面向工业无线网络的时间同步攻击检测

张思超[1, 2, 3, 4]，梁炜[1, 2, 3]，苑旭东[1, 2, 3]，张吟龙[1, 2, 3]，郑萌[1, 2, 3]

（1. 中国科学院沈阳自动化研究所机器人学国家重点实验室，辽宁 沈阳 110016；
2. 中国科学院网络化控制系统重点实验室，辽宁 沈阳 110016；
3. 中国科学院机器人与智能制造创新研究院，辽宁 沈阳 110169；4. 中国科学院大学，北京 100049）

摘 要：高精度的时间同步是保障工业无线网络（IWN, industrial wireless network）安全、可靠传输的基础。延迟攻击作为一类无法使用密码技术解决的时间同步攻击，严重威胁工业无线网络的安全运行。首先，在深入分析工业无线网络时间同步机制的基础上，构造了 3 种时间同步攻击模型，即单向全生命周期延迟攻击、双向全生命周期延迟攻击和单向非全生命周期延迟攻击，模型在目标节点未被捕获的前提下可实现较隐蔽的延迟攻击。其次，针对现有检测算法难以检测时间特征无明显变化的较隐蔽延迟攻击的问题，提出了一种基于贝叶斯模型的攻击检测算法，算法提取传输速率、传输时延、传输成功率及时间同步周期共 4 类代表性特征。此外，在贝叶斯特征信息矩阵中引入无线信道噪声模型，以保证在噪声干扰存在条件下的攻击检测和分类准确性。实验结果表明，所提算法在有噪声存在的情况下能够有效检测 3 种延迟攻击。

关键词：工业无线网络；时间同步攻击；延迟攻击；攻击检测；贝叶斯模型
中图分类号：TN92
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2023.00334

Time synchronization attack detection for industrial wireless network

ZHANG Sichao[1, 2, 3, 4], LIANG Wei[1, 2, 3], YUAN Xudong[1, 2, 3], ZHANG Yinlong[1, 2, 3], ZHENG Meng[1, 2, 3]

1. State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China
2. Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China
3. Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China
4. University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: High-precision time synchronization is the basis for ensuring the secure and reliable transmission of industrial wireless network (IWN). Delay attacks, as a class of time synchronization attacks which cannot be solved by cryptographic techniques, seriously threaten the secure operation of IWN. Firstly, based on the in-depth analysis on the time synchronization mechanisms of IWN, three-time synchronization attack models were proposed, including the one-way full life cycle delay attack, two-way full life cycle delay attack, and one-way non-full-life cycle delay attack. Stealthier delay attacks could be realized by the attack models under the premise that target nodes were not captured. Secondly, considering the problem that existing detection algorithms are difficult to detect stealthier delay attacks without obvious changes in time features, an attack detection algorithm based on a Bayesian model was proposed that extracts four representative features, including transmission rate, transmission delay, transmission success rate and time synchronization interval. In addition, in order to ensure the accuracy of the attack detection and classification in the presence of noise interference, the noise model of wireless channel was introduced to the Bayesian feature information matrix. Experimental results show that the proposed algorithm can effectively detect three kinds of attacks in the presence of noise.

Key words: industrial wireless network, time synchronization attack, delay attack, attack detection, Bayesian model

收稿日期：2022−11−23；**修回日期：**2023−03−11
通信作者：梁炜，weiliang@sia.cn
基金项目：国家重点研发计划（No.2021YFB3301000）；国家自然科学基金资助项目（No.62022088，No.62273332）
Foundation Items: The National Key Research and Development Program of China (No.2021YFB3301000), The National Natural Science Foundation of China (No.62022088, No.62273332)

0　引言

近年来，随着定制化生产、节能减排等需求在工业生产中越来越迫切，智能制造成为工业界和学术界关注的焦点[1-3]。在智能制造时代，工厂需要更加灵活、智能的生产线来应对用户多种多样的定制化需求及快速变化的市场需求。工业无线技术以其可移动、灵活、低成本等优点，已经成为智能制造的核心使能技术，广泛应用于石油、化工、冶金等流程工业，及汽车、电子、机器人等离散制造业[4-5]。

目前，面向流程工业，国际上拥有 WirelessHART（IEC 62591）、ISA100.11a（IEC 62734）和 WIA-PA（IEC 62601）三大工业无线标准[6-8]。面向离散工业，由我国牵头制定的 WIA-FA（IEC 62948）标准[9]，是面向离散制造业高速控制应用的工业无线国际标准。为了确保传输的高实时性和高可靠性，工业无线网络的数据链路层采用时分多址（TDMA, time division multiple access）避免传输冲突，保障数据在指定时间的收发。由此可见，保证全网时钟的统一是保障工业无线网络正常运行的首要条件，而高精度的时间同步是关键[10-13]。

时间同步攻击（TSA, time synchronization attack）是一种针对网络时间同步机制的攻击，可导致网络各节点之间产生时间偏差，降低系统、服务或设备性能，甚至造成灾难性的后果[14-17]。由于无线介质的开放性，无线网络更容易在时间同步阶段遭受干扰、欺骗、篡改等攻击[18-20]。工业无线网络一旦在时间同步阶段遭受数据篡改、重放攻击、延迟攻击等恶意攻击，就会造成节点与网关时钟不统一，导致网络通信性能下降，甚至网络崩溃。

大多数的时间同步攻击可以通过使用适当的密码技术解决。例如，为每个交换的消息提供身份验证以防止攻击者伪装成其他节点篡改交换消息的内容，为信标消息或其他消息添加序列号以防止重放攻击[21]。然而，延迟攻击是一种无法通过密码技术解决的时间同步攻击。延迟攻击通过延迟、更改发送时间以放大节点与实际时间的偏差干扰同步。目前所有时间同步机制都易受延迟攻击影响[22-24]。

