Journal of System Simulation

Volume 32 | Issue 5 Article 14

5-15-2020

A Route Recovery Mechanism Using Hybrid Anti-interference Method

Ziwen Sun
School of Internet of Things, Jiangnan University, Wuxi 214122, China;

Yanqi Zhang
School of Internet of Things, Jiangnan University, Wuxi 214122, China;

Yimin Xu
School of Internet of Things, Jiangnan University, Wuxi 214122, China;

A Route Recovery Mechanism Using Hybrid Anti-interference Method

Abstract

Abstract: Aiming at the jamming attacks in the industrial wireless sensor networks, a route recovery mechanism based on the WirelessHART graph routing is proposed. *The jamming attack detection method is used to obtain the node and area being attacked by the jamming attack*, the uncoordinated frequency hopping spread spectrum is used to generate the frequency hopping sequence of the node of being attacked by the jamming attack and that of the surrounding nodes, so that the traditional frequency hopping spread spectrum is performed on the nodes. Detects again*, and combines the routing cost and the WirelessHART graph routing algorithm to restore the node to the network*. The simulation results show that the route recovery mechanism can help the nodes to eliminate the influence of the interference attacks and successfully join the network under the condition of the ensuring throughput.

Keywords

industrial wireless sensor network, routing recovery mechanism, WirelessHART graph routing, jamming attack detection, uncoordinated frequency hopping spread spectrum

Recommended Citation

Sun Ziwen, Zhang Yanqi, Xu Yimin. A Route Recovery Mechanism Using Hybrid Anti-interference Method[J]. Journal of System Simulation, 2020, 32(5): 874-884.

第 32 卷第 5 期 系统仿真学报© Vol. 32 No. 5
2020 年 5 月 Journal of System Simulation May, 2020

一种采用混合抗干扰方法的路由恢复机制

孙子文*，张炎棋，徐宜敏
(江南大学物联网工程学院，江苏 无锡 214122)

摘要：针对工业无线传感器网络中的干扰攻击问题，得出一种基于 WirelessHART 图路由的被干扰攻击节点路由恢复机制。*通过干扰攻击检测方法获取被干扰攻击节点与干扰攻击区域*，利用非协调跳频扩频技术生成被干扰攻击节点与周围节点的跳频序列，从而进行传统跳频扩频，对被干扰攻击节点进行再检测，*结合路由代价与 WirelessHART 图路由算法将被干扰攻击节点恢复到网络中*。仿真结果表明路由恢复机制能够帮助被干扰攻击节点消除干扰攻击影响，并在保证吞吐量的情况下成功加入到网络中。

关键词：工业无线传感器网络；路由恢复机制；WirelessHART 图路由；干扰攻击检测；非协调跳频扩频

中图分类号：TP393 文献标识码：A 文章编号：1004-731X (2020) 05-0874-11

DOI: 10.16182/j.issn1004731x.joss.18-0638

A Route Recovery Mechanism Using Hybrid Anti-interference Method

*Sun Ziwen**, *Zhang Yanqi*, *Xu Yimin*

(School of Internet of Things, Jiangnan University, Wuxi 214122, China)

Abstract: Aiming at the jamming attacks in the industrial wireless sensor networks, a route recovery mechanism based on the WirelessHART graph routing is proposed. *The jamming attack detection method is used to obtain the node and area being attacked by the jamming attack*, the uncoordinated frequency hopping spread spectrum is used to generate the frequency hopping sequence of the node of being attacked by the jamming attack and that of the surrounding nodes, so that the traditional frequency hopping spread spectrum is performed on the nodes. Detects again*, and combines the routing cost and the WirelessHART graph routing algorithm to restore the node to the network*. The simulation results show that the route recovery mechanism can help the nodes to eliminate the influence of the interference attacks and successfully join the network under the condition of the ensuring throughput.

Keywords: industrial wireless sensor network; routing recovery mechanism; WirelessHART graph routing; jamming attack detection; uncoordinated frequency hopping spread spectrum

引言

工业无线传感器网络(Industrial Wireless Sensor Networks, IWSN)[1]是无线传感器网络[2]的一个新兴应用，常用于观测与控制各类工业任务。

相比于普通无线传感器网络，IWSN 所处的工作环境更为苛刻，时常面临安全性，可靠性及实时性的挑战。另外工业无线传感器网络所用的 WirelessHART 标准是开放式标注，采用多路径图路由机制，打破了普通 WSN 标准的使用环境限制，

收稿日期：2018-09-21 修回日期：2018-12-22;
基金项目：国家自然科学基金(61373126)，中央高校基本科研业务费专项资金(JUSRP51510)；
作者简介：孙子文(1968-)，女，四川，博士，教授，研究方向为模式识别、人工智能、无线传感网络理论与技术和信息安全。

