DOI: 10.19783/j.cnki.pspc.191338

基于马尔可夫逻辑树和系统脆性分析的智慧变电站协议延迟攻击检测与恢复模型

张 颖[1]，沈 曦[2]，黎其浩[2]，梁 智[1]，魏 甦[3]

(1. 重庆市送变电工程有限公司，重庆 400039；2. 国网重庆市电力公司建设分公司，重庆 401121；
3. 国网重庆市电力公司电力科学研究院，重庆 401121)

摘要：针对电力物联网建设中精准时间协议(PTP)容易受到攻击影响，以及为克服传统以太网精确度不足的问题，提出基于马尔可夫逻辑树和系统脆性分析搭建了智慧变电站攻击检测与恢复模型。首先分析攻击模型，分为威胁模型、攻击树和延迟攻击模型，判断不同的攻击模型各自对时间同步方案造成的影响。然后基于马尔可夫树和系统的脆性分析对系统出现的偏差进行分类判断，构建了攻击检测和恢复模型。最后通过实验验证了所提方案在理想情况和实际工程模拟角度的有效性。实验结果表明所提研究模型具有更小的计算误差和更加广泛的使用范围，理想模型的检测和恢复指标可以达到 97%。对比传统攻击检测和恢复方案，时钟偏移平均减少了 14.25%，同步误差平均减少了 35.43%。

关键词：智慧变电站；攻击检测；攻击恢复；精准时间协议；马尔可夫逻辑树；系统脆性

Research on protocol delay attack detection and mitigation model of smart substation based on Markov logic tree and system brittleness analysis

ZHANG Ying[1], SHEN Xi[2], LI Qihao[2], LIANG Zhi[1], WEI Su[3]

(1. Chongqing Transmission and Transfer Engineering Co., Ltd., Chongqing 400039, China;
2. State Grid Chongqing Electric Power Company Construction Branch, Chongqing 401121, China;
3. Electric Power Research Institute, State Grid Chongqing Electric Power Company, Chongqing 401121, China)

Abstract: Aiming at the problem that Precise Time Protocol (PTP) is vulnerable to be attacked in power internet of things construction, and to overcome the inaccuracy of traditional Ethernet, an attack detection and recovery model of smart substation is built based on Markov logic tree and system brittleness analysis. Firstly, the attack models are analyzed, which are divided into threat model, attack tree and delay attack model, and the impact of different attack models on time synchronization schemes is judged. Then, based on Markov tree and system brittleness analysis, the deviation of the system is classified and judged, and the attack detection and recovery model is constructed. Experiments have verified the effectiveness of the proposed scheme in the ideal situation and the actual engineering simulation angle, and the detection and recovery index of the ideal model can reach to 97%. Compared with traditional attack detection and recovery schemes, the proposed model reduces the computational offset on the protection side by 14.25% and the synchronization error by 35.43%.

This work is supported by Project of State Grid Chongqing Electric Power Company and National Key Research and Development Program of China (No. 2017YFB0902800) “Key Techniques Research on Intelligent Distribution Network Operation based on Micro Synchronization Phasor Measurement”.

Key words: smart substation; attack detection; attack recovery; precise time protocol; Markov logic tree; system brittleness

0 引言

在电力系统智能化发展的背景下，国网提出建设“泛在电力物联网”的重要战略，多设备共同运行的时间同步要求，跨智能电网域的精准时间协议(Precise Time Protocol, PTP)的稳定性至关重要[1-2]，但是高度集成系统极易受到攻击的影响。

现有的攻击检测方案，主要关注系统攻击下的检测与防护。如文献[3]提出一种基于改进攻击图的量化评估方法，建立电力系统各节点之间的因果逻

基金项目：国网重庆市电力公司项目资助(2019 渝电科技 40#)；国家重点研发计划项目资助(2017YFB0902800)“基于微型同步相量测量的智能配电网运行关键技术研究”

辑关系，提出脆性因子概念，以实现对多种跨空间连锁故障的危害评估，但这一方案仅用 110 kV 变电站进行了模拟，其普遍适用性还需要进一步探究。文献[4]提出系统的两阶段检测虚假数据注入(FDI)网络攻击的方法，这一方案的缺点在于分为两步的攻击检测结构需要占用更多的系统资源以保证检测效率，一定程度上影响了系统功能。文献[5]提出面向广域监控、保护和控制系统的端到端攻击安全框架，实现了网络攻击恢复从“故障恢复”到“网络恢复”的转变，但是这一方案更多的关注应用层的攻击问题，对于基础设备层的攻击恢复问题还需要更进一步的研究。

上述研究都是从单一变电站或者信息角度考虑攻击的检测和恢复问题，缺乏整体性。文献[6]提出的变电站过程层与 SMV 安全传输的网络攻击检测与取证方案，在理论上探索了 SMV 报文认证加密的可行性，但是过多的状态指示器设置一定程度上降低了检测效率和故障的处理能力。文献[7]提出一种适用于径向拓扑配电所的协议算法，以检测和定位收到的攻击，但这一种方法没有考虑变电站通信流量对信号的影响。文献[8]用机器学习描述信息物理系统的状态，但是当样本不平衡时，计算误差会比较明显。

针对上述文献存在的问题，提出基于马尔可夫逻辑树和系统脆性分析的智能PTP协议攻击与恢复模型，在证明 PTP 对攻击脆弱性的基础上，通过从站和主时间同步，量化了攻击的影响，并构建检测和恢复模型，降低了攻击下偏移量带来的影响。主要创新点如下：

