А. А. Балаев, В. С. Горбатов

МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ PLC-ТЕХНОЛОГИИ С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ ПЕТРИ[1]

Начиная с середины 1990-х годов в научной литературе стали появляться работы, посвященные вопросам выхода в глобальные сети с помощью технологии PLC (Power Line Communications), позволяющей использовать для высокоскоростного обмена данными обыкновенные сети электропитания по стандарту HomePlug AV [1]. Несмотря на заманчивость таких предложений, указанная технология обладает рядом существенных недостатков. В частности, с позиций обеспечения информационной безопасности существует практически неконтролируемая область распространения информации в достаточно широком пространстве сетей по мощным каналам ПЭМИН. Используемые штатные средства PLC-технологии предлагают крайне ограниченный набор функций управления всей областью развертывания сети. Поэтому по сравнению с классическими выделенными каналами передачи данных такая сеть представляется довольно уязвимой с многих точек зрения: относительно легкий доступ к силовым линиям передачи, велика опасность помех и сбоев, связанных с нестабильностью среды передачи данных, что особенно актуально для отечественных силовых сетей. В связи с этим исследование PLC-технологии с точки зрения безопасности передачи данных является достаточно актуальной задачей.

К наиболее значимым для PLC-сетей аспектам безопасности, на наш взгляд, следует отнести обеспечение условий доступности и целостности, так как очевидно, что передача конфиденциальной информации по PLC-сети связана со значительными рисками ее утечки и существенными затратами на их снижение. Покажем, что в указанных аспектах PLC-технология имеет определенный внутренний «потенциал» противодействия, по крайней мере, такой распространенной угрозе, как помехи естественного и/или искусственного происхождения. Этот механизм основан на идее использования поднесущих частот при блокировании основного канала передачи данных. Т. е. в случае внештатных отклонений показателей работы сети передаваемые пакеты перенаправляются по незатронутым атакой дополнительным каналам.

Продемонстрировать возможность такой практической реализации можно с помощью математической модели PLC-технологии на основе аппарата теории сетей Петри (СП) [2], используя подход работы [3], в которой аппарат СП был применен для моделирования процесса устранения неисправности некоторой технической системы.

Основным признаком нештатной ситуации при попытке информационной атаки на PLC-сеть за счет перегрузки и других внешних физических воздействий (помех) на среду передачи данных является нарушение штатного режима передачи информационных пакетов в сети по одной или нескольким поднесущим частотам (всего для передачи данных может использоваться 1536 поднесущих каналов). Для обеспечения устойчивой работы в целом система должна после обнаружения инцидента перевести передачу пакетов на другой канал, который к этому времени либо полностью свободен, либо загружен незначительно. В соответствии со стандартом Home Plug в штатной ситуации в сети имеется как минимум 64 свободных поднесущих частотных канала.

Рассмотрим упрощенный случай, когда ниже установленного критического предела оказывается пропускная способность только одного поднесущего канала. Будем считать, что

[1] Данная работа выполнена в ходе НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

в резерве также имеется один неиспользуемый канал, известны статистические данные об интенсивностях возникновения сбоев в передаче данных по основному каналу и длительности таких операций, как поиск «заглушенного» (заблокированного) канала и/или перенаправления пакетов на другую поднесущую частоту. По аналогии с [3] на рис. 1 представлена соответствующая модель PLC-технологии на основе СП.

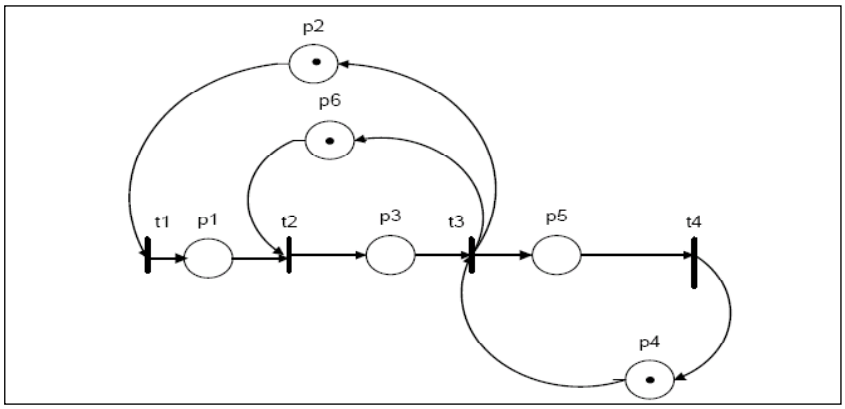

Рис. 1. Упрощенная модель безопасности PLC-технологии

Для нашего случая данная модель представляется в виде следующих основополагающих понятий аппарата СП — события и условия:

События	Предусловия	Постусловия
1	Нет	б, в
2	а, б, в	г, д
3	г, д	е, ж, а
4	Ж	нет

где условиями являются:

а) штатный режим работы системы;

б) инцидент (обнаружен сбой в системе);

в) обнаружена «заглушенная» частота поднесущей (отказ поднесущей);

г) подбор свободной (или малозагруженной) частоты поднесущей для перенаправления потока пакетов;

д) выбор новой частоты поднесущей для перенаправления потока пакетов;

е) замена частоты поднесущей;

ж) инцидент устранен.

Событиями для рассматриваемой сети являются:

1 — поступление сигнала о нештатной ситуации;

2 — поиск «заглушенной» частоты;

3 — подбор новой частоты поднесущей и перенаправление потока пакетов;

4 — восстановление системы.

При таких параметрах по аналогии с выводами работы [3] значение позиции p2 (фишка) есть число имеющихся в системе поднесущих частот (в нашем упрощенном случае количество поднесущих равно 1). Переходы соответствуют следующим событиям: t1 — отказ в передаче пакетов на данной частоте; t2 — обнаружение «заглушенной» частоты; t3 — замена частоты поднесущей и перенаправление потока пакетов; t4 — восстановление системы.

При наличии фишки в позиции ρ2 переход t1 срабатывает, но с задержкой, равной вычисленному случайному значению моделируемого отрезка времени между отказами (Рис. 1). После выхода фишки из t1 она попадает через ρ1 в t2. Если фишка находится в позиции ρ6, то это означает, что система располагает необходимыми ресурсами и может начать поиск «заглушенной» частоты. В переходе t2 фишка задерживается на время, равное значению длительности поиска «заглушенной» частоты. Далее фишка оказывается в ρ3, и если имеется свободная частота для поднесущей (фишка в ρ4), то запускается переход t3, из которого фишки войдут в ρ2, ρ5 и ρ6 через отрезок времени, требуемый для замены частоты поднесущей. После этого в t4 моделируется восстановление работы системы [3].

Таким образом, получена достаточно перспективная, на наш взгляд, математическая модель для исследования определенных аспектов безопасности функционирования сетей передачи данных на основе PLC-технологии. В частности, рассмотренную упрощенную модель поиска и замены одного «заглушенного» канала можно достаточно легко распространить на всю совокупность поднесущих частотных каналов.

Для развития предложенного подхода можно также воспользоваться результатами работы [4], в которой аппарат раскрашенных сетей Петри использован для моделирования процесса временно пораженного фрагмента PLC-сети, что является технически сложной задачей. Для реализации подобного механизма контроля работы PLC-сети в стандарте HomePlug AV используется протокол CSMA-CD и CSMA-CA, идея которого также состоит во множественном доступе с контролем несущей и обнаружением и/или устранением коллизий.

СПИСОК ЛИТЕРАТУРЫ:

1. Global Standards Initiatives of the HomePlug Powerline Alliance. URL: http://www.homeplug.org/tech/global_standards//.
2. *Котов В. Е.* Сети Петри. М.: Наука, 1984. – 160 с.
3. *Топольский Н. Г., Фирсов А. В., Афанасьев К. А.* Моделирование процесса устранения неисправности сетями Петри // Технологии техносферной безопасности. 2007. Август. Вып. 4. URL: http://ipb.mos.ru/ttb/2007-4/2007-4.html
4. *Zaitcev D. A.* An Evaluation of Network Response Time Using a Colored Petri Net Model of Switched LAN // Proceedings of Fifth Workshop and Tutorial on Practical Use of Colored Petri Nets and the CPN Tools. October 8–11. 2004. Aarhus, Denmark. P. 157–167.