大大提高 IWSN 的实用性[3]，但由于 IWSN 的无线通信特性，干扰攻击威胁成为了影响其安全性及可靠性的主要因素之一[4]。

针对 IWSN 安全的研究主要是围绕攻击检测方法展开。通过采用干扰攻击检测算法检测网络中是否存在干扰攻击，在对处于被攻击状态下的节点进行识别后，会对该节点进行屏蔽或丢弃[5]。恶意干扰攻击虽未直接破坏网络，但使得网络屏蔽或丢弃节点，浪费了网络中的节点资源，降低了网络寿命。因此，仅仅依靠防御与检测手段难以彻底消除恶意干扰攻击的影响，亟需研究能够将被干扰攻击节点恢复到网络中的机制，添加恢复手段来延长网络的生命周期。

关于被干扰攻击节点恢复问题的研究较少，但已有相关的研究工作在检测到干扰攻击后通过采取其它操作来抵抗干扰攻击。如文献[6]研究了一种基于 LEDIR 的节点恢复技术，在距离移动、交换消息总数以及节点移动数 3 个参数上改进现有的 LEDIR 算法，提出了一种 I-LEDIR 节点恢复算法，但不适用于工业无线传感器网络中使用；文献[7]提出一种芯片、传感器节点和系统相结合的 3 层节点恢复方法，通过对芯片端进行硬件修改、节点端进行跳频和扩频处理和系统端采用冗余路由，有效恢复网络链路，但实施复杂度过高。文献[8]提出了一种在检测到干扰攻击后能够抗干扰攻击的自适应速率通讯(Adaptive Rate Communication, ARC)方法，该方法将原始数据信息分解为多个编码的片段进行分别通信，以降低干扰攻击带来的干扰影响，并经过自适应调节报文分片的片长以获得更好的鲁棒性，降低了攻击的概率，但消耗能量较高。文献[9]则提出了一种在通信双方之间建立起低速率中继时隙信道(Low-rate Overlay Timing Channel, LOTC)的方法，即在干扰攻击检测方法检测出网络中存在人为恶意干扰攻击后，被干扰攻击节点能够与网络中其它传感器节点进行低速率通信，容易实现，能量消耗低，但低速率通信会导致网络吞吐量降低，影响正常通信。

本文得出一种结合非协调跳频扩频[10]、路由代价指标与 WirelessHART 图路由，进行被干扰攻击节点路由恢复的机制。通过非协调跳频扩频通信重新生成跳频序列，并结合干扰攻击检测方法，以摆脱干扰攻击的影响，通过将路由代价作为最小距离，引入 WirelessHART 图路由算法，以均衡网络消耗，将被干扰攻击节点重新添加到工业无线传感器网络中，最后通过合适的干扰攻击模型对被干扰攻击节点路由恢复机制进行验证。

1 网络模型与攻击模型

1.1 网络模型

假设一个网状拓扑结构的工业无线传感器网络，工业网络通信标准采用 WirelessHART 协议标准，路由协议采用图路由。由网络模型可知网络节点设置在普通的多信道(信道数 11~25)模式下通信，发送方的目标是在网络通信受环境干扰的情况下建立对接收方的通信。假设每个传感器节点配备有相应的频段，接收方具有可以有效进行传输、接收与计算数据的能力，此外通信双方具有认证机制，即每个接收方都保存发送方的认证信息，保证数据包的有效性。网络模型中 P_A 表示信号到达接收机的强度，P_A 的强度取决于信号的发送方能量、发送方与接收方之间的距离以及大小尺度衰落和环境干扰的影响。P_T 表示接收方所需的最小信号强度，即使得接收机能够成功获取信号的强度，并满足条件 $P_A>P_T$。

关于网络模型假设描述如下：

(1) IWSN 中的传感器节点随机分布在工业监测控制区域内；

(2) IWSN 形成后所有的传感器节点位置保持固定不变；

(3) 发送节点的信号强度大于等于环境干扰信号强度；

(4) 发送节点的信号强度大于等于接受节点接受数据的最小信号强度；

第 32 卷第 5 期 系统仿真学报 Vol. 32 No. 5
2020 年 5 月 Journal of System Simulation May, 2020

(5) 发送节点与接收节点信息数据保持同步。

将工业无线传感器网络定义为有向图 $G(V, \ell)$，其中 V 表示网络中传感器节点的集合，ℓ 表示传感器节点间无线连接的集合。假设 IWSN 中共有 k 个普通传感器节点，记做 $V=\{v_1, v_2,..., v_i,..., v_j,..., v_k\}$ $k\geqslant 2$，其中节点 v_i 的通信半径为 r_i。有向图 G 中的边 $e=(v_i, v_j)\in\ell$ 表示一对工业无线传感器节点(v_i, v_j)之间的单向无线连接，从 G 中的一条路径 $Path(v_1, v_j)$是多个边的有序组合序列，

$$Path(v_1,v_j)=((v_1,v_2),(v_2,v_3),...,(v_{i-1},v_i),...,(v_{j-1},v_j)) \quad (1)$$

