикой Фреше-Никодима [2]

$$\rho_B(c_1, c_2) = \mu(c_1 \triangle c_2),$$

где $c_1 \triangle c_2$- симметрическая разность множеств $c_1, c_2 \in 2^C$, а $\mu(c) = |c|$- мощность конечного множества c.

Рассмотрим семейство одноэлементных подмножеств множества C

$$S = \{\{k\} \mid k \in C\}.$$

Определим масштабированную метрику на S

$$\rho_S(\{k\}, \{s\}) = \frac{\alpha}{2} \cdot \rho_B(\{k\}, \{s\}).$$

Определим изометрию $f_1: \Pi \to S$ метрических пространств $\langle \Pi, \rho_\Pi \rangle$ и $\langle S, \rho_S \rangle$

$$f_1(\pi_k) = \{k\}.$$

Представим индикатор подмножества $\{k\} \in 2^C$ в виде кортежа длины n с единицей в k-ой позиции $\chi_k = (0,0,..,1,..,0) \in \mathbb{R}^n$. Обозначим $\rho_{\mathbb{R}^n}$- евклидову метрику на $\mathbb{R}^n$. Понятно, что

$$\rho_\Pi(\pi_k, \pi_s) = \rho_S(\{k\}, \{s\}) = \frac{\alpha}{\sqrt{2}} \cdot \rho_{\mathbb{R}^n}(\chi_k, \chi_s).$$

Полагая $\alpha = \sqrt{2}$ и обозначая

$$\mathrm{X} = \{\chi_k \mid k \in C\} \subset \mathbb{R}^n,$$

определим изометрию $f_2: \Pi \to \mathrm{X}$ пространств $\langle \Pi, \rho_\Pi \rangle$ и $\langle \mathrm{X}, \rho_{\mathbb{R}^n} \rangle$

$$f_2(\pi_k) = \chi_k.$$

Таким образом, измерения в одной номинальной шкале с n классификационными разрядами могут быть интерпретированы как измерения в n интервальных шкалах с евклидовой метрикой.

Обобщим сказанное на случай измерений m различных свойств объекта в номинальных шкалах.

Рассмотрим семейство из m номинальных шкал и соответствующее ему семейство фактор-множеств $\{\Pi_i\}_{i=1}^m$, где $\Pi_i = \{\pi_1^i, \pi_2^i, .., \pi_{n_i}^i\}$. По аналогии с предыдущим определим семейства $\{C_i\}_{i=1}^m$, $\{S_i\}_{i=1}^m$, $\{\mathrm{X}_i\}_{i=1}^m$, где $C_i = \{1,2,..,n_i\}$, $S_i = \{\{k\} \mid k \in C_i\}$, $\mathrm{X}_i = \{\chi_k^i \mid k \in C_i\} \subset \mathbb{R}^{n_i}$.

Обозначим $\Pi^m = \bigotimes_{i=1}^m \Pi_i$– декартово произведение фактор-множеств Π_i $\mathrm{X}^m = \bigotimes_{i=1}^m \mathrm{X}_i \subset \mathbb{R}^{\sum_{i=1}^m n_i}$– декартово произведение множеств X_i.

Обозначим $\pi_{k^m} = (\pi_{k_1}^1, \pi_{k_2}^2, .., \pi_{k_m}^m) \in \Pi^m$, $\pi_{s^m} = (\pi_{s_1}^1, \pi_{s_2}^2, .., \pi_{s_m}^m) \in \Pi^m$, $\chi_{k^m} = (\chi_{k_1}^1, \chi_{k_2}^2, .., \chi_{k_m}^m) \in \mathrm{X}^m$, $\chi_{s^m} = (\chi_{s_1}^1, \chi_{s_2}^2, .., \chi_{s_m}^m) \in \mathrm{X}^m \subset \mathbb{R}^{\sum_{i=1}^m n_i}$, $k^m = (k_1, k_2, .., k_m)$, $s^m = (s_1, s_2, .., s_m)$, и положим

$$\rho_{\Pi^m}(\pi_{k^m}, \pi_{s^m}) = \rho_{\mathbb{R}^{\sum_{i=1}^m n_i}}(\chi_{k^m}, \chi_{s^m}).$$

Вообще говоря, используя скалярное произведение на $\mathbb{R}^{\sum_{i=1}^m n_i}$, можно индуцировать и скалярное произведение на Π^m, полагая

$$(\pi_{k^m}, \pi_{s^m})_{\Pi^m} = (\chi_{k^m}, \chi_{s^m})_{\mathbb{R}^{\sum_{i=1}^{m} n_i}},$$

как это делается, например, во множественном анализе соответствий [3-4]. При таком подходе измерения в одной номинальной шкале трактуются как некоррелированные случайные величины.

Рассмотренная процедура легко обобщается на случай измерений, проводимых одновременно как в номинальных, так и в интервальных шкалах. Ее очевидным недостатком является каскадный рост размерности данных в зависимости от увеличения разрядности номинальных шкал.

Литература

1. Фридман, А Э. Основы метрологии. Современный курс [Текст] / А. Э. Фридман. – С-Пб.: НПО «Профессионал», 2008. – 284 с.: ил.

2. Богачев, В. И. Основы теории меры [Текст]: в 2 т. / В.И. Богачев - Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003.

3. Benzerci J.-P. Analyse des Donnes. Tome 2. L' analyse de correspondences. Paris: Dunod. 1973.

4. Greenacre M. Multiple and Joint Correspondence Analysis / Correspondence Analysis in the Social Sciences (pp.141-161). San Diego, CA: Academic Press. 1994.

О.В. Чернов, М.С. Шкиндеров, Р.М. Гизатуллин

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ МИКРОСЕКУНДНЫХ ИМПУЛЬСНЫХ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ ПО ДВУХПРОВОДНОЙ ЛИНИИ СЕТИ ЭЛЕКТРОПИТАНИЯ ЗДАНИЯ

(Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

Проблема борьбы с электромагнитными помехами, в том числе и преднамеренной ее разновидностью, становятся с каждым годом все более актуальной и в настоящее время рассматривается как неотъемлемая часть задачи информационной безопасности. Еще лет пятнадцать тому назад никто из гражданских потребителей электронных систем и не задумывался, что уже существует такая ветвь информационного терроризма как «электромагнитный терроризм». По определению, электромагнитный терроризм определяется как преднамеренная вредная генерация электромагнитной энергии, создающая помехи или сигналы в электронных системах и тем самым приводящая к сбою, повреждению или разрушению этих систем. При этом одним из наиболее вероятных и опасных путей воздействия преднамеренных электромагнитных помех (ЭМП) на электронные системы является сеть электропитания [1, 2, 3, 4, 5, 6]. Сообщество электромагнитной совместимости, которое имеет значительный опыт разрешения проблем непреднамеренных электромагнитных помех, несёт определенную ответственность по решению этой проблемы и введению разумных стандартов.

Хорошо известно, что в большинстве случаев, электропроводка здания