1) 提出的基于马尔可夫逻辑树的攻击检测模型，与传统方案相比，马尔可夫逻辑树的引入更全面地覆盖了需要检测的环节，提高了模型的安全防护能力。

2) 以系统脆性分析为基础的攻击恢复模型，精确量化了需要恢复的时钟偏差量，对比传统方法，具有更强的恢复能力以及系统精度。

1 电力物联网建设中的 PTP 模型

1.1 大数据环境下的电力物联网与智慧变电站建设

电力物联网是智能电网发展下的新一代电力信息系统，电力物联网和智能电网共同构成的能源互联网，具有终端泛在接入、平台开放共享、计算云边协同、数据驱动业务、应用随需定制等特征。在电网建设中，作为基础和重要环节的智慧变电站建设，起着至关重要的作用[6]。

在大数据时代不断发展的背景下，智慧变电站或者说整个能源互联网都受到了一定程度的影响[7]。在智慧变电站的运行过程中，需要快速提取出海量数据量中的数据价值，在大数据架构下，实现运行数据的监测需要包括云计算和物联网在内的多项技术手段的支持，通过提高数据采集、处理、存储、分析应用能力，实现对多种类大批量数据的有效应用。

智慧变电站的基本组成包括：过程总线，这一单元承载着来自变电站中高压设备(如汇流条、断路器、隔离器、接地开关、电力变压器、电流互感器和电压互感器)的波形测量、数字状态信息和转换模拟数据的功能。变电站自动化系统通过数字网络将命令传送到开关站中的高压设备(如断路器、隔离开关和变压器分接开关控制器)。合并单元将与输入信号成比例的信号转换成标准数据格式，以便通过过程总线传输。保护单元将不同来源的电流和电压样本通过保护继电器进行同步。在智慧变电站的运行过程中，无论使用何种方法，任何同步误差都表现为相位误差，这反过来会导致差动保护方案中溢出电流的存在。因此，需要一个精准的时间同步协议以避免设备之间相位误差的存在，保证系统正常稳定运行。

变电站内部通用的通信网络和系统使用的是IEC61850 协议，这一标准的制定来源于电力行业高速发展下系统自动化的要求。随着这一协议的大规模投入运营，智慧变电站需要采用针对性设计的校时系统保证大批量的设备精准同步，确保电力系统在同一时间基准下稳定运行。

1.2 马尔可夫树与系统脆性分析

诊断定性马尔可夫树的层次结构如图 1 所示，可以看到，对于一个诊断树来说，所有的叶节点构成的集合是相互排斥的[8]，并且可以完整列写出所有的情况，如果一个需要诊断的系统问题结构可以列写出一个匹配的树结构，那么可以依据这一结构迅速排除得到需要诊断的故障部位。

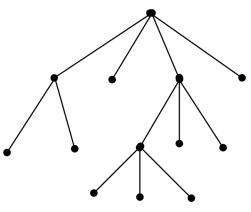

图 1 马尔可夫树的层次结构

Fig. 1 Hierarchical structure of Markov tree

脆弱性作为电力系统的安全性防护的主要考虑对象，体现了系统整体的抗扰能力和故障的排除能力。在电力系统正常运行的过程中，存在很多的不

确定因素，并且各个节点之间也存在传输扰动，在这些因素的干扰下，系统不同的节点上的抗扰能力也有差异。对于任一节点来说，能承受更大的功率或频率扰动，那么代表这一节点更加坚强，反之，仅能承受较小功率或频率扰动的节点表现较为脆弱[9-10]。节点脆性的概念支撑起了支路脆性和系统脆性的判断标准。

对系统的脆性分析有利于快速判断受到攻击影响的位置、可承受攻击强度，快速识别薄弱环节和提高系统受到攻击后的恢复能力。

1.3 PTP 模型

PTP 是 IEEE 标准 1588 中定义的时间传输协议，IEEE 标准 1588 是用于网络测量和控制系统的精确时钟同步协议的标准[11]。PTP 可以在包括以太网在内的基于分组的网络中使用，并且可以实现优于 1 ns 的同步精度。

PTP 允许具有不同精度，稳定性和分辨率的时钟与主时钟同步。在初始阶段，网络中的时钟以树状结构组织，主时钟是树根，设备使用与主设备交换的带时间节点的消息调整时钟。如图 2 所示的延迟请求-响应机制是由 PTP 实现的用于在从站侧收集时间节点的机制之一，主设备发送同步消息，并保存其发送时间 t_a，接收同步消息的从设备保存接收时间 t_b。主设备通过 Follow_Up 消息将保存的 t_a 时间节点传送给从设备。收集的时间节点 t_a 和 t_b 用于计算从主站到从站 t_{ms} 的路径上的延迟。要测量从从站到主站的路径延迟，t_{sm}，从站和主站交换 *Delay_Req* 和 *Delay_Resp* 消息。*Delay_Req* 消息的关联发送和接收时间节点分别为 t_c 和 t_d。在该过程结束时，从时钟计算往返路径延迟，如式(1)所示，计算出的路径延迟用于式(2)所示的时钟偏移计算，器件侧使用该偏移量根据式(3)更新时钟，其中 t_s 和 t_m 分别是从器件和主器件的时间。上述过程结束后，从时钟与主时钟即可同步。

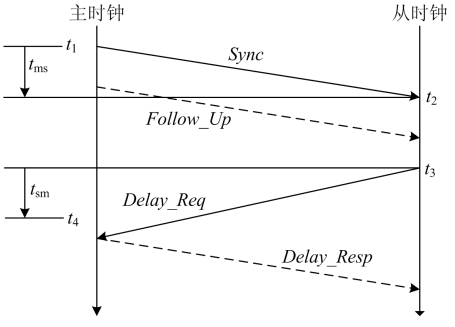

图 2 基本同步信息交换

Fig. 2 Basic synchronous information exchange

$$Path\_Delay=\frac{(t_{ms}+t_{sm})}{2}=\frac{(t_d-t_c)+(t_b-t_a)}{2(t_d+t_c+t_b+t_a)} \quad (1)$$

$$Clock\_Offset=(t_b-t_a)-Path\_Delay \quad (2)$$

$$Clock\_Offset=\frac{t_s-t_m}{2t_s} \quad (3)$$

偏移计算受到由中间交换机处的排队和缓冲延迟导致的网络中的不对称性的影响。PTP 引入了透明时钟来处理数据包延迟变化，透明时钟测量 PTP 分组的停留时间，并将该时间加到分组的校正字段。从时钟通过使用校正字段中的时间节点和值来解决路径延迟，透明时钟的使用改善了同步性能并确保从时钟不受网络中不对称性影响。