1.1.1 WirelessHART 图路由机制

多路径图路由机制广泛用于工业无线连接数据通信中，机制中包含网络源节点到网络目的节点的路由表，路由表包含每一个节点的邻居节点地址、路由代价与节点能量等信息[11]。

图路由在每一跳中均预留冗余连接，有效地改善了网络路由的鲁棒性。在一个配置良好的网络中，所有节点在图路由中至少有 2 个邻居，通过它们可以发送数据包，节点可以将数据包发送给路由表中任何的邻居。以从网关(Access Point, AP)到普通传感器节点 E 的图路由策略为例，途经 A，B，C，D 传感器设备，为了发送一个包，AP 可以将它转发到设备 A 或 B，这些设备可以采取几种可选的路由：[AP, B, D, E]，[AP, B, C, E]，[AP, A, C, E]，[AP, A, D, E]，无论选用哪种方式，它最终都会到达最终节点 E 上。在实际应用中，正确配置的路由策略会通过图路由算法选择合适邻居图与最好的接收信号水平(Receive Signal Level, RSL)节点，保证路径连接有最好的通信质量，本文采用文献[12]的工业无线传感器网络图路由算法。

1.1.2 路由代价指标

由于工业无线传感器网络本身的特性，在判断路径的优劣时，通常需要以路由代价指标作为评判标准，路由代价指标通常可选择延迟抖动、延迟时间、能量有效性以及丢包率等[13]。为成功将被干扰节点重新加入到网络路由中，本文路由代价的指标采用丢包率、延迟时间与节点能量有效性等 3 个指标。

在 IWSN 通信中，网络中的每个传感器节点 v_i 均含有节点的延时信息、丢包率以及节点 v_i 的剩余能量等路由代价指标，同样网络的每一条链路 $e_{ij}=(v_i, v_j)\in\ell$ 也含有链路延时信息、链路丢包率以及节点 v_i 与 v_j 的剩余能量信息等路由代价指标。定义 $delay(v_i)$为网络中节点 v_i 的延时函数，$energy(v_i)$为网络中节点 v_i 的能量函数，$delay(e_{ij})$为链路 e_{ij} 的延时函数，$energy(e_{ij})$为链路 e_{ij} 的能量函数，$LinkCost$ 表示一跳邻居间通信的代价，v_S 表示源节点，v_D 表示目的节点。

路径 l 的代价指标为：

$$Cost(l)=Delay(l)+Energy(l)+PDR(l) \quad (2)$$

(1) 能量指标

采用参考文献[14]中的能量损耗计算模型来运算路由协议的能耗参数，模型如图 1 所示。

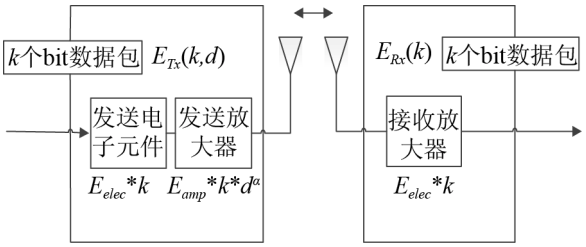


图 1 能量损耗计算模型

Fig. 1 Energy loss calculation model

图 1 中，E_{elec} 为发送与接收电路的能耗；E_{amp} 为放大电路的功耗；d 为数据传输距离；α 为传播环境的传播衰减指数，则发送 k bit 数据包时消耗的能量为：

$$E_{Tx}=E_{Tx\_elec}+E_{Tx\_amp}=E_{elec}\times k+E_{amp}\times k\times d^{\alpha} \quad (3)$$

接收节点接收 k bit 数据包时消耗的能量为：

$$E_{Rx}=E_{Rx\_elec}=E_{elec}*k \quad (4)$$

由公式(3)~(4)可知，路径 $l=Path(v_S,v_D)$在传输 k bit 数据包时的能量指标计算为

$$Energy(l)=\sum_{(v_i,v_j)\in Path(v_S,v_D)}E_{Tx}(v_i,v_j)+\sum_{(v_i,v_j)\in Path(v_S,v_D)}E_{Rx}(v_i,v_j) \quad (5)$$