国内外学者针对延迟攻击检测开展了相关研究工作，根据检测基本原理的不同可分为两类：一类是基于参考时钟偏差的延迟攻击检测方法[25-26]，即通过比较网络时钟与外部参考时钟的偏移量来进行检测，但引入外部参考时钟本身就引入了安全风险，一旦外部参考时钟遭受攻击，整个网络将无法准确检测延迟攻击；另一类是基于自身时钟偏差的延迟攻击检测方法[27-30]，即通过比较自身时钟的延迟或者偏移量来进行攻击检测，但这类方法均选取了与时间相关的特征作为判断依据，不适用于时间特征无明显变化的较隐蔽延迟攻击。此外，上述两类方法均没有考虑干扰、噪声对检测模型的影响，模型泛化性较差；并且大多假设攻击模型的前提是节点已被捕获，这种假设条件过强。

针对以上问题，为了有效防御工业无线网络延迟攻击，本文提出了一种基于贝叶斯模型的攻击检测算法，主要贡献包括 3 个方面。

1) 在深入分析工业无线网络时间同步机制的基础上，提出了 3 种时间同步攻击模型，模型在目标节点未被捕获的前提下可实现较隐蔽的延迟攻击。

2) 针对上述攻击模型，提出了一种基于贝叶斯模型的攻击检测算法，模型包括传输速率、传输时延、传输成功率及时间同步周期 4 类特征信息，可有效对攻击进行检测和分类；同时，考虑无线信号噪声干扰对攻击检测的影响，将无线信道噪声刻画成特征信息矩阵引入贝叶斯模型中，提高了检测准确率。

3) 搭建了工业无线网络通信平台，对所提算法进行了算法对比、检测性能评估等实验。实验结果表明本算法在有噪声存在的情况下可有效检测出 3 种攻击，且检测准确率较高。

1　相关工作

1.1　基于参考时钟偏差的延迟攻击检测方法

文献[25]提出了一种引入外部标准时间源（GPS/北斗）的时间同步设备检测铁路网中网络时间协议（NTP, network time protocol）的方法。在时间同步过程中，客户端在与服务器完成时间同步报文交互后不对自身时钟进行调整，而是验证所计算的偏移量，若在该客户端上游未发生攻击时，其计算偏移量应接近于 0，若计算的偏移量超出阈值并超过一定次数便会报警，表明受到了延迟攻击。文献[26]针对电力系统中使用的精准时间协议（PTP, precise time protocol），提出采用

独立于主站时钟的外部参考时钟与从站时钟进行对比，通过计算时钟的偏移量判断从站是否受到了延迟攻击。

1.2　基于自身时钟偏差的延迟攻击检测方法

文献[27]通过比较网络内部所有时钟之间的相对偏移量实现延迟攻击的检测，同时将 PTP 划分成块，以确定延迟攻击发生的位置。然而该方法存在一定缺陷，如果攻击者攻击了全部从站时钟或者大多数从站时钟，检测模型将无法判断是否存在延迟攻击；同时比较网络中所有时钟的相对偏移量将耗费大量计算资源，这对于资源有限的无线通信设备是不适用的。文献[28]提出了一种基于三向握手协议的方法，以软件方式完全排除了非确定性因素，并且可以使节点准确地估计一对节点之间的相对时钟偏移和端到端时延，从而纠正时间同步错误以及精确检测延迟攻击。文献[29]在时钟偏移检测的基础上增加了时间率的检测，采用最小二乘估计计算发送时间、时间率估计值，根据发送时间估计值和实际值偏差、时间率估计值和实际值偏差分别设置阈值检测并排除异常同步信息。文献[30]提出了一种基于混合马尔可夫树的延迟攻击检测模型，模型在计算时延、同步时间间隔、时钟偏移的同时，增加了对时钟偏移概率的估计，即考虑了时间同步误差对时钟偏移的影响，将变化后的概率分布与建模的概率表对比分析出概率的异常分布情况，从而降低误报率。文献[28-30]均选取了与时间相关的特征作为判断依据，如时钟偏移、时延、同步时间间隔等。

2　工业无线网络时间同步机制

工业无线网络多采用基于发送机–接收机模型的时间同步机制，一般支持两种时间同步方式：单向时间同步（被动同步）和双向时间同步（主动同步）[12-13]。单向时间同步流程如图 1 所示，时间源节点周期性发送信标帧/时间同步帧，非时间源节点接收到信标帧/时间同步帧后，根据信标帧/时间同步帧中的时戳值校准本地时间值，以达到全网时间同步的目的。

双向时间同步流程如图 2 所示，非时间源节点收到信标帧/时间同步帧后向时间源节点发送请求帧，随后时间源节点向非时间源节点发送响应帧，非时间源节点根据收到的信标帧/时间同步帧和响应帧计算帧发送时间并进行时间同步。

$$T_{\text{delay}} = [(T_{\text{br}} - T_{\text{asn}}) + (T_{\text{ar}} - T_{\text{pt}})] / 2 \tag{1}$$

$$T_{\text{s}} = T_{\text{asn}} + T_{\text{delay}} \tag{2}$$

其中，T_{delay} 为单帧发送时间，T_{br} 为收到信标帧/时间同步帧的时间值，T_{asn} 为信标帧/时间同步帧中的绝对时间值，T_{ar} 为时间源节点收到请求帧的时间值，T_{pt} 为非时间源节点发送请求帧时的时间值，T_{s} 为非时间源节点校准后的时间值。

