时间触发以太网与时间敏感网络时钟同步失效对比分析

彭逸飞，涂晓东*，许 都，王颢钢，谢 军，蒋体钢

(电子科技大学信息与通信工程学院 成都 611731)

【摘要】确定性网络技术逐步应用于航电、工业自动化、车载等任务关键系统，如时间触发以太网 (TTE)、时间敏感网络 (TSN) 等，但时间同步技术是这类网络可靠运行的基础，目前缺乏量化分析模型以及不同协议时间同步服务可靠性对比分析。针对该问题，分析了上述两种协议时间同步过程，提炼出导致时间同步失效的因素，提出两种时间同步协议失效概率的评估模型，在此基础上对比分析了失效场景与失效概率，最后使用 OPNET 对两种时间同步协议的失效概率进行仿真，仿真结果与建模结果一致。该时间同步失效概率评估模型可供行业参考。

关 键 词 失效分析； 可靠性； 时间同步服务； 时间敏感网络； 时间触发以太网

中图分类号 TP336 文献标志码 A doi:10.12178/1001-0548.2022223

Comparative Analysis of Clock Synchronization Failure Between Time-Triggered Ethernet and Time-Sensitive Network

PENG Yifei, TU Xiaodong*, XU Du, WANG Haogang, XIE Jun, and JIANG Tigang

(School of Information and Communication Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Deterministic network technology like Time-triggered Ethernet (TTE) and Time-sensitive Networking (TSN) is gradually applied to mission critical systems such as avionics, industrial automation and vehicle mounted systems. Time synchronization technology is the essential precondition for these networks' proper functioning. Nevertheless, there is no analytical model nor comparative analysis for the reliability of time synchronization services in different protocols. Aiming at this problem, we analyze the time synchronization process of the two protocols of above-mentioned networks, and extract the factors that lead to the failure. Then, we propose a theoretical evaluation model of the failure probability for these two protocols. On this basis, the failure scenario and failure probability are compared and analyzed. Finally, we use OPNET simulator to verify the consistency with the theoretical analysis. The time synchronization failure probability evaluation model proposed in this paper can provide reference for relevant personnel.

Key words failure analysis; reliability; synchronization service; time-sensitive networking; time-triggered ethernet

确定性网络 (deterministic networking, DN) 技术是一类在承载多种混合流量的网络中控制并降低特定业务流端到端时延以及抖动的技术。它能给“时间敏感”业务提供确定性业务保证的能力，其基本特征主要包括：时钟同步、零拥塞数据丢失、可靠数据包交付等。时间触发以太网 (time-triggered ethernet, TTE) 和时间敏感网络 (time-sensitive networking, TSN) 是两种代表性的 DN 网络，其关键技术之一是建立可靠的网络时间同步。

SAE AS6802 时间同步协议[1] 定义了时间触发以太网 (TTE)，满足了分布式综合化航电系统[2-3] 的发展需求，并已经逐步在航空电子系统中得到应用。为了进一步满足分布式综合化的需求，保障混合关键网络中高安全的时间触发业务与其他业务隔离，构建支撑飞行控制系统和航电系统的机载统一通信网络，基于 SAE AS6802 协议对系统可靠性影响的分析将变得尤为重要。

文献 [4-5] 已经通过形式化方法对 AS6802 协议收敛性进行验证，文献 [6] 仅讨论了如何利用 TTE 网络构建单一拜占庭失效场景下的应用层协

收稿日期：2022－07－06；修回日期：2023－02－25

作者简介：彭逸飞 (1997－)，男，博士生，主要从事确定性网络、网络可靠性方面的研究.

*通信作者：涂晓东，E-mail：xdtu@uestc.edu.cn

议。文献 [7-8] 利用形式化方法对 TTE 时钟精度进行证明。文献 [9-10] 研究了 TTE 网络故障的仿真模拟方法，文献 [11] 研究了故障注入测试方法，但并未给出失效概率评估方法。虽然前人已经对 TTE 网络有了一定的研究，但并未对协议失效场景进行系统分析，也未给出时间同步失效概率计算方法。

目前 TSN 技术的研究主要活跃在车载网络和工业网络领域。文献 [12] 着重研究了车载时间敏感软件定义网络，将 TSN 与软件定义网络 (software define network, SDN) 结合，研究结果表明，在较低的网络层上，自动控制流的可见性对于在整个网络基础设施中提供隔离和访问控制至关重要。文献 [13-14] 也在探索 TSN 技术与边缘计算网络的结合方式。

TSN 网络采用 IEEE Std802.1AS 协议中规定的算法实现时间同步。文献 [15] 使用 Petri Net 技术对该协议进行了形式化验证，但并未考虑 802.1AS 的失效场景。文献 [16] 分别对无线以及工业场景无故障情况下运行该协议组成的多跳网络时钟精度等性能进行了评估。文献 [17] 探讨了几种在 TSN 网络中时间敏感流的可靠性保障机制。但均未给出可靠性理论评估方法。故目前 802.1AS 时间同步缺乏针对各种失效场景下的系统性分析以及失效概率评估方法。

针对目前两种协议缺乏失效场景系统性分析和对比的问题，本文首先根据协议分析了时间同步过程以及造成时间同步失效的原因，在此基础上对比了两种协议的失效场景。再针对目前两种协议缺乏失效概率理论分析的问题，分别给出了失效概率的计算模型，并用模型进行失效概率对比，用 OPNET 软件进行失效概率模拟。结果表明本文提出的模型计算结果与仿真结果一致。