(2) 延时指标

定义路径 $l=Path(v_S,v_D)$的延时函数为路径上节点的延迟与相邻节点之间链路的延迟和，因此可得网络中路径 $l=Path(v_S,v_D)$的延时函数为

$$Delay(l)=\sum_{v_i\in l}Delay(v_i)+\sum_{e_{ij}\in l}Delay(e_{ij}) \quad (6)$$

定义网络中的最高延时指标为 D，若路径 $l=Path(v_S,v_D)$的最小延时函数满足条件

$$Delay(l)<D \quad (7)$$

则路径 $l=Path(v_S,v_D)$可视为符合工业无线传感器网络 G 路由通信延迟的一条路径。

(3) 丢包率指标

路径 l 的丢包率指标表示为：

$$PDR(l)=\sum_{v_i\in l}PDR(v_i)\Big/num(l) \quad (8)$$

式中：$PDR(v_i)$为传感器节点 v_i 的丢包率；$num(l)$为路径 l 中的传感器节点个数。

1.2 攻击模型与检测

1.2.1 攻击模型网络拓扑

网络中的恶意干扰攻击者会攻击通信范围内的传感器节点，因此当网络中存在恶意干扰攻击时，通过干扰攻击入侵检测方法，会发现源节点到目的节点的路径中存在一片干扰区域，该干扰区域中的节点均受到恶意干扰攻击者的干扰攻击，处于干扰攻击区域内的传感器节点与邻居节点通信受到限制使得网络通信过程中路由受阻。受到恶意干扰攻击者干扰攻击后的网络拓扑如图 2 所示。即在恶意干扰攻击节点 3 的影响下，导致本应正常通信的节点 8，11，22 及相关节点通信信道受到干扰，需在检测出受到干扰的节点后重新计算路由代价，采取有效的抗干扰方法将这些受干扰节点恢复到网络中。

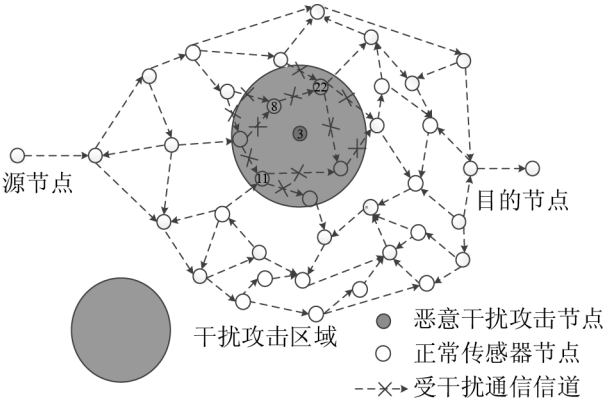


图 2 受到干扰攻击时的网络拓扑

Fig. 2 Network topology when under interference attacks

1.2.2 干扰攻击入侵检测

(1) 评判标准

将丢包率(PDR)作为干扰攻击入侵检测度量属性的评判标准。PDR 是指节点发送过程中丢失的数据包和节点发送数据包的百分比，即

$$PDR=(n-m)/n \quad (9)$$

式中：n 为发送节点发出的数据包个数；m 为通过接收节点接收的数据包数量；$n–m$ 为发送过程中丢失的数据包个数。

当干扰攻击造成数据包丢失时，PDR 均会发生变化，从而检测出节点处于被干扰攻击状态。

(2) 检测方法

采用统计过程控制理论中的控制图法作为分析方法。通过“三倍标准偏差法”来建立控制图中的上、下限[15]。

即将中心线确定在被控制对象的不合格率平均值 E 上，并以中心线为基准向上、向下偏移三倍标准偏差 D，确定上、下控制界限，建立不合格率控制表如表 1 所示。

表 1 不合格率控制表

Tab. 1 Fail rate control table

上下限	不合格率
上线(UCL)	UCL=E+3D
平均(AVG)	AVG=E
下线(LCL)	LCL=E–3D

在无干扰攻击环境下，计算网络中各节点的丢包率平均值如式 10 所示。

$$\overline{p}_i = \left(\sum_{j=1}^{n} \dot{p}_{ij} \right) \Big/ n \tag{10}$$

式中：n 为作为样本的数据包丢失率组数；$\dot{p}_{ij}$ 为节点 i 的第 j 组数据包丢失率。则不合格率控制表中的丢包率的平均值 E 与标准差 D 为：

$$E = \sum_{i=1}^{m} \overline{p}_i \tag{11}$$

$$D = \sqrt{\sum_{i=1}^{m} \left(\overline{p}_i - E \right)^2 \Big/ m} \tag{12}$$

式中：m 是节点的个数。

在无干扰的环境下，基站收集各节点的 PDR 数据。从收集的数据中选取部分样本数据，利用“三倍标准偏差法”对样本数据处理得出不合格率控制表。在控制图中不断监视节点的 PDR 是否在控制表的上下限内，判断网络中各节点是否处于被干扰攻击状态，若在控制表上下限内，则节点处于正常状态，对节点不做处理；否则节点处于被干扰攻击状态，对节点进行屏蔽，最终，完成循环检测中的一次节点检测。