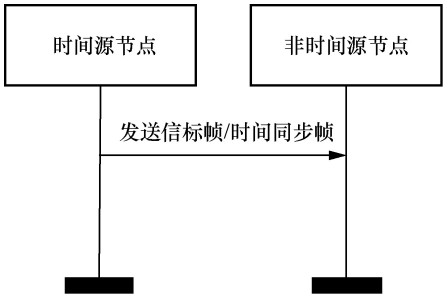

图 1　单向时间同步流程

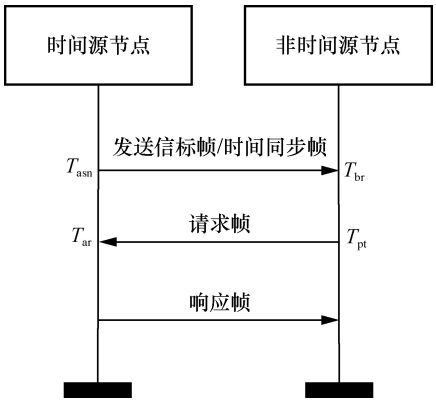

图 2　双向时间同步流程

3　攻击模型

针对工业无线网络常用基于发送机–接收机模型的时间同步，发动延迟攻击通常需要先捕获发送机，即时间源节点；再通过控制时间源节点将 t 时刻发送的信标帧/时间同步帧延迟 e 时间后发送给接收机，即非时间源节点；非时间源节点接收到延迟的信标帧/时间同步帧并校准本地时钟，从而产生时间偏差，捕获前提下的延迟攻击模型如图 3 所示。然而，工业无线网络主要的应用场景大多为工厂、车间等室内封闭空间，时间源节点如网关设备、路由设备、接入设备等，通常部署在工厂或车间特定空间且有专人维护，其捕获难度较大。因此，本文构造了 3 种在时间源节点未被捕获前提下的延迟攻击。

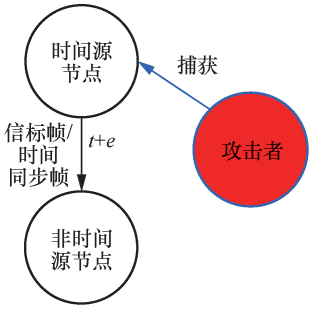

图 3　捕获前提下的延迟攻击模型

一般地，攻击者可以在以下两种情况下发动延迟攻击。

3.1　非时间源节点入网前发动攻击

1) 单向全生命周期延迟攻击

非时间源节点通过信标帧/时间同步帧与时间源节点进行单向时间同步。攻击者在非时间源节点开启的同时对其进行定向干扰，使得非时间源节点无法收到信标帧/时间同步帧；在某一时刻，攻击者获取了 1 个时间源节点的信标帧/时间同步帧，然后停止干扰，在延迟了 e 时间后重放信标帧/时间同步帧；随后，每当时间同步周期到来时重复上述操作，从而导致非时间源节点始终比时间源节点慢 e 时间。单向全生命周期延迟攻击模型如图 4 所示。

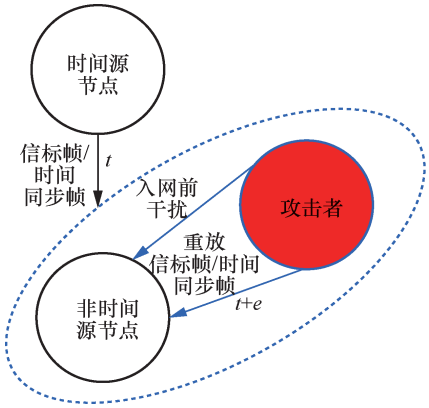

图 4　单向全生命周期延迟攻击模型

2) 双向全生命周期延迟攻击

非时间源节点在入网前通过信标帧/时间同步帧与时间源节点进行单向时间同步，加入网络后的首个超帧与时间源节点进行双向时间同步，之后再执行单向时间同步。攻击者在非时间源节点开启的同时对其进行定向干扰，使得非时间源节点无法收到信标帧/时间同步帧；在某一时刻，攻击者获取了 1 个时间源节点的信标帧/时间同步帧，然后停止干扰，在延迟了 e 时间后重放信标帧/时间同步帧；当非时间源节点加入网络后，在第 1 个超帧与时间源节点进行双向时间同步并获得帧发送时间 T_{delay}，此时非时间源节点将比时间源节点快 f 时间；在下一个时间同步周期到来时，攻击者进行定向干扰并延迟 f 时间重放信标帧/时间同步帧；随后，每当时间同步周期到来时重复上述操作，从而导致非时间源节点始终比时间源节点快 f 时间。双向全生命周期延迟攻击模型如图 5 所示。

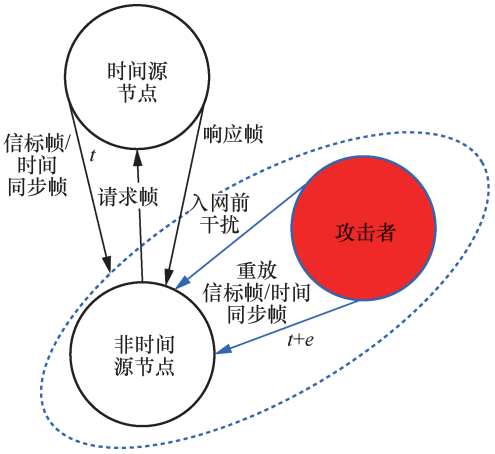

图 5　双向全生命周期延迟攻击模型

3.2　非时间源节点入网后发动攻击

单向非全生命周期延迟攻击：非时间源节点入网后与时间源节点只进行单向时间同步。在某个时间同步周期到来时，攻击者对非时间源节点进行定向干扰并获取时间源节点的信标帧/时间同步帧；攻击者为了使攻击更加隐蔽，在延迟很短一段时间 Δg 后重放信标帧/时间同步帧（Δg 一般小于时间同步精度）；随后，每当时间同步周期到来时，攻击者会比上次增加一段时延 Δg 后重放信标帧/时间同步帧，直至累计时延达到 e 后不再增加，从而导致非时间源节点始终比时间源节点慢 e 时间。单向非全生命周期延迟攻击模型如图 6 所示。