1　AS6802 同步失效场景与故障概率评估模型

网络失效是指由于组件故障造成的网络的非正常运行。本文进一步将网络时钟同步失效进行定义。

定义 1　定义网络时钟同步失效为网络中未发生故障的设备数量不足以保障协议的正确运行，或者网络形成了多个相互独立的同步集团。

相关参数如表 1 所示。

表 1　关键参数含义说明

参数	含义
t_{global}	全局时钟基线
$\Delta_{\text{CM}i}$	CM设备i相对于全局时钟的偏差
$\Delta_{\text{SM}j}$	SM设备j相对于全局时钟的偏差
$t'_{\text{global,CM}i}$	全局时钟视图下CM设备i的当前时刻
$t'_{\text{global,SM}j}$	全局时钟视图下SM设备j的当前时刻
n	网络中SM设备总个数
$G(v,e)$	网络拓扑邻接矩阵
GM	TSN时钟同步主节点的位置
k	TTE网络中发生故障的SM总个数
k_{leaf}	TSN网络时钟同步树最下层交换机所连叶节点数量
t_{elapse}	每一同步轮次的观测时刻
S_m	同步集团m中的SM设备数量
Q	同步集团检测阈值
$R(t)$	代指SW或Node可靠度函数，假定服从故障率为λ的指数分布。
λ	代指SW或Node的故障率
h	网络分割方法
V_h	剩余正常同步服务集团中SM的个数

1.1　AS6802 同步过程与同步失效因素分析

AS6802 协议规定时间同步过程可分解为冷启动和稳定同步两个主要阶段，每个阶段均通过 PCF 帧 (protocol control frame) 交互实现，交互过程如图 1 所示。

SM(synchronization master) 和 CM(compression master) 为协议定义的两种协议实体。SM 协议实体通常运行在终端节点上，CM 协议实体通常运行在交换机上。通过协议交互模型可知，如果交互过程中 PCF 帧发生了丢失、超时等异常，就存在导致系统无法正常进入同步状态，或者无法正常维持同步的风险。

其同步关键为协议中定义的时钟容错平均算法，即 CM 设备会首先对每个轮次来自 SM 的时间信息进行排序，其次选取位于序号居中的时间信息，取平均后作为本次修正的参考时钟。

根据该算法，结合协议运行流程[8]，假设全局时钟基线为每次同步之前各个设备的本地时钟相对于t_{global}存在偏差，假定各个设备相对于全局时钟基线的偏差为：

$$\Delta_{\text{CM}i} = t_{\text{global}} - t_{\text{local,CM}i} \tag{1}$$

$$\Delta_{\text{SM}j} = t_{\text{global}} - t_{\text{local,SM}j} \tag{2}$$

式中，$t_{\text{local,device}}$代表设备 device 的本地视图。

可以得到校正后的时钟值为：

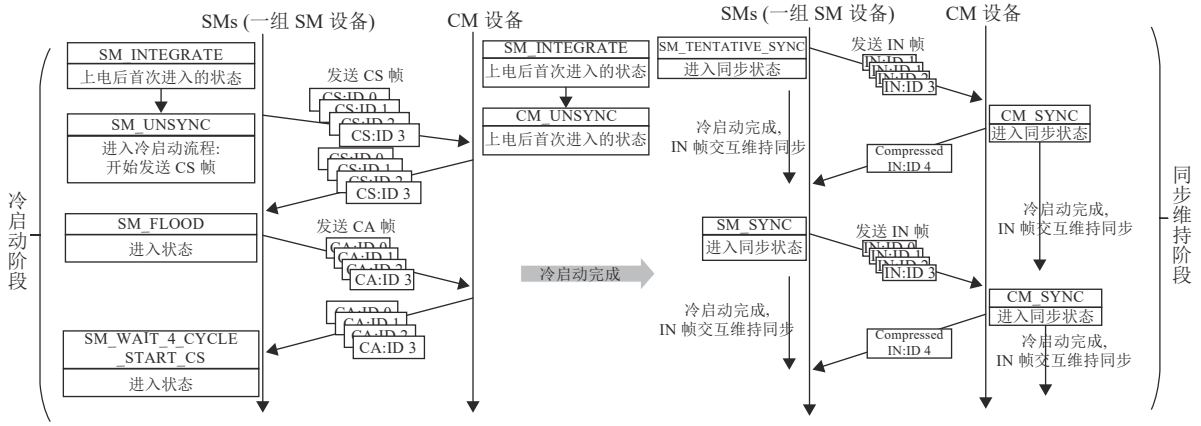


图 1 协议交互模型

$$t'_{\text{global,CM}i} = t_{\text{elapse}} + \frac{\Delta_{\text{SM}(k+1)} + \Delta_{\text{SM}(n-k)}}{2} \tag{3}$$

$$t'_{\text{global,SM}i} = t_{\text{elapse}} + \frac{\Delta_{\text{SM}(k+1)} + \Delta_{\text{SM}(n-k)}}{2} \tag{4}$$

式中，t_{elapse}为 SM 完成一次时间同步算法后的观测点。需要说明的是，式 (3) 和式 (4) 形式上是一致的，这说明 AS6802 时间同步算法组建的网络系统，各个设备的时钟均收敛到第$k+1$与第$n-k$个设备的时钟平均值，这也体现了分布式时间同步算法无主时钟的特点。

结论 1 通过式 (3) 和式 (4) 可得，对于共有n个 SM 设备的系统，在系统中有k个 SM 设备故障，并且不考虑时钟偏移的情况下，不失一般性地假设各个 SM 设备的 PCF 帧的固化时刻按照设备编号递增排序，最终交换机与 SM 设备时钟会保持一致，且时钟同步的最终值仅和落入窗内的第$k+1$和第$n-k$个 SM 设备的时钟有关。

1.2 AS6802 失效保障机制与失效模式转化

AS6802 协议定义了 3 种失效保障机制。

1) 自检测对机制

Self-check pair 算法要求各个设备 (包括交换机和端系统) 需要对发送到链路的数据帧进行完整性检查与一致性检查。

每个设备将会包含两个独立运行的协议服务实体，正常情况下，这两个协议服务实体的动作应该保持一致。当两个协议实体不一致时，会阻止协议数据帧输出。

2) Central guardian 机制配合 leaky bucket 机制

Central guardian 算法要求交换机对输入的数据帧进行时间完整性和数据完整性检查，对于不满足完整性要求的数据帧，交换机会将其丢弃。

Leaky Bucket 算法通常是用来限定流量占用的带宽，配合 Central guardian 实现协议帧合理性检查：在确定性网络中拓扑通常是固定的，所以交换机可以检查是否接收到了异常来源的数据帧，或者某些来源的数据帧数量异常，同时利用 leaky bucket 限定特定流量的带宽。