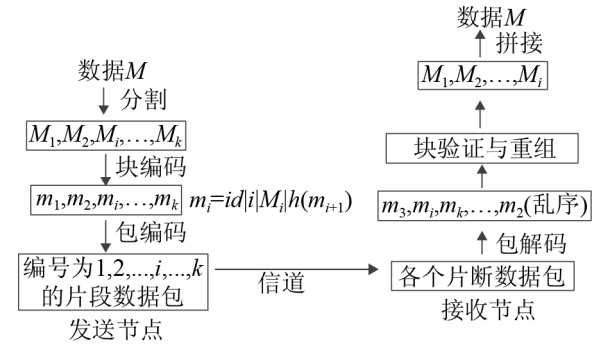
2 被干扰攻击节点恢复机制

2.1 扩频抗干扰技术

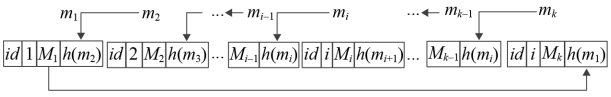
扩展频谱通信技术(Spread Spectrum, SS)简称扩频技术，该技术是对抗信号干扰时经常使用的对策，扩频技术通常在发送端通过扩频码进行扩频调制，在接收收端以相关解调技术接收数据，以达到抵抗干扰的效果[16]。该技术主要包括有直接序列扩频(Direct Sequence Spread Spectrum，DSSS)、跳频扩频(Frequency Hopping Spread Spectrum，FHSS)、跳时扩频(Time Hopping Spread Spectrum，THSS)与啁啾扩频(Chirp Spread Spectrum，CSS)等。每个技术又可分为传统扩频技术与非协调扩频技术。传统扩频技术通常采用伪码发生器、载波发生器、振荡器、调制器与解调器等，实际应用中易于实施、抗环境干扰效果明显，但是需要提前共享密钥，可能会被干扰攻击者窃取或篡改共享密钥，从而突破传统扩频技术实施攻击；非协调扩频技术不需要提前共享密钥，虽然实施复杂，但可靠性相比于传统技术更高。

2.1.1 UFH 抗干扰方法

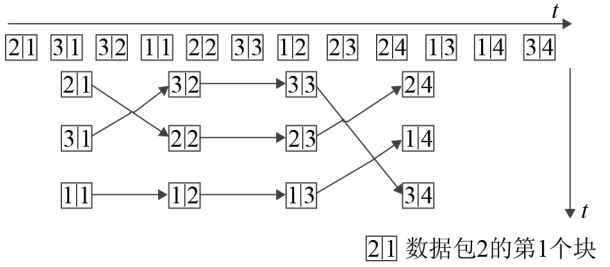
UFH 为非协调跳频扩频技术(Uncoordinated Frequency Hopping Spread Spectrum)，为有效抵御干扰，其在数据发送之前与接收之后都需要通过一系列处理。



(a) UFH 通信过程



(b) 循环 hash 链



(c) UFH 重组图

图 3 UFH 数据处理过程示意图
Fig. 3 UFH data process diagram

(1) 发送端的处理主要包括数据分割、块编码和包编码等几个阶段：

1) 数据分割：发送节点将数据包 M 分割为块 $M_1, M_2, M_i, ..., M_k (k \geqslant 2)$。

2) 块编码压缩：对各个块 M_i 进行块编码压缩处理，编码压缩后对应的块数据包 m_i 格式为：

$$m_i = id \,|\, i \,|\, M_i \,|\, h(m_{i+1}) \tag{13}$$

式中：id 为块 m_i 所属数据包 M_i 的编号；i 为数据 M 中块 m_i 与 M_i 的编号；$h(m_{i+1})$为一个数据包 m_{i+1} 的 hash 函数值，因此所有块的 hash 值可组成一个相互连接的循环 hash 链。

3) 包编码：将每个块添加相应序号(序号数为 1,2,...,i)的数据包中，然后各数据包进入通信信道。

(2) 接收端的处理主要包括包解码、hash 链验证重组和拼接几个阶段。

1) 包解码：接收节点收到的所有块数据包中，包含正常片段数据包与干扰攻击产生的数据包，接收节点对可解码的块数据包进行解码，不可解码的数据包片段则视为干扰，不断获取各个块 m_3, m_i, m_k,..., m_2 ($k \geqslant 2$)。

2) 块验证与重组：首先验证块 m_i 中的 id，确定其所属数据 M，计算比较块的 hash 函数，找到其前驱块 m_{i-1} 和后继块 m_{i+1}，将块 m_i 插入到前驱块与后继块中，即加入到 hash 链路中。对每个块进行上述操作，最终获得来自发送端的一个完整 hash 链，按照 hash 链提取块 m_i 中的 M_i。