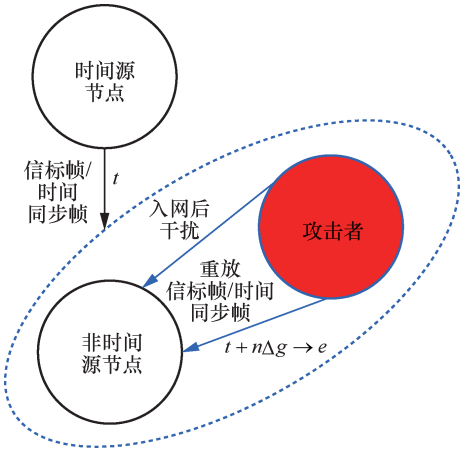

图 6　单向非全生命周期延迟攻击模型

为了提高延迟攻击的隐蔽性，本文制定了相应的攻击规则。工业无线网络数据链路层采用 TDMA 机制，因此，时间源节点和非时间源节点超帧时隙的划分是严格对应的，即时间源节点发送时隙对应非时间源节点接收时隙，时间源节点接收时隙对应非时间源节点发送时隙。工业无线网络通常规定，时间源节点在超帧的第 1 个时隙内发送信标帧/时间同步帧。相应地，非时间源节点在超帧的第 1 个时隙内接收信标帧/时间同步帧进行时间同步。基于上述规定，攻击者想要发动隐蔽的延迟攻击需要遵循两个攻击规则，如图 7 所示。重放信标帧/时间同步帧的时刻必须在非时间源节点接收信标帧/时间同步帧的时隙（超帧的第 1 个时隙）内，如图 7(a)所示；攻击累计的时延必须保证在 1 个时隙内，如图 7(b)所示。

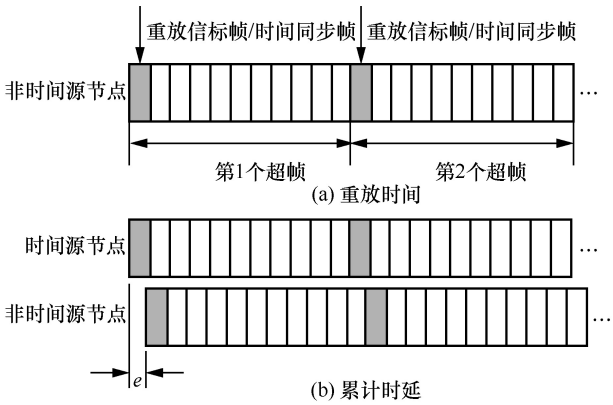

图 7　攻击规则

4　基于贝叶斯模型的攻击检测算法

由于贝叶斯模型具有“由果溯因”的特点，本文面向所述 3 类攻击，提出了基于贝叶斯模型的攻击检测算法，可用于攻击的检测和分类。在特征信息选取方面，延迟攻击会造成网络节点时钟不统一，进而影响网络性能，因此，本文选取了传输速率、传输时延、传输成功率、时间同步周期 4 类特征信息作为观测信息，其中传输时延和时间同步周期用于检测时间特征有明显变化的非全生命周期延迟攻击；传输速率和传输成功率用于检测时间特征无明显变化的较隐蔽延迟攻击。同时，无线环境普遍存在干扰和噪声，会对检测结果产生影响，为此本文将无线信道噪声刻画成特征信息矩阵引入贝叶斯模型，以提高攻击检测准确率。

首先，对条件概率分布作条件独立性假设，即

$$P(X=x\mid Y=c_k)=P(X^{(1)}=x^{(1)},X^{(2)}=x^{(2)},X^{(3)}=x^{(3)},X^{(4)}=x^{(4)}\mid Y=c_k) \tag{3}$$

其中，X 表示 4 类观测信息，$x^{(1)}$表示传输速率，$x^{(2)}$表示传输时延，$x^{(3)}$表示传输成功率，$x^{(4)}$表示时间同步周期，Y 表示 4 种分类信息，c_1 表示单向全生命周期延迟攻击，c_2 表示双向全生命周期延迟攻击，c_3 表示单向非全生命周期延迟攻击，c_4 表示无攻击。

根据贝叶斯定理计算后验概率

$$P(Y=c_k\mid X=x)=\frac{P(X=x\mid Y=c_k)P(Y=c_k)}{\sum_{k=1}^{4}P(X=x\mid Y=c_k)P(Y=c_k)} \tag{4}$$

其中，$P(Y=c_k)$ 表示某种攻击的先验概率分布，$P(X=x\mid Y=c_k)$ 表示某种攻击下传输速率、传输时延、传输成功率、时间同步周期的概率分布，由于对条件概率分布作了条件独立性假设，式(4)可表示为

$$P(Y=c_k\mid X=x)=\frac{P(Y=c_k)\prod_{j=1}^{4}P(X^{(j)}=x^{(j)}\mid Y=c_k)}{\sum_{k=1}^{4}P(Y=c_k)\prod_{j=1}^{4}P(X^{(j)}=x^{(j)}\mid Y=c_k)} \tag{5}$$

然后，采用极大似然估计法对先验概率和条件概率进行估计，先验概率 $P(Y=c_k)$ 的极大似然估计为

$$P(Y=c_k)=\frac{\sum_{i=1}^{N}I(y_i=c_k)}{N},k=1,2,3,4 \tag{6}$$

设第 j 个特征 $x^{(j)}$ 可能取值的集合为 $\{a_{j1},a_{j2},\cdots,a_{js_j}\}$，条件概率 $P(X^{(j)}=a_{jl}\mid Y=c_k)$ 的极大似然估计为

$$P(X^{(j)}=a_{jl}\mid Y=c_k)=\frac{\sum_{i=1}^{N}I(x_i^{(j)}=a_{jl}\mid y_i=c_k)}{\sum_{i=1}^{N}I(y_i=c_k)},\quad j=1,2,3,4;l=1,2,\cdots,s_j;k=1,2,3,4 \tag{7}$$