3) 集团检测机制

集团检测机制用于保证网络不会分裂成多个相互独立的同步集团。如图 2 所示，该拓扑包含 2 台 CM 设备和 4 台 SM 设备，CM1、SM1、SM2 设备的时钟在 1:00±10 min 范围内，CM2、SM3、SM4 设备的时钟在 3:00±10 min 范围内。CM1 检测到 SM1、SM2 的信息落入窗中 (图中 CM1 窗口所示)，由结论 1 可知，CM1 本轮次的参考时间为 (1:00+1:10)/2，即 1:05，而 SM3、SM4 的信息由于没有落入 CM1 窗内，而不被 CM1 使用，对于 CM2 类似。这样就使得网络形成了两个互不相干的时间同步集团。根据定义 1，此时发生时间同步失效。

为了处理这种失效，协议规定了集团检测算法，该算法本质为设备监视落入窗内的时间信息个数，当该信息数量低于集团检测阈值Q时 (换句话来说如果有大部分时间信息均未落入窗内)，设备就会认为自己当前处于小集团中，进而会选择进行重启或者冻结。集团检测的关键在于阈值Q的确定，下面给出确定方法。

结论 2 根据结论 1，在交换机不发生故障，且网络设备均开启失效保障机制的前提下，网络中 SM 设备的数量为$n \geqslant 2k$，同步集团检测的阈值Q至少应为 $n-k$。(其中k为发生故障的设备数量)。

证明：

1) 当$Q < n-k$时，意味着系统第$n-k$个 SM 设备的时钟发生故障，这与结论 1 矛盾。

2) 利用反证法，假定当$Q \geqslant n-k$时，仍同时存

在 m 个稳定同步的子系统，则应有：

$$S_1+\cdots+S_m=n \tag{5}$$

$$S_1>Q,\cdots,S_m>Q \tag{6}$$

则可推得：

$$mQ\leqslant S_1+\cdots+S_m=n \tag{7}$$

由：

$$\frac{n}{m}>Q\geqslant n-k \tag{8}$$

可得：

$$n<\frac{m}{m-1}k \tag{9}$$

式中，$m\in[2,n]$。

所以，当$m=2$时，右边取最大值，故网络中 SM 设备的数量为$n\geqslant 2k$，同步集团检测的阈值Q至少应为$n-k$。

如图 2 所示，SM 总个数为 4 个，此时应设置集团检测阈值为 2。观察 CM1，落入 CM1 窗内的时钟信息数量为 2，2=2 不满足$2>Q$，所以同步集团 1 集团检测成功。同步集团 2 同理。

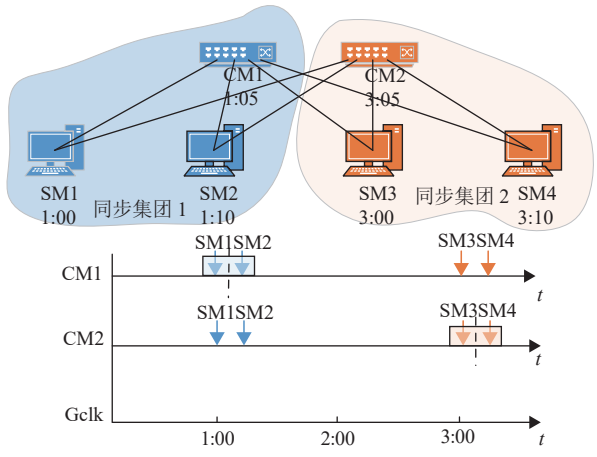


图 2　网络形成多个不相交同步集团

根据定义 1，当网络中有超过k个设备发生故障时，将无法满足 AS6802 协议正常运行的要求，协议将无法维持当前网络的时钟同步服务，最终导致同步失效。

1.3　AS6802 协议失效概率评估模型

利用 1.2 节中所述的故障保障机制，可以将构成 TTE 网络中的任何一个运行 AS6802 协议的设备看作为一个两状态组件 (正常工作状态和失效状态)。TTE 网络最终是否能够正常同步则取决于当前网络中正常工作的设备数量与阈值的关系。事实上，此种 TTE 网络的可以正常同步的概率取决于可用设备的数量。因此，AS6802 协议构建的时间同步网络是典型的 k-out-of-n 系统。k-out-of-n 系统可采用二项分布进行建模[18]，因此给出如下定理。

定理 1　在不考虑 CM 发生故障的情况下，可以给出由 n 个设备组成的系统，由于 k 个 SM 设备发生失效而导致网络同步故障概率为：

$$f_{\text{prob}}(t)=\sum_{i=k}^{n}\binom{n}{i}(1-R(t))^iR(t)^{n-i} \tag{10}$$

式中，$R(t)$ 如表 1 定义为节点可靠性函数。

当网络规模较大时，对网络同步故障概率的求解将变得复杂，这主要是因为导致网络失效的排列组合数量急剧增多。考虑到一般情况下交换设备的故障率相较于端系统会低一个数量级，根据式 (10) 可以得出：

结论 3　对于 TTE 网络，随着网络规模变大，交换设备 (CM) 发生故障将成为导致网络故障的主要因素。(由于篇幅限制，本文将证明过程上传到 Github，网址为 https://github.com/YifeiPengEE/AS6802_IEEE8021AS)

进一步考虑实际情况，设备的失效通常小于10^{-3}，所以本文对于 k-out-of-n 的求解进行如下简化。当$\lambda<10^{-2}$，且运行时间小于 100 h 时，同步失效可近似为 (由于篇幅限制，本文将证明过程上传到 Github，网址为 https://github.com/YifeiPengEE/AS6802_IEEE8021AS)：

$$f_{\text{prob}}(t)=\sum_{i=k}^{n}\binom{n}{i}(1-R(t))^iR(t)^{n-i}\approx \binom{n}{k}(1-R(t))^i \tag{11}$$