3) 拼接：接收节点将块 M_1, M_2, M_i,..., M_k ($k \geqslant 2$)拼接为数据包 M。

2.1.2 UFH-FHSS 混合抗干扰方法

相比于传统抗干扰通信的循环依赖关系[17]在面对窃取、修改或冒充密钥等针对性强的恶意干扰攻击时存在安全隐患的问题，非协调跳频扩频技术有更高的安全性，但数据包验证重组导致耗能较高。所以通过 UFH-FHSS 混合方案来抵抗恶意干扰，即在网络初始化通信阶段采用非协调跳频扩频技术作为通信模式，在该模式下生成正常通信阶段传统跳频扩频所需要的跳频序列，打破传统扩频技术提前共享扩频序列带来的循环依赖的限制。非协调跳频扩频技术中通信双方在各自的频率通道之间随机跳跃，在不需要扩频序列的情况下保持通信，能够防止因跳频序列被攻击者窃取造成的干扰攻击影响，提高网络初始化通信阶段的安全性。同时，通过非协调跳频扩频生成的跳频序列进行传统跳频扩频通信，能够在网络节点能量受限的情况保持较低的能耗。

2.2 路由恢复

首先通过干扰攻击检测方法检测出被干扰攻击节点(节点被屏蔽，路由表中删除)，从而划分存在干扰区域，然后对被干扰攻击节点进行重启，利用抗干扰攻击方法中的非协调跳频扩频技术重新生成被干扰攻击节点与周围节点的跳频序列，被干扰攻击节点利用新的跳频序列进行传统跳频扩频，使用干扰攻击检测方法对该被干扰攻击节点进行检测，若新的跳频序列依然被干扰攻击者窃取或篡改，则干扰攻击区域内节点采用非协调跳频扩频通信，若被干扰攻击节点处于正常状态，则干扰攻击内节点采用传统跳频扩频通信，之后结合均衡路由代价指标与 WirelessHART 图路由算法将被干扰攻击节点恢复加入到网络路由中，流程图如图 4 所示。

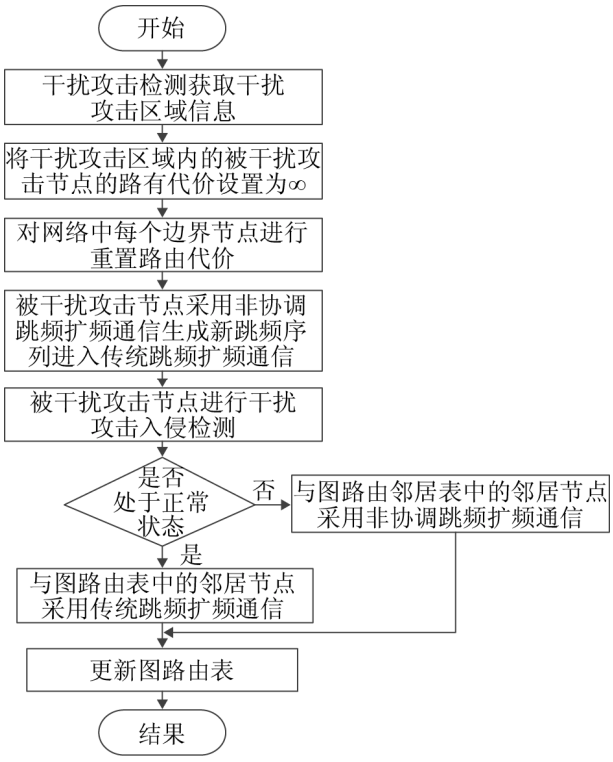


图 4 被干扰攻击节点恢复机制流程图

Fig. 4 Flow chart of recovery mechanism for interfered attack nodes

DOI: 10.16182/j.issn1004731x.joss.18-0638

第 32 卷第 5 期 系统仿真学报 Vol. 32 No. 5
2020 年 5 月 Journal of System Simulation May, 2020

具体步骤描述如下：

(1) 恶意干扰攻击者会攻击通信范围内的正常节点，通过干扰攻击入侵检测方法将网络中的被干扰攻击节点检测出来，获得网络中的干扰攻击区域，根据图路由表获取网络正常时的边界节点并进行标记。

(2) 在干扰攻击区域内的被干扰攻击节点无法将数据包传输到目的节点 v_D，故将全部被干扰攻击节点到目的节点的路由代价设置为∞。

(3) 干扰攻击区域边界的传感器节点即边界节点 v_B 生成重置数据包 M_{RESET}，若边界节点 v_B 到目的节点 v_D 所通过的上一跳节点在干扰攻击区域内，则数据包 M_{RESET} 用来通知重置路由代价，且数据包 M_{RESET} 中 *Cost* 值设置为边界节点 v_B 到目的节点 v_D 的路由代价，将数据包 M_{RESET} 通过广播的形式传输给周围的邻居节点，之后将边界节点 v_B 到达目的节点 v_D 的路由代价再重置为∞，否则不发送数据包 M_{RESET}。