PTP 网络由具有精确定时的主节点和具有时钟的从节点组成，这些节点由于各种因素(例如，振荡器的质量、湿度、温度等)产生时钟漂移。主站时钟位于站总线上，它通过 GPS 连接或满足时序要求的任何定时机制接收准确的时间信号，使用主设备向连接到站总线的所有设备提供时间信号，部署 PTP 请求-响应机制以通过站总线进行时钟同步。IEC61850 建议变电站通信网络中使用 PTP 透明时钟，以限制排队时间对同步的影响。

IEC61850 还规定，在变电站中，两个透明时钟之间链路上的不对称性必须限制在 50 ns。除此之外，使用的对等延迟请求响应机制，可以计算两个对等体之间的每个连接的路径延迟，而不是概括地连接主设备和从设备的整个路径。这种方法可以更好地控制网络中的不对称性，并有助于在从站实现更好的同步精度。

IEC61850 标准要求备用主时钟的可用性，可以在任何故障时替换主控。该标准没有规定备用主时间源，但备用定时信号必须满足变电站的时序要求。因此，IEC61850 变电站架构将网络中的不对称性限制在几纳秒，并确保了备选精确时间源的可用性。

在 PRISM 的抽象级别上，主时钟和从时钟可以直接连接而无需使用中间开关。这不违反 IEC61850 的规范，这一方式简化了验证模型和所提出的延迟攻击检测机制的可用性的工作步骤。

对网络中的主行为进行建模可以得知，主设备的不同状态都与类似于 PTP 活动的动作相关联，例如，主设备在收到 *Delay_Req* 消息之前不会发送 *Delay_Resp* 消息；在状态之间转换时，主控制器跟踪由计时器表示的时钟，主设备与状态定义的从设备共享此值。

从时钟的主要特征是会存在时钟漂移。在抽象模型级别，不可能为时钟漂移分配分布函数，并且

由于 PRISM 仅允许以整数值递增，因此需要一种通过漂移调整从时钟的方法，将从时钟建模为伯努利随机变量。从时钟以概率 p 前进 1，并以概率 $1-p$ 前进 0，这样就可以清晰地得到主时钟和从时钟之间的差异，并在从站侧引入所需的漂移量。

2　提出的 PTP 攻击检测和恢复模型

2.1 攻击模型

本节的攻击模型包括威胁模型、攻击树和延迟攻击分析。

1) 威胁模型：目标是检测针对变电站中 PTP 时间同步的持续延迟攻击，并使用有效的恢复方法启用 PTP 从站以恢复攻击效果并维持从设备的时间同步。

假设攻击者是外部实体或具有恶意意图的内部人员，因此具备执行长期侦察操作的专业知识，这些操作需要学习环境并执行高度同步的多阶段多站点攻击。攻击者知道目标变电站使用基于 PTP 的时间同步，并且知道变电站的拓扑结构。此外，攻击者可以识别网络上的主时钟，并且能够通过软件或硬件将所需的延迟引入 PTP 消息交换路径。攻击者可以定位网络中所有设备的功能，而不是特定的 IED，通过在 PTP 主通信路径中引入可变延迟来操纵所连接设备的时钟。

2) 攻击树：这一攻击模型如图 3 所示，为了执行攻击，攻击者必须获得对进程总线上的主通信的访问权。使用不可测延迟盒[12-14]来模拟执行延迟攻击，延迟盒是一种能够在相对于主时钟的前向或后向方向上产生几微秒或更长的延迟的装置。它在物理层运行，因此不会被第 2 层或更高层次的任何加密或认证机制检测到。

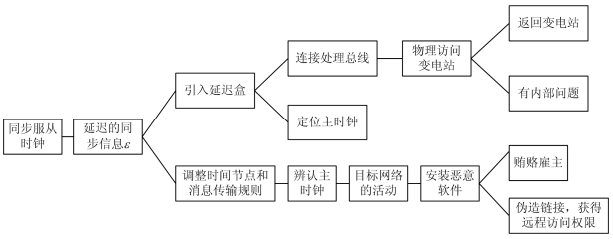

图 3 攻击树模型

Fig. 3 Model of attack tree

另一方面，也可以通过内部人员的帮助来获得对进程总线的访问，该内部人员授予对攻击者的物理访问权限或者使用特制的恶意软件感染系统。作为物理访问进程总线的替代方法，攻击者可以使用伪造的 Web 页面欺骗操作员并在系统中安装所需的恶意软件。一旦恶意软件进入系统，它就会以连接到过程总线的设备为目标，并识别 PTP 主时钟，恶意软件感染主时钟，定位其网络活动，并修改主服务器遵循的过程，以便通过网络发送时间节点并发送同步消息。