评估 TTE 网络时间同步失效概率的算法如下。

Algorithm 1 TTE Synchronization Failure Probability Algorithm

Input:

$R_{\text{Node}}(t),R_{\text{SW}}(t),G(v,e),n$

Output:

$f_{\text{prob}}(t)$

1. comb={}，$f_{\text{prob}}(t)$=0;//初始化
2. $k=\left\lfloor\frac{n}{2}\right\rfloor$;//根据结论 2, 获取集团检测阈值
3. Q=n-k;
4. comb=get_tt_failcomp($G(v,e)$,Q);//根据邻接矩阵和集团检测阈值获取所有由交换机导致网络失效的故障组合
5. foreach i in comb;
6. $f_{\text{prob}}(t)$ += tteget_failprob(i,$R_{\text{Node}}(t)$,$R_{\text{SW}}(t)$);//根

据式 (11), 分别计算各种交换机故障组合情况下的故障概率

7. endforeach;

8. return $f_{\text{prob}}(t)$;

该算法的输入包括节点、交换机的可靠度函数 $R(t)$，网络的邻接矩阵$G(v,e)$以及网络中 SM 的总数量n。算法输出为网络时钟同步失效概率函数 $f_{\text{prob}}(t)$。其中 1～3 行为相关参数的初始化操作。第 4 行调用get_*tt*_failcomp()函数，该函数用于根据结论 2，获取当前网络拓扑下，所有可能造成时钟同步失效的设备失效集合。该算法遍历各种交换机失效场景。下面进行举例说明 (其中深色为失效设备)，如图 3a 所示为正常网络，图 3b 为系统中交换机未发生失效，此时根据结论 2，则系统中至少存在 4 个以上节点发生失效，才会导致系统时间同步失效，则此时失效情场景: {Node3,Node4,Node5,Node6}。图 3c 所示为一台交换机失效场景示例，当 SW1 发生失效后，意味着 Node1 与 Node2 也无法正常与其他节点通信，根据结论 2，与 SW2 连接的节点，至少存在 2 个节点失效才会导致系统时间同步失效，则此时失效情况为: {SW1,Node3,Node4}。图 3d 为在当前拓扑下，当 SW1 与 SW2 均发生失效时，导致系统时间同步失效，则此时失效情况为: {SW1,SW2}。第 4 行 comb 变量就保存了这些会导致系统时间同步失效场景的可能集合。5～7 行为遍历 comb 统计的所有失效场景，tteget_failprob()函数利用式 (11) 求解各种场景下的失效概率进行求和，该求和结果作为系统最终的失效概率。

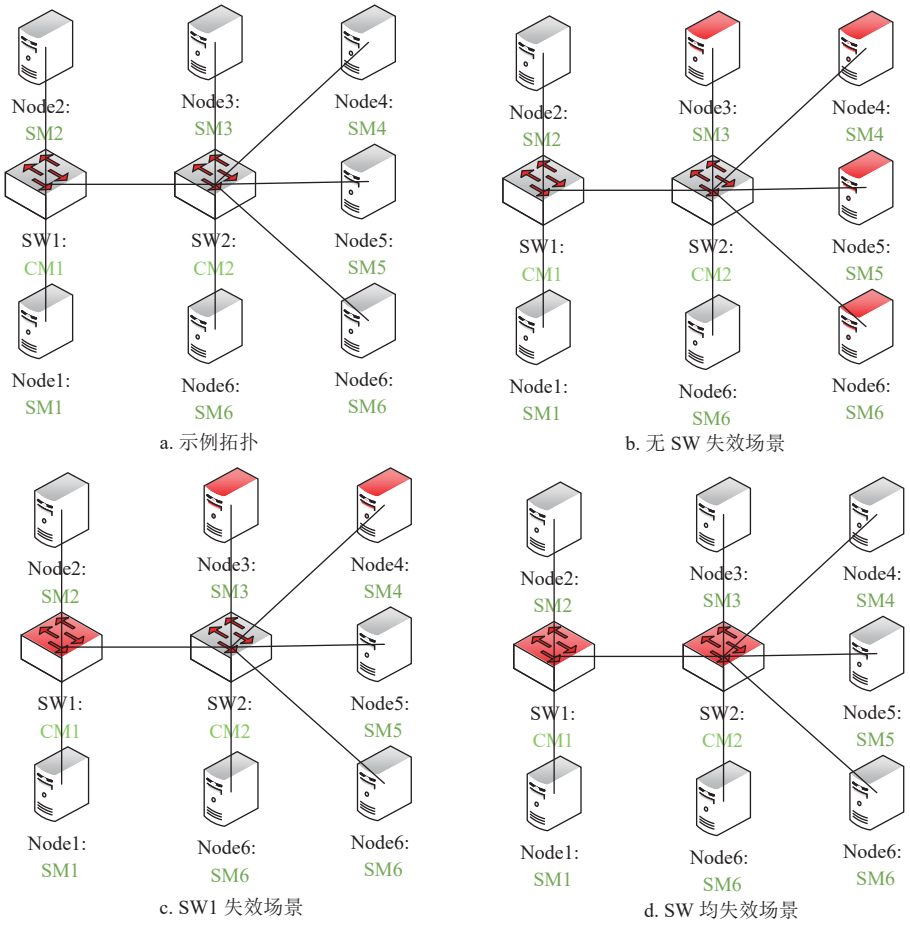


图 3　TTE 网络时钟同步失效组合示例

2　802.1AS 系统模型与可靠性评估模型

2.1　802.1AS 同步过程与同步失效因素分析

802.1AS 协议实现的同步过程同样也可以人为地划分为冷启动阶段和同步维持两个阶段。协议的正常运转通过如下 3 类业务实现。

1) 基于 Announce 报文交互，实现的 BMCA (best master clock algorithm) 算法；

2) 基于 Sync 等报文交换，实现网络时间同步；

3) 基于 Pdelay 等报文交互，实现的频率和延时参数补偿；

图 4 为 802.1AS 协议流程。网络设备初始化

后，首先 Announce 报文获取对端设备的信息 (包括同步优先级、时钟源等)。根据所获取的信息，按照 BMCA 算法规定的比较规则，选出主从设备，生成全局时钟树。此后，端到端之间通过交互 Pdelay 相关报文获取链路时延、端到端频率偏差等相关信息。同时主设备周期性地下发 Sync 报文，用于更新从设备的时钟信息，进而实现周期性的时钟校准。