(4) 边界节点 v_B 的某个邻居节点 v_O 在收到数据包 M_{RESET} 后，提取数据包中的 *Cost* 值，若该 *Cost* 值与发送节点的 *LinkCost* 值的和等于接受数据包 M_{RESET} 节点 v_O 的 $Cost(v_O)$，则传感器节点 v_O 到目的节点 v_D 的通信路径可能经过干扰攻击区域。节点 v_O 对数据包 M_{RESET} 中的 *Cost* 值进行修改，将 *Cost* 设置为节点的 $Cost(v_O)$值，将数据包 M_{RESET} 通过广播的形式传输给周围的邻居节点，之后将节点 v_O 的 $Cost(v_O)$值重置为∞。若该 *Cost* 值与发送节点的 *LinkCost* 值的和不等于接受数据包 M_{RESET} 节点 v_O 的 $Cost(v_O)$，则传感器节点 v_O 到目的节点 v_D 的通信路径不需要经过干扰攻击区域，故节点 v_O 标记为路径经过被干扰攻击节点的节点，更新到图路由的路由表信息中，并丢弃数据包 M_{RESET}。

(5) 干扰攻击区域内的被干扰攻击节点采用非协调跳频扩频进行通信，重新与邻居节点生成相应的新跳频序列，在一段时间内向邻居节点发出测试数据包 M_{TSET}，之后采用 1.2 节的干扰攻击入侵检测方法对被干扰攻击节点进行检测，判断是否恢复正常状态，若处于正常状态，则被干扰攻击节点利用新跳频序列进行传统跳频扩频通信，否则进行非协调跳频扩频通信。

(6) 获取网络中所有被标记为路径经过被干扰攻击节点的节点与所有干扰攻击区域的边界节点，对其路由代价进行判断，若节点的路由代价为∞，则不进行操作，若节点的路由代价不为∞，即该节点具有与目的节点 v_D 传输的有效路径，该节点重新建立路由数据包 M_{New}，将数据包 M_{New} 的 *Cost* 值设置为该节点的路由代价，将数据包 M_{New} 通过广播的形式传输给该节点周围的邻居节点，重新建立被干扰攻击节点的路由代价。

(7) 若接收节点 v_i 从发送节点 v_j 接收到数据包 M_{New} 后，接收节点 v_i 从数据包 M_{New} 中获取发送节点 v_j 到目的节点 v_D 的路由代价 $Cost(v_j)$，从图路由表中获得节点 v_j 的 *LinkCost*，并将图路由表中 v_j 的 *Cost* 值设置为 $Cost(v_j)+LinkCost$。

(8) 若传感器节点 v_i 是首次收到数据包 M_{New}，或 $Cost(v_j)+LinkCost<Cost(v_i)$，则将 $Cost(v_i)$设置为 $Cost(v_j)+LinkCost$，并且把数据包 M_{New} 中的 *Cost* 值设置为 $Cost(v_i)$，之后将更新后的数据包 M_{New} 通过广播的形式传输给节点 v_i 周围的邻居节点，告知邻居节点 v_i 的路由代价指标发生改变，并更新到图路由的路由表信息中，否则不处理，并将数据包 M_{New} 丢掉。

(9) 经过路由恢复步骤，干扰攻击区域内的被干扰攻击节点可重新建立到达目的节点 v_D 的路由代价，更新图路由表中每个节点的信息，WirelessHART 图路由算法根据路由表信息，重新建立被干扰攻击节点区域与各网络节点之间的路由。

3 实验结果分析

在仿真传感器网络时，OPNET 具有高效率、对真实实际应用的支持能力强以及拥有丰富的可利用的模型库等优点[18]。因此，选择仿真工具 OPNET 进行仿真。使用的参数配置如表 2 所示。包大小服从均值 512，方差 64 的均方分布；在管

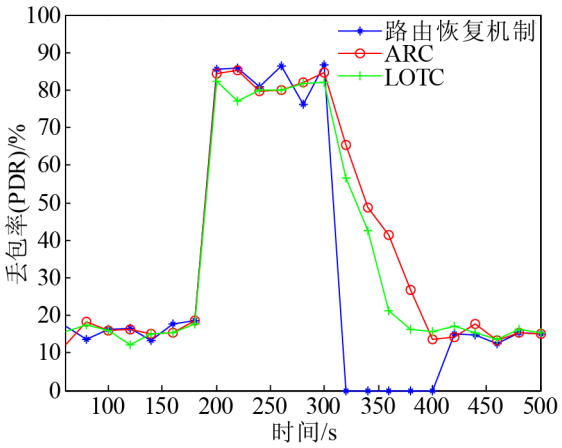
道阶段引入概率分布曲线将流量传输速率控制在 200~250 Kbit/s 之间随机分布。