其中，$x_i^{(j)}$表示第 i 个样本的第 j 个特征；a_{jl}表示第 j 个特征可能取的第 l 个值；I 为指示函数，指定义在某集合上的函数，表示其中有哪些元素属于某一子集。

于是，攻击检测分类可表示为

$$y=f(x)=\arg\max\frac{P(Y=c_k)\prod_{j=1}^{4}P(X^{(j)}=x^{(j)}\mid Y=c_k)}{\sum_{k=1}^{4}P(Y=c_k)\prod_{j=1}^{4}P(X^{(j)}=x^{(j)}\mid Y=c_k)} \tag{8}$$

式(8)中分母对所有 c_k 都是相同的，所以

$$y=\arg\max_{c_k}P(Y=c_k)\prod_{j=1}^{4}P(X^{(j)}=x^{(j)}\mid Y=c_k) \tag{9}$$

然而，无线信道普遍存在干扰和噪声，会对概率估计产生一定影响，因此将噪声协方差矩阵引入条件概率估计，具体做法如下：

$$\boldsymbol{F}_{4\times4}^{k}=\boldsymbol{M}_{4\times4}^{k}\boldsymbol{I}_{4\times4}^{k}\boldsymbol{M}_{4\times4}^{k\ \mathrm{T}}=\begin{bmatrix}\frac{1}{\sigma_1^2}P^2(X^{(1)}=a_{1l}) & 0 & 0 & 0\\ 0 & \frac{1}{\sigma_2^2}P^2(X^{(2)}=a_{2l}) & 0 & 0\\ 0 & 0 & \frac{1}{\sigma_3^2}P^2(X^{(3)}=a_{3l}) & 0\\ 0 & 0 & 0 & \frac{1}{\sigma_4^2}P^2(X^{(4)}=a_{4l})\end{bmatrix} \tag{11}$$

$$\boldsymbol{I}_{4\times4}^{k}=\sum_{4\times4}^{k\ -1} \tag{12}$$

最终，攻击检测分类可表示为

$$y=\arg\max_{c_k}P(Y=c_k)\prod_{j=1}^{4}\boldsymbol{F}_{4\times4}^{k} \tag{13}$$

延迟攻击检测算法见算法 1。

算法 1　延迟攻击检测算法

输入：训练样本集 $T=\{(x_1,c_1),(x_2,c_2),\cdots,(x_N,c_N)\}$，观测信息 x

输出：检测结果 y

计算 $P(Y=c_k),k=1,2,3,4$

计算 $P(X^{(j)}=a_{jl}\mid Y=c_k),j=1,2,3,4;l=1,2,\cdots,\ s_j;$ $k=1,2,3,4$

计算 $\boldsymbol{F}_{4\times4}^{k}=\boldsymbol{M}_{4\times4}^{k}\boldsymbol{I}_{4\times4}^{k}\boldsymbol{M}_{4\times4}^{k\ \mathrm{T}}$

计算 $y=\arg\max_{c_k}P(Y=c_k)\prod_{j=1}^{4}\boldsymbol{F}_{4\times4}^{k}$，得到检测结果

5　实验及分析

为验证所提算法的有效性，本文搭建了 WIA-FA 工业无线网络通信平台，如图 8 所示。平台由 1 个网关设备、1 个接入设备、1 个现场设备、1 个攻击设备和 1 个通用软件无线电外设（USRP, universal software radio peripheral）组成，各设备功能如下。

- 网关设备：用于 WIA-FA 网络与外部网络（以太网）的互联及与接入设备的通信，同时作为全网的时钟源，实现网络时间同步。
- 接入设备：通过有线网络与网关设备连接，通过无线网络与现场设备通信，用于网关设备与现场设备交互数据的转发。
- 现场设备：通过有线网络与摄像机连接，用于视频数据的采集与无线传输，作为非时间源节点与网关设备进行时间同步。
- 攻击设备：内置定向天线，用于对现场设备进行定向干扰及发动延迟攻击。
- USRP：用于生成高斯白噪声，模拟无线信道的干扰和噪声。

将 $P(X^{(j)}=a_{jl}\mid Y=c_k)$ 转换成 4×4 矩阵 $\boldsymbol{M}_{4\times4}^{k}$

$$\boldsymbol{M}_{4\times4}^{k}=\begin{bmatrix}P(X^{(1)}=a_{1l}) & 0 & 0 & 0\\ 0 & P(X^{(2)}=a_{2l}) & 0 & 0\\ 0 & 0 & P(X^{(3)}=a_{3l}) & 0\\ 0 & 0 & 0 & P(X^{(4)}=a_{4l})\end{bmatrix} \tag{10}$$

设 $\sum_{4\times4}^{k}$ 为第 k 个分类下观测信息的噪声协方差矩阵，$\boldsymbol{I}_{4\times4}^{k}$ 为 $\sum_{4\times4}^{k}$ 对应的信息矩阵。将信息矩阵 $\boldsymbol{I}_{4\times4}^{k}$ 引入 $\boldsymbol{M}_{4\times4}^{k}$，得到 $\boldsymbol{F}_{4\times4}^{k}$ 为

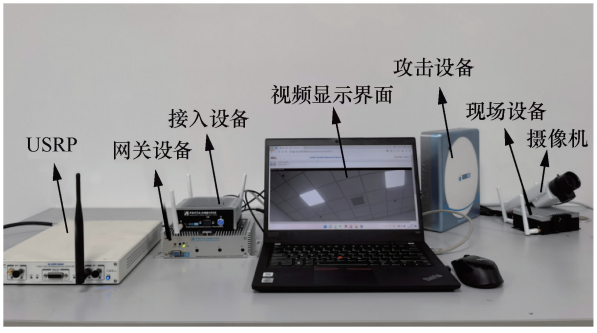

图 8　WIA-FA 工业无线网络通信平台

WIA-FA 工业无线网络配置参数见表 1。

表 1 WIA-FA 工业无线网络配置参数

配置参数	参数值
通信协议	WIA-FA
通信频率/GHz	2.4
信道带宽/MHz	20
通信功率/dBm	14～15
超帧长度/（个时隙）	256
时隙大小/ms	10
时间同步周期/（个超帧）	2
高斯白噪声/dBm	0