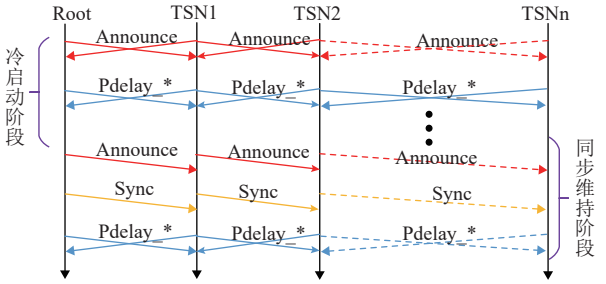


图 4　协议交互模型

通过对协议流程的分析可以看出，如果协议数据帧发生了丢失或者报文发生了延时发送，就会对网络的时间同步造成影响，甚至会导致网络形成多个独立的同步集团。然而 802.1AS 协议仅对超时事件给出了记录机制，并没有说明其他可靠性保障机制。所以可以给出如下失效模式。

2.2　802.1AS 失效处理机制与失效概率评估模型

首先需要说明 802.1AS-2020 介绍了时钟树冗余策略，但是并没有给出多时钟树生成算法以及类似的时钟容错平均算法，所以本文暂不讨论。

802.1AS 对故障的处理机制可以简单理解为：发生超时后，BMCA 进行重新选举，进而形成新的时钟树。如图 5 所示，假设某一时刻 TSN1 发送的 Sync 报文发生了故障，即承载在 Sync 报文中的时间信息发生了突变 (变大)。当 TSN 设备 2 接收到后，就会将自身的时钟修正到 Sync 报文中指定的时刻。此外如果当前设备运行在立即转发模式 (非锁步模式)，则会将该错误的 Sync 报文向下游设备传播。当 TSN 节点 2 依据 Sync 报文中的时间信息修订本地时钟后，触发 Announce 报文接收超时故障，进而导致该节点重新进入 BMCA 算法的选举状态，下游节点类似。并且选举过程需要一定时间后才会稳定。

由此可以得出，虽然 BMCA 算法拥有一定的能力可以使得系统从故障中恢复，但是仍然会引入抖动。并且 BMCA 算法的自恢复能力是有限的，如果失效设备一致无法恢复，极端情况下有可能导致系统分裂成多个同步集团。

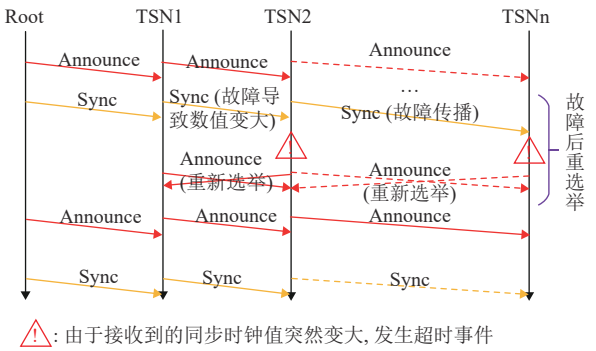


图 5　故障处理机制说明

BMCA 算法本质是按照广度优先遍历的结果，以 GM 节点为根节点，实现逐层同步。所以在不考虑恶意攻击的前提下，802.1AS 协议失效可以定义为至少一台非最下层交换机所连接叶节点设备发生故障的概率。

根据式 (10)，802.1AS 网络同步失效概率为：

$$f_{\text{prob}}(t) = 1 - (P_1 + P_2) \tag{12}$$

式中，

$$P_1 = R(t)^n$$

$$P_2 = (1 - R(t))^{n - k_{leaf}} \sum_{i=1}^{k_{\text{leaf}}} \binom{k_{\text{leaf}}}{i} (1 - R(t))^i R(t)^{k_{\text{leaf}} - i}$$

P_1表示网络所有设备均不发生故障的概率；P_2表示仅边缘设备发生故障的概率。

对 802.1AS 算法进行故障概率分析可以分为两个步骤，依据广度优先遍历算法求解网络时钟同步树，根据式 (12) 计算网络同步失效概率，具体算法如下。

Algorithm 2 TSN Synchronization Failure Probability Algorithm.

Input:

$R_{\text{Node}}(t)$,$R_{\text{SW}}(t)$,G(v,e),GM

Output:

$f_{\text{prob}}(t)$

1. bmca_result={};k_{leaf}=0,$f_{\text{prob}}(t)$=0;//初始化

2. bmca_result=BMCA($G(v,e)$,GM);//根据网络拓扑和 GM 节点的位置，求解时钟同步树

3. k_{leaf}=get_kleaf_cnt(bmca_result);//获取最下层交换机所连叶节点数量

4. $f_{\text{prob}}(t)$=tsnget_failprob($R_{\text{Node}}(t)$,$R_{\text{SW}}(t)$,k_{leaf});//根据式 (12)，计算失效概率

5. return $f_{\text{prob}}(t)$;

该算法的输入包括节点、交换机的可靠度函数$R(t)$，网络的邻接矩阵$G(v,e)$。算法输出为网络时钟同步失效概率函数$f_{\text{prob}}(t)$。其中第 1 行为相关参数的初始化操作。第 2 行根据 802.1AS 标准给出的 BMCA 算法求取当前时钟树，结果保存在bfs_result中。第 3 行 get_kleaf_cnt()函数，依据bfs_result结果，求取当前同步树的最下层叶子节点数量。第 4 行 tsnget_failprob() 函数依据式 (12) 计算系统最终的失效概率。