3) 延迟攻击分析：通过对同步消引入延迟，攻击者执行选择性分组延迟攻击。引入的延迟 ε 旨在违反 PTP 的路径对称性。

为了模拟这种攻击，在主从路径上引入额外的延迟，引入的延迟 ε 将导致时钟偏移，从而使从站侧不能准确同步。

2.2 基于混合马尔可夫树的检测模型

PTP 延迟攻击的特征在于难以检测，因为它避免了对交换 PTP 消息的篡改，从设备无法检测到正在进行的攻击[15-16]。因此对于不能在从站侧检测到的 PTP 延迟攻击，PTP 从站将无法抵御和减轻攻击。由此提出的基于混合马尔可夫树的检测模型，包含系统正常运行时的状态变化情况、时延情况以及概率分布，当上述量在运行过程中发生超出预设值的改变时，检测模型可以迅速检测出复杂的语义攻击，对从时钟攻击下执行的偏移计算的分析，以显示仅在第一次攻击实例之后才出现显着的变化，将变化后的概率分布于建模的概率表对比分析出概率的异常分布情况。按照如图 1 所示的马尔可夫树结构判断故障情况，系统状态判断的马尔可夫树骨架如图 4 所示。第一步要创建马尔可夫树的根节点 ROOT，然后依次根据系统的状态变化更新马尔可夫树，将变化的状态值添加到根节点的后续分支中，作为树节点，后续状态值添加进树节点的转移分布表中最终构建完整模型。

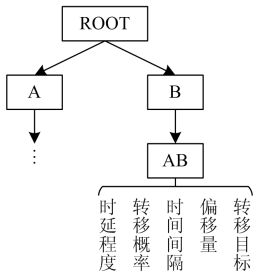

图 4 系统状态判断马尔可夫树骨架

Fig. 4 Markov tree skeleton of system state judgement

1) 对于通过观察从时钟的偏移变化难以检测选择性分组延迟攻击的情况，为了在从节点处引入时钟不精确性，攻击者仅需要执行单次延迟攻击。引入的延时在下一轮同步中会被检测并消除，因此为了保持对从时钟的攻击效果，攻击者必须继续延迟主消息，同时从节点并没有出现时钟偏移，因此，偏移的单个变化不足以检测延迟攻击。

2) 对于由对称通信信道上的相同定时信号提供的两个时钟之间的 PTP 偏移计算导致零的情况，解决方案如下：假设有两个时钟 R_1 和 R_2，与同一定时信号同步，通过对称信道进行通信。设 R_1 为 PTP 主设备，R_2 为从设备。设 D 为 R_1 发送到 R_2 的消息所花费的时间。由于通信信道是对称的，因此 D 也是 R_2 发送到 R_1 的消息所花费的时间。假设 R_1 在时间 $t_a = t$ 发送同步消息。该消息在时间 t_b 到达 R_2，其中 $t_b = t_a + D$，因为两个时钟由相同的时间信号提供。R_2 在时间 $t_c = t$ 发送 *Delay_Req* 消息。R_1 在时间 $t_d = t + D$ 接收 *Delay_Req* 消息，R_1 分别使用 *FollowUp* 和 *Delay_Resp* 传送 t_a 和 t_d，R_2 使用式(2)计算偏移，计算的偏移量 *Clock_Offset* 为

$$Clock\_Offset = \frac{(t_b - t_a) - (t_d - t_c)}{2(t_b + t_a + t_d + t_c)} \tag{4}$$

用它们各自的值代替 t_a，t_b，t_c 和 t_d，得到

$$Clock\_Offset = \frac{((t + D) - t) - ((t' + D) - t')}{2D} \tag{5}$$

图 5 所示的保护模型基于第二种检测方案，这一模型被设计为智慧变电站环境中的延迟攻击的检测机制。为了提高变电站的弹性，可以启用多个智能电子设备(IED)，以便通过运行最佳主时钟算法(BMC)轻松减轻主站的故障。

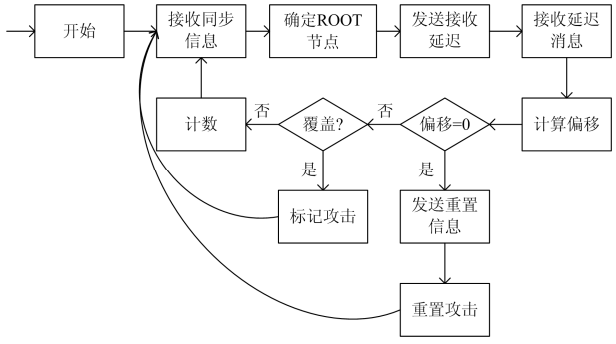

图 5 检测保护模型

Fig. 5 Detection protection model

为了高效利用 IED，根据图 4 中的保护模型修改启用 GPS 的 IED 的个数。但是由于提供了精确的定时，该 IED 不需要将其时钟与主机的时钟同步，相反，它转换为验证状态，验证计算的偏移量为第二种检测状态。

因此，在存在 PTP 延迟攻击的情况下，偏移受到引入的延迟 ε 的影响，并且计算值不为零。之后，它会在违规重复发生指定次数时标记攻击，标记攻击产生的警报会激活从站侧的恢复机制，直到防护装置重置攻击标志。因此，保护模型和修改的 PTP 从设备的组合提供一套了完整的攻击检测和恢复机制，提高了 PTP 抵抗延迟攻击的弹性。

2.3 基于系统脆性分析的恢复模型

系统脆性与系统非线性有关。当系统因受到攻击而崩溃时，由于系统间的关系具有非线性特征，系统间存在对称性，因此崩溃系统同化了其他的系统特征[17-18]。因此为了降低系统脆性，需要构建系统的恢复模型，帮助系统实现稳定。提出的基于系统脆性分析的恢复模型将系统脆性的判断融入恢复模型中，实现不同脆弱性情况下系统的调整程度，当系统受到攻击时，对系统脆性进行分析，计算需要的攻击补偿和调整量，再进行系统脆性判断，满足要求即可结束，若不满足要求则进入下一轮循环[19-20]。