运行 WIA-FA 工业无线网络通信平台，分别对现场设备进行 3 组延迟攻击实验，并在现场设备端统计传输速率、传输时延、传输成功率、时间同步周期、时钟偏移、时钟偏移概率信息，得到数据集，实验说明见表 2。

5.1 算法对比分析

分别采用文献[28-30]提出的检测算法对测试集（表 2）中包含的单向全生命周期延迟攻击、双向全生命周期延迟攻击、单向非全生命周期延迟攻击进行检测，将检测结果与所提算法进行对比，检测结果对比见表 3。

可以看出，文献[28-30]提出的算法对于时间特征无明显变化的单向全生命周期延迟攻击和双向全生命周期延迟攻击无法检测，本文所提算法表现出更完整的检测能力，能够有效检测出上述 3 种攻击。

5.2 检测性能评估

本文针对无线信道干扰、噪声引起的检测准确率低的问题，在原有检测模型基础上引入了噪声协方差矩阵。本实验分别对未引入噪声协方差的检测模型及引入噪声协方差的检测模型进行了检测性能评估。

攻击检测常用的评价指标包括准确率、精确率和召回率。

准确率定义为

$$A=\frac{\mathrm{TP+TN}}{\mathrm{TP+FN+FP+TN}} \tag{14}$$

精确率定义为

$$P=\frac{\mathrm{TP}}{\mathrm{TP+FP}} \tag{15}$$

召回率定义为

$$R=\frac{\mathrm{TP}}{\mathrm{TP+FN}} \tag{16}$$

其中，TP 表示将攻击预测为攻击数，FN 表示将攻击预测为非攻击数，FP 表示将非攻击预测为攻击数，TN 表示将非攻击预测为非攻击数。检测性能评估结果见表 4。

可以看出，检测模型对于 3 种攻击的检测效果较好，而引入噪声协方差的检测模型在准确率、精确率、召回率方面均优于未引入噪声协方差的检测模型。双向全生命周期延迟攻击的检测性能全面优于单向全生命周期延迟攻击，这是由于前者导致传输速率、传输时延、传输成功率的变化大于后者导致的变化。单向非全生命周期延迟攻击的检测性能

表 2 实验说明

攻击名称	流程	训练集	测试集
单向全生命周期延迟攻击	进行 2 000 次时间同步，时延为 2 ms	200 次有攻击，800 次无攻击	200 次有攻击，800 次无攻击
双向全生命周期延迟攻击	进行 2 000 次时间同步，时延为 2 ms	200 次有攻击，800 次无攻击	200 次有攻击，800 次无攻击
单向非全生命周期延迟攻击	进行 2 000 次时间同步，累计时延为 2 ms	200 次有攻击，800 次无攻击	200 次有攻击，800 次无攻击

表 3 检测结果对比

检测算法	单向全生命周期延迟攻击	双向全生命周期延迟攻击	单向非全生命周期延迟攻击
文献[28]算法	检测失败	检测失败	检测成功
文献[29]算法	检测失败	检测失败	检测成功
文献[30]算法	检测失败	检测失败	检测成功
所提算法	检测成功	检测成功	检测成功

表 4　　**检测性能评估结果**

检测性能	检测模型	单向全生命周期延迟攻击	双向全生命周期延迟攻击	单向非全生命周期延迟攻击
准确率	未引入噪声协方差的检测模型	94.5%	95.3%	96.2%
	引入噪声协方差的检测模型	96.7%	97.8%	98.6%
精确率	未引入噪声协方差的检测模型	83.7%	85.9%	88.6%
	引入噪声协方差的检测模型	89.6%	92.4%	95.1%
召回率	未引入噪声协方差的检测模型	90.0%	91.5%	93.0%
	引入噪声协方差的检测模型	94.5%	97.0%	98.0%

优于单向全生命周期延迟攻击和双向全生命周期延迟攻击，这是由于单向非全生命周期延迟攻击不仅使得传输速率、传输时延、传输成功率发生变化，还导致时间同步周期发生改变。

5.3　攻击时延对检测性能的影响

在单向全生命周期延迟攻击和双向全生命周期延迟攻击中，攻击时延越小，现场设备与网关设备的时间偏差就越小，因而对传输速率、传输时延、传输成功率的影响就越小。本实验希望通过描述攻击时延与检测性能的关系，计算检测模型能够识别的最小攻击时延。

通过设置攻击设备的攻击时延，即攻击造成的时延占一个时隙的百分比，对现场设备分别进行攻击时延为 5%～50%的单向全生命周期延迟攻击和双向全生命周期延迟攻击，每种攻击时延下进行 1 000 次时间同步（其中 200 次有攻击，800 次无攻击），不同攻击时延下的检测性能如图 9 所示。

由图 9(a)可知，不同攻击时延对检测准确率的影响较小，这是由于攻击时延的大小对 TN 的影响较小。由图 9(b)可知，不同攻击时延对检测精确率有一定程度的影响，但不能完全反映攻击时延与检测性能的关系，因为攻击时延的大小对 FP 的影响较小。由图 9(c)可知，不同攻击时延对检测召回率的影响较大，即反映检测模型对攻击的识别能力影响较大。单向全生命周期延迟攻击与双向全生命周期延迟攻击的攻击时延超过 10%后，检测召回率均达到了 90%以上，说明检测模型在攻击时延为一个时隙的 10%以上时达到了较好的检测性能。