3 仿真与分析

3.1 失效场景对比分析

对 TTE、TSN 同步失效场景进行对比，如表 2 所示。当 TTE 网络运行 1.2 节所述的失效保障机制后，将大部分失效模式转化为静默失效。由于遗漏失效和崩溃失效对外特性与静默失效类似，即均为缺失部分数据帧，因此在 3.2 节仿真中考虑将 TTE 网络节点的故障模式设置为静默故障，即根据表 1 节点都以$1-R(t)$的概率发生静默失效。

表 2 TTE、TSN 失效场景对比

失效分类		TTE同步失效场景		TSN同步失效场景	
失效模式类别	具体失效名称	具体失效场景	对系统的影响	具体失效场景	对系统的影响
随机失效	胡言乱语失效	故障设备发送大量CS帧或CA帧或IN帧或无效帧	1) Bus guardian和leaky bucket会抑制这种失效模式在网络中传播 2) 当前失效模式转变为静默失效模式	故障设备发送大量Announce帧或Sync帧或Pdelay帧或无效帧	根据故障发生的位置，可能会导致：1)网络分裂成多个同步集团；2)影响边缘节点的同步精度；3)导致系统重新运行选举算法，进而导致同步精度降低
	伪装失效	故障设备在应该发送CS、CA、IN帧的阶段发送其他类型，但是正确的帧；并且这些帧有可能模拟其他正常设备的内容	1) Bus guardian会抑制这种伪装的数据帧 2) self-check pair机制的合理性检查会抑制数据帧不满足实时镜像时域精确间隔的行为，使得当前失效模式转变为静默失效模式	故障设备发送带有错误信息的Announce帧或Sync帧或Pdelay帧	
轻微不合规格失效	SOS Time失效	由于故障设备本地晶振老化，导致CS、CA以及IN帧轻微偏离正确的接收窗口	self-check pair机制的合理性检查会抑制数据帧不满足实时镜像时域精确间隔的行为；使得当前失效模式转变为静默失效模式	由于故障设备本地晶振老化，导致Announce帧或Sync帧或Pdelay帧出现超时现象	偶尔超时会导致同步精度降低
崩溃/遗漏失效	静默失效	设备未发送任何帧，或者未在应该发送CS、CA、IN帧的时刻发送数据帧	仍然存在	设备未发送任何帧，或者未在应该发送Announce帧或Sync帧或Pdelay帧的时刻发送数据帧	根据故障发生的位置，可能会导致：1)网络分裂成多个同步集团；2)影响边缘节点的同步精度；3)导致系统重新运行选举算法，进而导致同步精度降低
	遗漏失效	设备未接收任何帧，或者未在应该接收CS、CA、IN帧的时刻收到数据帧	仍然存在	设备未接收任何帧，或者未在应该接收Announce帧或Sync帧或Pdelay帧的时刻发送数据帧	
	崩溃失效	设备未发送或者接收任何帧	仍然存在	设备未发送或者接收任何帧	
拜占庭失效	不一致失效	设备部分端口未在应该发送CS、CA、IN帧的时刻发送数据帧	1) self-check pair机制的合理性检查会抑制数据帧不满足实时镜像时域精确间隔的行为； 2)使得当前失效模式转变为静默失效模式	1)设备部分端口未在应该发送Announce帧或Sync帧或Pdelay帧的时刻发送数据帧； 2)发送的帧的内容不一致	根据故障发生的位置，可能会导致：1)网络分裂成多个同步集团；2)影响边缘节点的同步精度；3)导致系统重新运行选举算法，进而导致同步精度降低
	不一致遗漏失效	设备部分端口未在应该接收CS、CA、IN帧的时刻接收数据帧	1)集团检测机制保障系统不会分裂为两个同步集团		

对于 TSN 网络，由于 802.1AS 协议并未规定类似的失效保障机制，因此几乎每一种失效模式都有可能导致网络同步失效。因此 3.2 节直接将 TSN 网络节点的故障模式设置为时钟大幅度偏移，即根据表 1 节点的同步时钟都以$1-R(t)$的概率发生大幅度偏移。

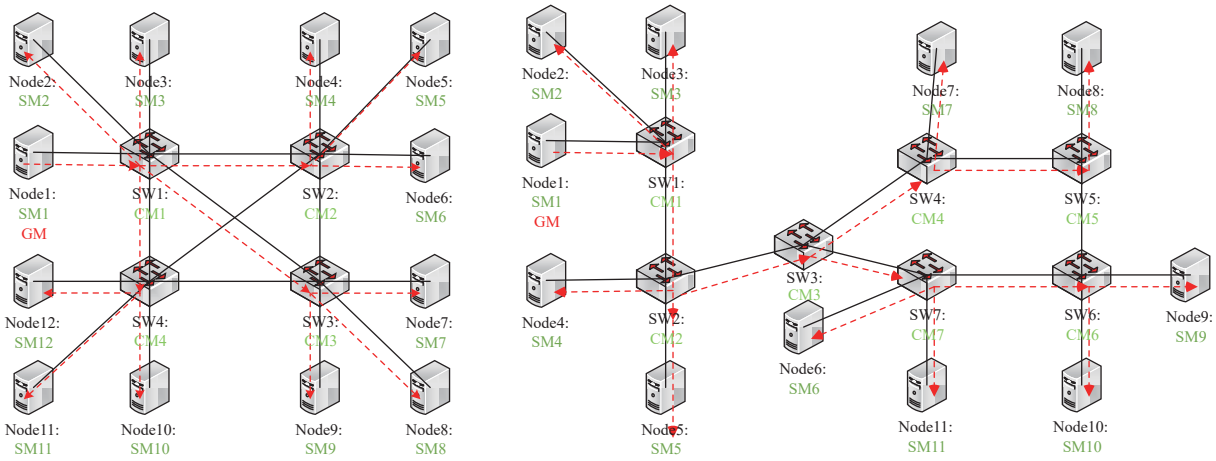
3.2　失效概率对比分析

通过对比理论计算和 OPNET 仿真的方式说明本文的故障概率计算算法的合理性。

图 6a 和图 6b 分别给出了本次采用的两种拓扑仿真[19]。其中实线连线为实际物理链路，SW 代表运行 AS6802-CM 或运行 802.1AS 协议的交换机，Node 代表运行 AS6802-SM 或 802.1AS 协议的端系统。这些端系统通常可以是摄像头、雷达、GPS 等设备。