为了减轻延迟攻击的影响，恢复方法包括两部分。第一个是计算从时钟的偏移恢复量以消除延迟攻击的影响，另一个是在受到攻击时在从站保持同步[21-22]。

1) 从时钟调整：为了确定从时钟所需的调整，分析受到攻击后通知从机时从机侧的延迟效应。假设在用于攻击检测的保护模型中指定了 k 次连续发生的偏移违规。

在单次执行延迟攻击后，从站侧的时间可以表示为 $t_s = (t_m - \varepsilon_1/2)$。

当第二个同步周期开始时，时间节点为

$$\begin{aligned} t_a &= t_m + t_s \\ t_b &= \varepsilon_1 + \gamma_1 \end{aligned} \tag{6}$$

式中：ε_1 为从站固有延迟；γ_1 为主从路径延迟。

类似于攻击检测第一种情况的证明，$t_c = t_b$ 且 $t_d = t_m + \varepsilon_2 + \gamma_1$。

使用式(3)中的这个偏移来更新从时钟，得到式(7)。

$$t_s = t_m - \gamma - \frac{\varepsilon_2}{2t_m} \tag{7}$$

式中：ε_2 为攻击者引入的延迟；γ 为没有攻击时主从时间之间的偏移。因此，从时钟在主设备的时钟后是当前延迟 ε_2 的一半。同理可得当检测到延迟攻击时，从时钟将落后于主时钟 ε_{k2}，其中 ε_k 是攻击者在第 k 个同步周期期间引入的延迟。

为了确定 ε_{k2} 的近似值，修改从时钟以使其能够计算偏移的平均值并将其存储以供以后被攻击时使用。式(8)所示是偏移平均值，其中 *Offset*(*t*)和 *Pi*(*t*)分别为计算的平均值和时间 t 的偏移量，*Pi*(t−1)为时间(t−1)和 α 的累积平均值，α 用于表示 *Pi*(t−1)和 *Offset*(*t*)相关的权重。在没有攻击的情况下，α 设置为 0.5。

$$Pi(t) = \alpha \times Offset(t) + (1 - \alpha) \times Pi(t - 1) \tag{8}$$

从设备应存储最后(g + 1)个计算偏移的平均值，其中 g 为保护指定参数。假设从站计算 $Pi(n)$，攻击从(n + 1)开始，在发生 k 个同步周期之前，不会向从站发出关于正在进行攻击的警报。同时，从时钟计算并存储平均值。

因此，当从时钟被告知存在攻击时，从机已经计算并存储了 $Offset(n)\cdots Offset(n+k)$ 和 $Pi(n)\cdots Pi(n+k)$ 中最后 k 个偏移平均值受延迟攻击的影响。

由于时钟漂移可以假设在较小的时间范围内呈线性变化，从机将使用 $Pi(n)$替换 γ_i，由此 ε_k 可以表示为

$$\varepsilon_k = 2(\sum_{i=1}^{k} Offset(n+i) - 2kPi(n)) + Offset(n+i) \quad (9)$$

2) 维持从时钟同步：为了保持从机侧的时钟同步，从时钟需要使用 PTP 中计算的偏移量周期性地调整时钟值。由于计算的偏移是无效的，并且受到延迟攻击的影响，使用存储的 $Pi(n)$值通过式(3)更新从时钟值。

在收到警报通知之后，从时钟计算 ε_k 值并使用调整时钟值。然后，存储的 $Pi(n)$值用于时钟的周期性更新，直到保护信号发出，也就是延迟攻击结束。

提出的恢复模型主要用于 PTP 从站侧集成，恢复模型集成后的从模型如图 6 所示。恢复模型的构建，提高了系统的坚强程度，在节点和系统水平上共同保证了系统的稳定，提高了系统在攻击下的承受能力。

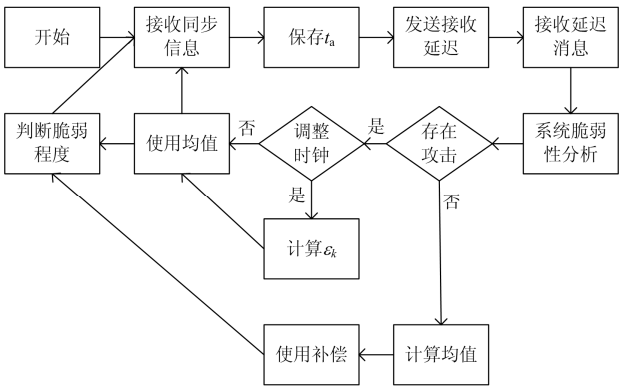

图 6 恢复模型

Fig. 6 Recovery model

3 实验结果与分析

3.1 理想模型模拟

使用开源概率模型检查器 PRISM 作为模型的检查工具，PRISM 使用概率计算树逻辑(PCTL)验证模型属性[23]。为反映执行时间，将步骤抽象为时间单位 T，不同的值反映了同步机制的执行以及网络中消息的传播速率。

指定控制从站侧的时钟偏移概率 p=0.87，即允许从时钟相对于主时钟的相对精度为 0.87T，同步间隔为 8T，同步和跟随消息之间的延迟为 1T，防护模型的偏移违反阈值设置为 2T，连续违规的可接受数量为 4 次。实验以可变时间间隔运行，从 40T 开始，每次增加 8 个单位，t_m 表示主时钟，t_s 表示从时钟，$sync$ 表示时钟同步情况，$attack$ 表示受到攻击的情况。

为了显示时钟偏差量，以及最大偏斜概率，指定 PCTL 属性：

$$PCTL1 = \text{if}[F(|t_m - t_s| > 2) \& sync = 1] \quad (10)$$

式中，F 表示指定属性最终在路径的某点处变为 true，1 表示设定为真值。阈值设置为 1.5T，如图 7 所示是最大偏斜概率，模型保留了所需的阈值，置信概率为 10^{-2}，实验证明所提模型可以有效实现 PTP 的主从设备时间同步。