由图 9 的检测结果可以看出，检测模型对于双向全生命周期延迟攻击具有更好的识别能力，再次证明了双向全生命周期延迟攻击对传输速率、传输时延、传输成功率的影响大于单向全生命周期延迟攻击的影响。

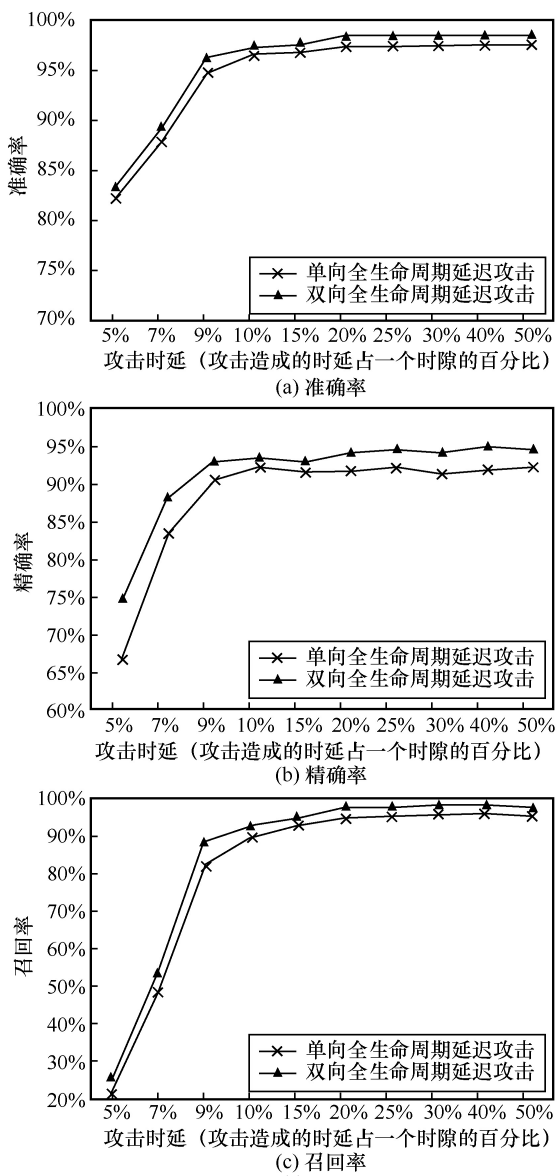

图 9　不同攻击时延下的检测性能

6　结束语

本文针对工业无线网络时间同步机制进行了全面的研究及分析，在目标节点未被捕获的前提下

设计了 3 种较隐蔽的时间同步攻击。在此基础上，针对 3 种攻击模型提出了一种基于贝叶斯模型的攻击检测算法，同时考虑无线信道噪声因素建立贝叶斯特征信息矩阵，通过求解最大后验概率实现了攻击的检测和分类。实验结果表明，所提算法相比现有算法具有更完整的检测能力，能够检测出时间特征无明显变化的较隐蔽延迟攻击，同时在噪声存在的情况下展现了较好的检测性能。在今后的研究工作中，将继续研究其他因素对攻击检测的影响，如网络规模的扩大所产生的影响，以不断提升算法检测能力。

参考文献：

[1] LIANG W, ZHENG M, ZHANG J L, et al. WIA-FA and its applications to digital factory: a wireless network solution for factory automation[J]. Proceedings of the IEEE, 2019, 107(6): 1053-1073.

[2] WOLLSCHLAEGER M, SAUTER T, JASPERNEITE J. The future of industrial communication: automation networks in the era of the internet of things and industry 4.0[J]. IEEE Industrial Electronics Magazine, 2017, 11(1): 17-27.

[3] SAUTER T, SOUCEK S, KASTNER W, et al. The evolution of factory and building automation[J]. IEEE Industrial Electronics Magazine, 2011, 5(3): 35-48.

[4] SHI H G, ZHENG M, LIANG W, et al. Transmission scheduling with order constraints in WIA-FA-based AGV systems[J]. IEEE Internet of Things Journal, 2021, 8(1): 381-392.

[5] LIANG W, ZHANG J L, SHI H G, et al. An experimental evaluation of WIA-FA and IEEE 802.11 networks for discrete manufacturing[J]. IEEE Transactions on Industrial Informatics, 2021, 17(9): 6260-6271.

[6] WANG Q, JIANG J. Comparative examination on architecture and protocol of industrial wireless sensor network standards[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2197-2219.

[7] PETERSEN S, CARLSEN S. WirelessHART versus ISA100.11a: the format war hits the factory floor[J]. IEEE Industrial Electronics Magazine, 2011, 5(4): 23-34.

[8] ZHENG M, LIANG W, YU H B, et al. Performance analysis of the industrial wireless networks standard: WIA-PA[J]. Mobile Networks and Applications, 2017, 22(1): 139-150.

[9] SHI H G, ZHENG M, LIANG W, et al. AODR: an automatic on-demand retransmission scheme for WIA-FA networks[J]. IEEE Transactions on Vehicular Technology, 2021, 70(6): 6094-6107.

[10] 吴宝明, 李声飞. 基于最优线性拟合的 WSN 时间同步算法研究[J]. 传感技术学报, 2010, 23(12): 1787-1791.
WU B M, LI S F. Study on optimal linear fit time synchronization algorithm for wireless sensor network[J]. Chinese Journal of Sensors and Actuators, 2010, 23(12): 1787-1791.

[11] 周贤伟, 韦炜, 覃伯平. 无线传感器网络的时间同步算法研究[J]. 传感技术学报, 2006, 19(1): 20-25, 29.
ZHOU X W, WEI W, QIN B P. Research on time synchronization in wireless sensor network[J]. Chinese Journal of Sensors and Actuators, 2006, 19(1): 20-25, 29.