为了便于理解，当网络采用 AS6802 协议时，仅观察拓扑中标记为 SM/CM 的设备，如图 6a 所示，此时 Node1 运行 AS6802-SM 协议，别名为 SM1。SW1 运行 AS6802-CM 协议，别名为 CM1。当采用 802.1AS 协议时，其中标记为 GM 的设备为主时钟，如图 6b 所示，各个设备均运行 802.1AS 协议，假定 Node1 为当前拓扑下的 802.1AS-GM 设备 (主节点)，虚线箭头给出了 BMCA 算法形成的时钟同步树，其他节点均为运行 802.1AS 协议的普通节点。

表 3 所示为本次对比试验所采用的参数设置，该参数设置与所选择的仿真拓扑无关，需要说明的是，上述R_{dur}持续时间或AS_{TO}超时时间均是指离散时间仿真器中的仿真时间，而非实际设备的运行时间。



a. 仿真拓扑 1　　b. 仿真拓扑 2

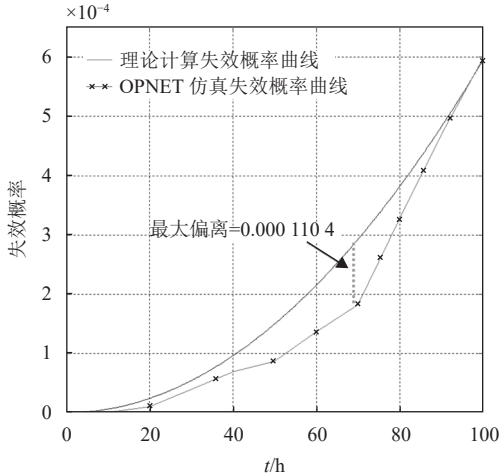
图 6　OPNET 网络仿真拓扑

表 3　仿真参数说明

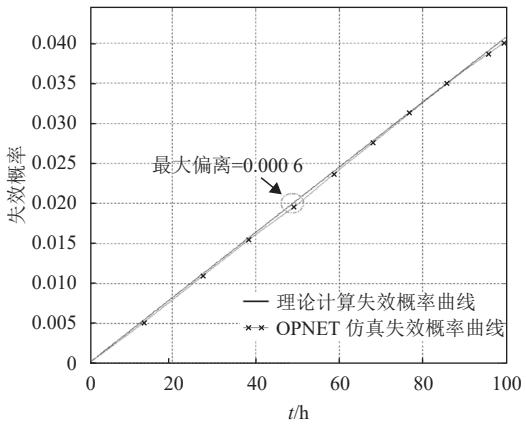
变量名	变量取值	说明
λ_{Node}	10^{-5}	节点故障率
λ_{SW}	10^{-4}	交换机故障率
Sim_{times}	1.5×10^{5}	仿真轮次
R_{dur}/ms	20	每个轮次持续时间
AS_{TO}	$3\times R_{dur}$	802.1AS超时时间
Seed	128	随机种子值

图 7 和图 8 分别展示了两种拓扑下 AS6802、802.1AS 网络按照算法 1 和算法 2 理论计算和使用 OPNET 进行 150 000 次试验后取平均的结果。其中节点相关参数按照表 1 进行设定，纵坐标代表失效概率，横坐标代表所模拟的系统运行时间。

对比理论计算结果曲线和 OPNET 仿真结果曲线，失效概率偏差范围均在一个数量级。理论计算方法所获得曲线与仿真所得失效概率最大偏离不高于同一个数量级 (如图中标注)。说明本文提出的时间同步协议故障概率量化估计模型与 OPNET 仿真实验得出的结果基本一致。理论计算与 OPNET 仿真两种失效概率曲线存在偏差，主要原因是计算二项分布结果时对排列组合的计算进行了放缩与近似 (由于篇幅限制，本文将证明过程上传到 Github，网址为 https://github.com/YifeiPengEE/AS6802_IEEE8021AS)。