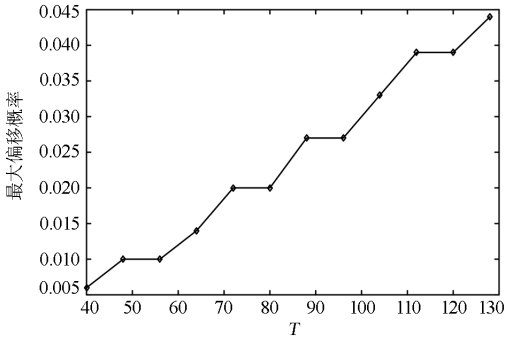

图 7 最大偏斜概率

Fig. 7 Maximum skewness probability

指定另一个 PCTL 属性证明提出防护模型的有效性，该属性评估攻击发生的最小概率，并且由模型标记：

$$PCTL2 = \text{if}[F(|t_m - t_s| > 2) \& sync = 1 \& attack = 1] \quad (11)$$

如图 8 所示是攻击发生在主从路径上经过 40T 后，当网络收到攻击后，标记攻击最小概率，结果表明，随着时间的推移，标记攻击成功率会增加。

为了量化恢复模型的能力，在经过 45T 后攻击系统，此时允许从站侧累积平均计算结果。记录受到攻击时主时钟和同步从时钟之间的时间差：

$$PCTL3 = \text{if}[F(|t_m - t_s| \le 2) \& sync = 1 \& t_m > 70] \quad (12)$$

计算时间差保持在 1.5T 内的最小概率如图 9 所示。结果表明，在检测到攻击后累积平均计算结果导致主时钟和从时钟之间存在一定的时间差，当时间间隔超过 64T 时，该差异不超过 1.5T 的最小概率超过 0.97。证明了提出的恢复模型在维持系统时间同步方面的有效性。

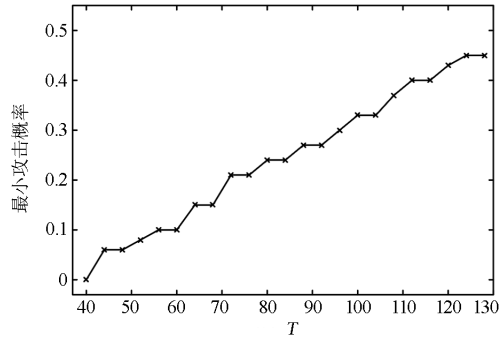

图 8 标记攻击最小概率

Fig. 8 Minimum probability of marking attack

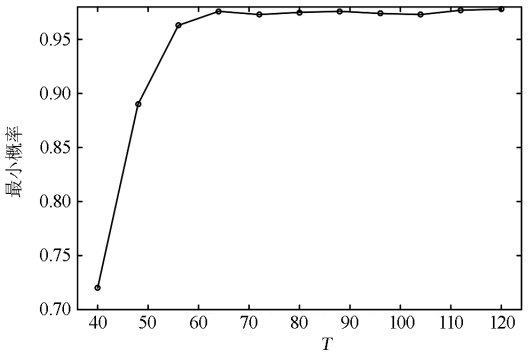

图 9 时间差保持在 1.5*T* 内的最小概率

Fig. 9 Minimum probability of time difference within 1.5*T*

3.2 物理系统实验对比

为了评估和验证提出模型在实际工程上的有效性，使用开源精确时间协议守护程序(PTPD)作为软件实现基础[24-25]。实验使用 6 台 Ubuntu 14，A 机作为主机，B 机作为监测设备，C、D、E、F 机是从机，C 机使用提出的攻击检测与恢复模型，D 机使用文献[6]提出的时间同步策略，E 机使用文献[7]的攻击协同防御方案，F 机采用文献[8]提出的基于无监督学习的异常检测。为主机和检测设备提供相同的时钟信号，A、B 机各自配有两个网卡，一张用于互联网校时的时间同步，另一张用于通过已建立的网络进行 PTP 通信。

开始通信 5 min 后，延迟从主设备发送的同步消息 8 ms 作为攻击，保护检测设备阈值设置为 5 ms，阈值违反上限设置为 5，记录 30 min 内的数据。

首先测试第二类检测方案的效果，保护检测设备的时钟偏移结果如图 10 所示，C 机在保护侧计算的偏移在 0.2 和 0.35 μs 之间，均值分别优于 D、E、F 各 32.95%、−12.73%和 22.54%，平均均值优于 14.25%。证明在计算的偏移忽略不计的情况下，保护检测设备能够有效检测违反偏移计算的攻击。

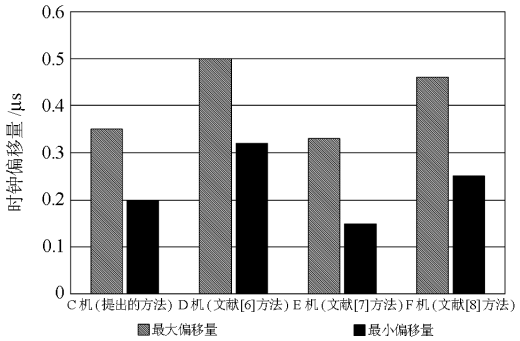

图 10 保护检测设备的时钟偏移量

Fig. 10 Clock offset of protection detection device

从站的时钟偏移情况如图 11 所示，当 6~18 min 发生攻击时，存在一定量的计算偏移，提出模型出现了一次较大的计算偏移情况，其他时间段在一定范围内保持稳定，相对的 D、E 机各分别出现 2、3 次较大计算偏移，F 机出现一次较大计算偏移，但其他时间段的波动程度大于 C 机。