[12] 汪付强, 曾鹏, 于海斌. 一种低开销的双向时间同步算法[J]. 仪器仪表学报, 2011, 32(6): 1357-1363.
WANG F Q, ZENG P, YU H B. Low overhead two-way time synchronization algorithm[J]. Chinese Journal of Scientific Instrument, 2011, 32(6): 1357-1363.

[13] 杨雨沱, 梁炜, 张晓玲, 等. 面向工厂自动化无线网络的时间同步方法[J]. 计算机研究与发展, 2014, 51(3): 511-518.
YANG Y T, LIANG W, ZHANG X L, et al. Time synchronization method of wireless network for factory automation[J]. Journal of Computer Research and Development, 2014, 51(3): 511-518.

[14] 程利娟, 王福豹, 段渭军. 无线传感器网络时间同步算法的安全性研究[J]. 计算机应用研究, 2007, 24(11): 6-8.
CHENG L J, WANG F B, DUAN W J. Research on security of time synchronization in wireless sensor networks[J]. Application Research of Computers, 2007, 24(11): 6-8.

[15] GANERIWAL S, PÖPPER C, ČAPKUN S, et al. Secure time synchronization in sensor networks[J]. ACM Transactions on Information and System Security, 2008, 11(4): 1-35.

[16] YANG W, WANG Q, QI Y, et al. Time synchronization attacks in IEEE802.15.4e networks[C]//Proceedings of 2014 International Conference on Identification, Information and Knowledge in the Internet of Things. Piscataway: IEEE Press, 2015: 166-169.

[17] 杨伟, 王沁, 万亚东, 等. IEEE802.15.4e 标准的安全多跳时间同步协议设计[J]. 计算机科学, 2017, 44(3): 175-181, 194.
YANG W, WANG Q, WAN Y D, et al. Design of secure multi-hop time synchronization protocol for IEEE802.15.4e[J]. Computer Science, 2017, 44(3): 175-181, 194.

[18] CHHETRI S R, RASHID N, FAEZI S, et al. Security trends and advances in manufacturing systems in the era of industry 4.0[C]//Proceedings of 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). Piscataway: IEEE Press, 2017: 1039-1046.

[19] LIANG L L, LIU Y Z, YAO Y G, et al. Security challenges and risk evaluation framework for industrial wireless sensor networks[C]//Proceedings of 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT). Piscataway: IEEE Press, 2017: 904-907.

[20] PAN F, PANG Z B, LUVISOTTO M, et al. Physical-layer security for industrial wireless control systems: basics and future directions[J]. IEEE Industrial Electronics Magazine, 2018, 12(4): 18-27.

[21] MARTI S, GIULI T J, LAI K, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]//Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. New York: ACM Press, 2000: 255-265.

[22] 尹香兰, 齐望东. LiteST: 一种无线传感器网络轻量级安全时间同

步协议[J]. 通信学报, 2009, 30(4): 74-85.
YIN X L, QI W D. LiteST: a lightweight secure time synchronization protocol for wireless sensor networks[J]. Journal on Communications, 2009, 30(4): 74-85.

[23] KIM K T. SAEP: secure, accurate and energy-efficient time synchronization protocol in WSNs[J]. IEICE Transactions on Communications, 2011, E94-B(6): 1587-1597.

[24] 秦绍华, 陈冬岩. 具有容错性的无线传感器网络时间同步协议[J]. 软件学报, 2012, 23(1): 126-133.
QIN S H, CHEN D Y. Fault-tolerant time synchronization protocol for wireless sensor networks[J]. Journal of Software, 2012, 23(1): 126-133.

[25] 赵庭达, 武晓春. 基于 TCPN 的铁路时间同步网延迟攻击应对策略研究[J]. 铁道标准设计, 2022, 66(8): 168-174.
ZHAO T D, WU X C. Research on countermeasures against delay attack of railway time synchronization network based on TCPN[J]. Railway Standard Design, 2022, 66(8): 168-174.

[26] MOUSSA B, KASSOUF M, HADJIDJ R, et al. An extension to the precision time protocol (PTP) to enable the detection of cyber attacks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(1): 18-27.

[27] MOHSEN M, AMIR H J. A new delay attack detection algorithm for PTP network in power substation[J]. International Journal of Electrical Power & Energy Systems, 2021, 133: 107226.

[28] KIM E J, JEONGSIK I N, YOUM S, et al. Delay attack-resilient clock synchronization for wireless sensor networks[J]. IEICE Transactions on Information and Systems, 2012, E95-D(1): 188-191.

[29] 孙子文, 吴梦芸, 白勇. 抗延迟攻击的 WSN 时间同步方法[J]. 传感技术学报, 2014, 27(7): 982-987.
SUN Z W, WU M Y, BAI Y. Delay attack- resistant time synchronization for WSN[J]. Chinese Journal of Sensors and Actuators, 2014, 27(7): 982-987.

[30] 张颖, 沈曦, 黎其浩, 等. 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[J]. 电力系统保护与控制, 2020, 48(3): 113-121.
ZHANG Y, SHEN X, LI Q H, et al. Research on protocol delay attack detection and mitigation model of smart substation based on Markov logic tree and system brittleness analysis[J]. Power System Protection and Control, 2020, 48(3): 113-121.

[作者简介]

张思超（1988– ），男，中国科学院沈阳自动化研究所副研究员，主要研究方向为工业无线网络、无线网络安全等。

梁炜（1974– ），女，博士，中国科学院沈阳自动化研究所研究员，主要研究方向为工业无线网络、网络信息安全等。

苑旭东（1980– ），男，博士，中国科学院沈阳自动化研究所副研究员，主要研究方向为工业 TSN、工业无线网络。

张吟龙（1988– ），男，博士，中国科学院沈阳自动化研究所副研究员，主要研究方向为工业信息处理、多源信息融合等。

郑萌（1983– ），男，博士，中国科学院沈阳自动化研究所研究员，主要研究方向为工业物联网、网络化控制系统等。