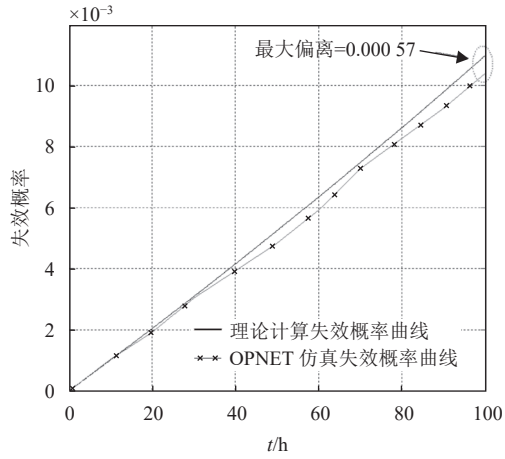


a. 拓扑 1-TTE 失效概率曲线

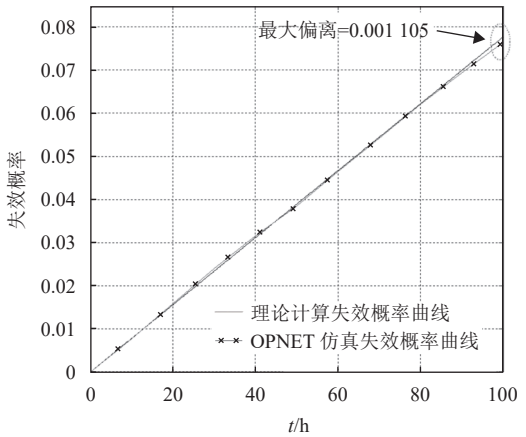


b. 拓扑 1-TSN 失效概率曲线

图 7 拓扑 1 同步失效概率对比



a. 拓扑 2-TTE 失效概率曲线



b. 拓扑 2-TSN 失效概率曲线

图 8 拓扑 2 同步失效概率对比

4 结 束 语

失效模式作为协议的薄弱环节，在设计使用这两种协议组网的过程中需要重点考虑。本文针对两种协议提出的失效概率模型符合 OPNET 失效概率仿真结果，可以为相关人员评估两种协议时间同步服务可靠性提供方法。此外，从本文的分析与仿真可看出，802.1AS 时间同步相对于 AS6802 故障概率较高，未来可以通过改进同步机制，如采用分布式时钟容错算法等策略，提高时钟同步服务的可靠性，进而提高 TSN 网络整体可靠性。此外，当前针对可靠性的量化评估采用的是 k-out-of-n 系统基本可靠度模型，未来计划在评估精度与仿真性能方面，对比其他可靠度模型。

参 考 文 献

[1] Time-Triggred Ethernet. SAE aerospace standard AS6802[S]. USA: STEINER W, 2012.

[2] WANG H C, NIU W S. A review on key technologies of the distributed integrated modular avionics system[J]. Wirel Inf Netw, 2018, 25(3): 358-369.

[3] ZHANG W W, LIU J Q, et al. A survey of optimal hardware and software mapping for distributed integrated modular avionics systems[J]. Applied Sciences, 2020, 10(8): 2675.

[4] STEINER W, DUTERTRE B. The TTE thernet synchronisation protocols and their formal verification[J]. Critical Computer-Based Systems, 2013, 4(3): 280-300.

[5] STEINER W, JOHN R. Model checking a fault tolerant startup algorithm: From Design exploration to exhaustive fault simulation [C]//2004 International Conference on Dependable Systems and Networks. [S.l.]: IEEE, 2004: 189-198.

[6] LOVELESS A, FIDI C, WERNITZNIGG S, et al. A proposed byzantine fault-tolerant voting architecture using time-triggered ethernet[EB/OL]. (2017-01-21). https://ntrs.nasa.gov/citations/20170010131.

[7] TANG X Q, LI Q, LU G S, et al. Safe clock synchronization mechanism for multi-cluster TTE thernet networks[C]//2018 Wireless Communications and Signal Processing. [S.l.]: IEEE, 2018: 1-6.

[8] TANG X Q, LI Q, LU G S, et al. An application-level method of arbitrary synchronization failure detection in TTE thernet networks[J]. Journal of Circuits, Systems, and Computers, 2020, 29(7): 1-19.

[9] PAVKOVIC B, SANDIC M, et al. A genetic simulation strategy: Application to single-fault analysis of TTEthernet synchronization protocol[EB/OL]. (2021-05-01). https://www.sciencedirect.com/science/article/abs/pii/S1383762121001193.

[10] 杨劲赫, 李 峭, 汤雪乾. TTE 高完整性和标准完整性配置下同步机制和容错能力对比分析[J]. 载人航天, 2020, 26(1): 63-68.
YANG J H, LI Q, TANG X Q. Comparative analysis of synchronization mechanism and fault tolerance of TTE network with high integrity and standard integrity configurations[J]. Manned Spaceflight, 2020, 26(1): 63-68.

[11] 陶淑婷, 毛雅欣, 张永波. 时间触发以太网容错机制及其

验证方法[C]//中国航天电子技术研究院科学技术委员会 2020 年学术年会论文集. 北京: 中国航天电子技术研究院, 2020: 700-706
TAO S T, MAO Y X, ZHANG Y B. Time-Triggered ethernet fault-tolerant mechanism and its verification method [C]//Proceedings of the 2020 Academic Annual Meeting of the Science and Technology Committee of the China Academy of Aerospace Electronics Technology. Beijing: China Academy of Aerospace Electronics Technology, 2020: 700-706.

[12] HACKEL T, MEYER P, KORF F, Secure time-sensitive software-defined networking in vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 72(1): 35-51.

[13] WANG Y M, YANG S S, REN X B. IndustEdge: A time-sensitive networking enabled edge-cloud collaborative intelligent platform for smart industry[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2386-2398.

[14] POPA P, ZARRINA B, BARZEGARANA M, et al. The FORA fog computing platform for industrial IoT[EB/OL]. (2021-05-10). https://www2.compute.dtu.dk/~mohba/papers/2.pdf.

[15] TANG S Y, HU X Y, ZHAO L. Modeling and security analysis of ieee 802.1as using hierarchical colored petrinets[C]//2020 IEEE Global Communications Conference Taipei, China: IEEE, 2020: 1-6.

[16] VAL I, SEIJO O, TORREGO R. IEEE 802.1AS clock synchronization performance evaluation of an integrated wired-wireless TSN architecture[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 2986-2999.

[17] KEHRER S, KLEINEBERG O, HEFFERNAN D. A comparison of Fault-Tolerance concepts for IEEE 802.1 time sensitive networks (TSN)[C]//Proceedings of the 2014 IEEE Emerging Technology and Factory Automation. Barcelona: IEEE, 2014: 1-8.

[18] 宋保维. 系统可靠性设计与分析[M]. 西安: 西北工业大学出版社, 2008
SONG B W, System reliability design and analysis[M]. Xi'an: Northwestern Polytechnical University Press, 2008.

[19] 朱海龙, 严园园. TSN 网络中时钟同步可靠性提升方法[J]. 北京邮电大学学报, 2021, 44(2): 20-25.
ZHU H L, YAN Y Y. Measures of reliability improvement of clock synchronization in time sensitive networking[J]. Journal of Beijing University of Posts and Telecommunications, 2021, 44(2): 20-25.

编　辑　税　红