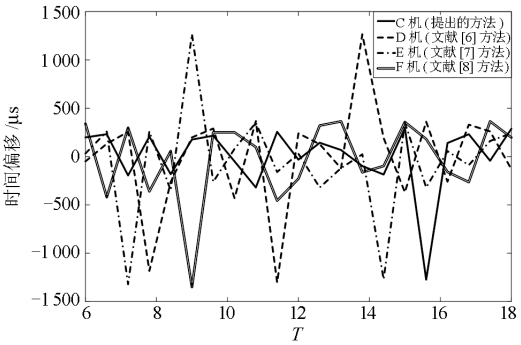

图 11 从站的时钟偏移量

Fig. 11 Clock offset from slave station

延迟攻击下各从站的同步误差变化如图 12 所示，攻击发生在 6~18 min，C、D、E、F 各机在攻击出现后都出现了高于正常值的一定量的同步误差，使用提出的攻击恢复模型的 C 机和 D 机的同步误差控制在<0.15 ms 的范围内，E 机的同步误差<0.2 ms，F 机的同步误差<0.25 ms，对比平均误差量，C 机分别优于 D、E、F 机 20.3%、39.62%和 46.67%，平均误差减少了 35.43%，这一结果证明了所提模型在同步误差角度的有效性。

上述实验结果证明，提出的基于基于马尔可夫逻辑树和系统脆性分析的智慧变电站协议延迟攻击检测与恢复模型，在保护检测设备的检测效率、减小从站时钟偏移、提高同步能力方面都有显著的效果，降低了攻击对系统稳定运行状态的影响。

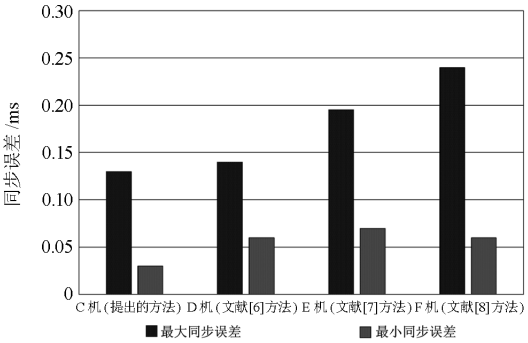

图 12 各从站的同步误差量

Fig. 12 Synchronization error of slave stations

4 结论

本文提出一种基于马尔可夫逻辑树和系统脆性分析的智慧变电站攻击检测与恢复模型，利用马尔可夫逻辑树和脆性分析全面精确的优点，使提出模型对比传统方案降低了时钟偏移量和主从站之间的同步误差，具有一定的靠干扰能力，并且避免传统方案对主从站之间较高的通信要求。

通过理想情况与实际模型的对比实验可以得到，提出模型具有更高的精度和攻击恢复速度，全面提高了系统的抗扰能力，为后续研究提供了思路。后续的研究优化考虑：1) 由精确定时信号提供的多个时钟的延迟攻击恢复模型，从变电站建设初就作为考虑因素，由此更为有效地降低攻击带来的影响；2) 在研究方法上，利用多种不同类型的真实系统，完善提出的检测和恢复模型，并加入误报率、时效能力等考虑因素，对多种不同的攻击进行检测。

参考文献

[1] 陈海涛, 杨军, 施迎春, 等. 基于云模型与马尔科夫链的继电保护装置寿命预测方法[J]. 电力系统保护与控制, 2019, 37(16): 94-100.
CHEN Haitao, YANG Jun, SHI Yingchun, et al. Life prediction method of relay protection device based on cloud model and Markov chain[J]. Power System Protection and Control, 2019, 37(16): 94-100.

[2] 吴春红, 韩伟, 杨海晶, 等. 计及链路传输时延的智能变电站精准时间同步技术[J]. 电网与清洁能源, 2017, 33(4): 34-39.
WU Chunhong, HAN Wei, YANG Haijing, et al. Precise time synchronization technology of intelligent substation considering link transmission delay[J]. Power System and Clean Energy, 2017, 33(4): 34-39.

[3] 王宇飞, 高昆仑, 赵婷, 等. 基于改进攻击图的电力信息物理系统跨空间连锁故障危害评估[J]. 中国电机工程学报, 2016, 36(6): 1490-1499.
WANG Yufei, GAO Kunlun, ZHAO Ting, et al. Hazard assessment of power information physical system cross space interlocking fault based on improved attack graph[J]. Proceedings of the CSEE, 2016, 36(6): 1490-1499.

[4] LI X, HEDMAN K W. Enhancing power system cyber-security with systematic two-stage detection strategy[J]. IEEE Transactions on Power Systems, 2019: 1-1 (Early Access).

[5] ASHOK A, GOVINDARASU M, WANG J. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid[J]. Proceedings of the IEEE, 2017, 105(7): 1389-1407.

[6] 侯连全, 章坚民, 金乃正, 等. 变电站过程层与 SMV 安全传输的网络攻击检测与取证设计[J]. 电力系统自动化, 2016, 40(17): 87-92.
HOU Lianquan, ZHANG Jianmin, JIN Naizheng, et al. Network attack detection and forensics design for safe transmission of substation process layer and SMV[J]. Automation of Electric Power Systems, 2016, 40(17): 87-92.

[7] MACWAN R, DREW C, PANUMPABI P, et al. Collaborative defense against data injection attack in IEC61850 based smart substations[C] // 2016 IEEE Power & Energy Society General Meeting, July 17-21, 2016, Boston, MA, USA.

[8] VALDES A, MACWAN R, BACKES M. Anomaly detection in electrical substation circuits via unsupervised machine learning[C] // 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), July 28-30, 2016, Pittsburgh, PA, USA.

[9] 肖燕. 新一代智能变电站信息流架构设计[J]. 中国电机工程学报, 2016, 36(5): 1245-1251.
XIAO Yan. Information flow architecture design of new generation intelligent substation[J]. Proceedings of the CSEE, 2016, 36(5): 1245-1251.

[10] ZHANG J, LI J, CHEN X, et al. A security scheme for smart substation communications considering real-time performance[J]. Journal of Modern Power Systems and Clean Energy, 2019, 7(4): 948-961.

[11] 孟月波, 刘光辉, 徐胜军. 一种具有边缘保持的多尺度马尔可夫随机场模型图像分割方法[J]. 西安交通大学学报, 2019, 53(3): 56-65.
MENG Yuebo, LIU Guanghui, XU Shengjun. An image segmentation method of multi-scale Markov random field model with edge preserving[J]. Journal of Xi'an Jiaotong University, 2019, 53(3): 56-65.

[12] MUNOZ H, TAHERI A, CHANDA E K. Fracture

energy-based brittleness index development and brittleness quantification by pre-peak strength parameters in rock uniaxial compression[J]. Rock Mechanics & Rock Engineering, 2016, 49(12): 4587-4606.

[13] TASLIGEDIK A S, PAMPANIN S. Rocking cantilever clay brick infill wall panels: a novel low damage infill wall system[J]. Journal of Earthquake Engineering, 2016, 21(7): 1023-1049.

[14] 庞策, 张亚生, 申曲. 精确时间同步协议在空间无线信道下的适应性研究[J]. 计算机测量与控制, 2018, 26(3): 236-240.
PANG Ce, ZHANG Yasheng, SHEN Qu. Research on the adaptability of precise time synchronization protocol in space wireless channel[J]. Computer Measurement and Control, 2018, 26(3): 236-240.

[15] 王电钢, 黄林, 刘捷. 考虑负荷虚假数据注入攻击的电力信息物理系统防御策略[J]. 电力系统保护与控制, 2019, 47(1): 34-40.
WANG Diangang, HUANG Lin, LIU Jie. Defense strategy of power information physical system considering load false data injection attack[J]. Power System Protection and Control, 2019, 47(1): 34-40.

[16] 凌光, 许伟国, 王志亮, 等. 基于 EPON＋的高可靠性固定时延网络在智能变电站应用研究[J]. 电力系统保护与控制, 2016, 44(14): 89-94.
LING Guang, XU Weiguo, WANG Zhiliang, et al. Application of high reliability fixed time delay network based on EPON + in intelligent substation[J]. Power System Protection and Control, 2016, 44(14): 89-94.

[17] 郝唯杰, 杨强, 李炜. 基于 FARIMA 模型的智能变电站通信流量异常分析[J]. 电力系统自动化, 2019, 43(1): 215-226.
HAO Weijie, YANG Qiang, LI Wei. Abnormal analysis of communication flow in intelligent substation based on FARIMA model[J]. Automation of Electric Power Systems, 2019, 43(1): 215-226.

[18] 张纯笑, 徐嘉龙, 张亮, 等. 新型智能变电站通信网络时间同步脆弱性分析[J]. 光通信研究, 2017(3): 16-19.
ZHANG Chunxiao, XU Jialong, ZHANG Liang, et al. Vulnerability analysis of time synchronization in new intelligent substation communication network[J]. Optical Communication Research, 2017(3): 16-19.

[19] 张纯笑. 新一代智能变电站网络时间同步系统脆弱性研究[D]. 北京: 华北电力大学, 2018.
ZHANG Chunxiao. Research on vulnerability of new generation intelligent substation network time synchronization system[D]. Beijing: North China Electric Power University, 2018.

[20] 姜海涛, 王黎明, 周超, 等. 智能变电站网络异常分析方法[J]. 电力信息与通信技术, 2017(2): 58-62.
JIANG Haitao, WANG Liming, ZHOU Chao, et al. Network anomaly analysis method of intelligent substation[J]. Electric Power Information and Communication Technology, 2017(2): 58-62.

[21] 席禹, 邹俊雄, 蔡泽祥, 等. 基于报文识别与流量管控的智能变电站保护控制信息安全防护方法[J]. 电网技术, 2017, 41(2): 624-629.
XI Yu, ZOU Junxiong, CAI Zexiang, et al. Information security protection method of intelligent substation protection and control based on message identification and flow control[J]. Power System Technology, 2017, 41(2): 624-629.

[22] 佟为明, 高吉星, 金显吉, 等. 智能变电站过程层网络报文传输时间计算及抖动抑制方法[J]. 电力自动化设备, 2018, 38(6): 67-74.
TONG Weiming, GAO Jixing, JIN Xianji, et al. Calculation of process layer network message transmission time and jitter suppression method of intelligent substation[J]. Electric Power Automation Equipment, 2018, 38(6): 67-74.

[23] 叶远波, 孙月琴, 黄太贵, 等. 智能变电站继电保护二次回路在线监测与故障诊断技术[J]. 电力系统保护与控制, 2016, 44(20): 134-141.
YE Yuanbo, SUN Yueqin, HUANG Taigui, et al. On line monitoring and fault diagnosis technology for secondary circuit of relay protection in intelligent substation[J]. Power System Protection and Control, 2016, 44(20): 134-141.

[24] CHEN Haoyong, WANG Xiaojuan, LI Zhihao, et al. Distributed sensing and cooperative estimation/detection of ubiquitous power internet of things[J]. Protection and Control of Modern Power Systems, 2019, 4(4): 151-158. DOI: 10.1186/s41601-019-0128-2.

[25] FAN Wen, LIAO Yuan. Wide area measurements based fault detection and location method for transmission lines[J]. Protection and Control of Modern Power Systems, 2019, 4(4): 53-64. DOI: 10.1186/s41601-019- 0121-9.

收稿日期：2019-10-28；　修回日期：2019-12-03

作者简介：

张　颖(1979—)，男，本科，工程师，主要研究领域为电气自动化、继电保护等；E-mail: sepi_rich@yeah.net

沈　曦(1980—)，男，本科，高级工程师，主要研究领域为电气自动化、继电保护等；

黎其浩(1979—)，男，大专，工程师，主要研究领域为电气自动化、继电保护等。

(编辑　葛艳娜)