表 2 仿真参数
Tab. 2 Simulation parameters

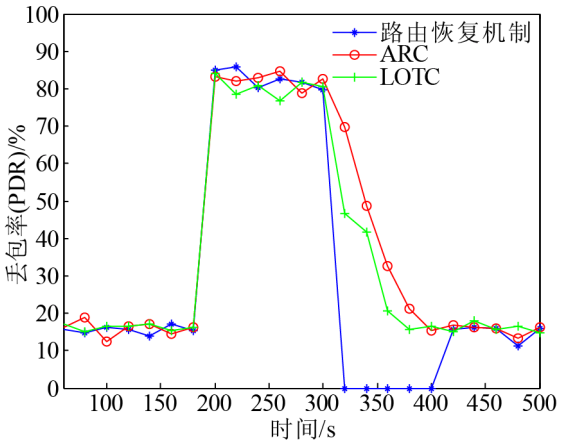
场景及节点参数	取值
仿真工具版本	OPNET 14.5 PL8 教育版
传输速率/(Kbit/s)	200~250
工作频段/GHz	2.4
包大小/byte	Normal(512,64)
仿真时间/s	500
仿真范围/m	500×500
通信距离/m	100
节点个数	40
noise figure	6.5×10^{7}

为研究被干扰攻击节点恢复机制的性能，通过仿真实验评估本文网络节点在智能型干扰攻击模型下路由恢复机制的性能，并与文献[8]的自适应速率通信方法 ARC 以及文献[9]的低速率中继时隙信道方法 LOTC 的性能进行对比。

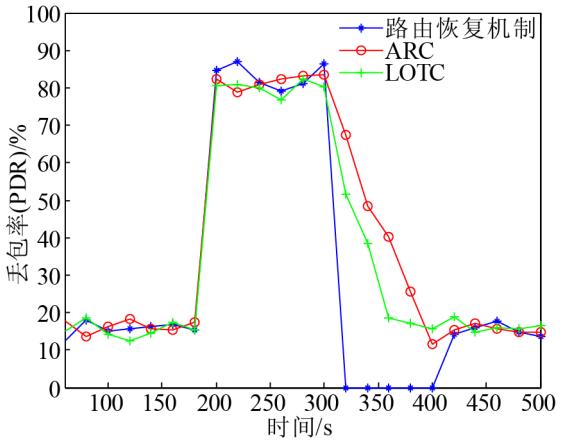
仿真集中关注工业无线传感器网络中被干扰攻击节点在正常状态、被干扰攻击状态、屏蔽状态与路由恢复之后状态的 PDR 比率与吞吐量变化，其中节点的网络拓扑结构如图 2 所示，仿真阶段分为无干扰攻击、有干扰攻击阶段、被干扰攻击节点屏蔽阶段与路由恢复阶段，为避免随机性，设置仿真时间为 500 s。为保证网络建立完整的路由表，数据在仿真开始前 60 s 不计入仿真结果；仿真时间 60~80 s 为无干扰攻击阶段，仿真时间 180~320 s 为有干扰攻击阶段，激活恶意节点 3 对周围传感器节点 8、11 和 22 进行攻击，恶意节点发送干扰数据包碰撞正常数据包，导致正常数据包破损或丢失，具体仿真的结果如图 5，仿真时间 320~400 s 为被干扰攻击节点检测阶段，通过干扰攻击入侵检测方法检测出处于被干扰攻击状态的节点，并对其进行屏蔽，从图路由表中删除，文献[8]与文献[9]方法中对处于干扰攻击状态的节点不进行操作，仿真时间 400~500 s 为被干扰攻击节点恢复阶段，将被干扰攻击节点重新加入到网络路由中，此时 ARC 方法中被干扰攻击节点完成转入自适应速率通信，LOTC 方法中被干扰攻击节点完成低速率中继时隙信道。



(a) 节点 8 的 PDR 变化图



(b) 节点 11 的 PDR 变化图



(c) 节点 22 的 PDR 变化图

图 5 3 个网络节点 PDR 变化图
Fig. 5 Three network nodes PDR changing graph

https://dc-china-simulation.researchcommons.org/journal/vol32/iss5/14
DOI: 10.16182/j.issn1004731x.joss.18-0638

第 32 卷第 5 期 系统仿真学报 Vol. 32 No. 5
2020 年 5 月 Journal of System Simulation May, 2020

3.1 节点 PDR 影响

仿真首先针对网络节点的 PDR，通过观察各阶段 PDR 变化曲线，初步分析各方法在干扰攻击下数据包是否能够正常发送与接收，各节点 PDR 变化仿真图如图 5 所示。干扰攻击下各种方法的网络节点在各个阶段的平均 PDR 如表 3 所示。

如图 5 所示，在仿真时间 60~180 s 的无干扰攻击阶段中，网络传感器节点受到环境干扰影响，PDR 维持在一定水平波动，在仿真时间 180~320 s 的有干扰攻击阶段中，网络传感器节点不仅受到环境干扰，还受到恶意节点的干扰攻击，节点 8，11 与 22 在恶意干扰攻击下的 PDR 明显升高，在仿真时间 320~400 s 的被干扰攻击节点检测阶段中，干扰攻击检测方法成功检测出节点 8，11 与 22 处于被干扰攻击状态。

表 3 网络节点各阶段的平均 PDR
Tab. 3 Average PDR for each phase of network node /%

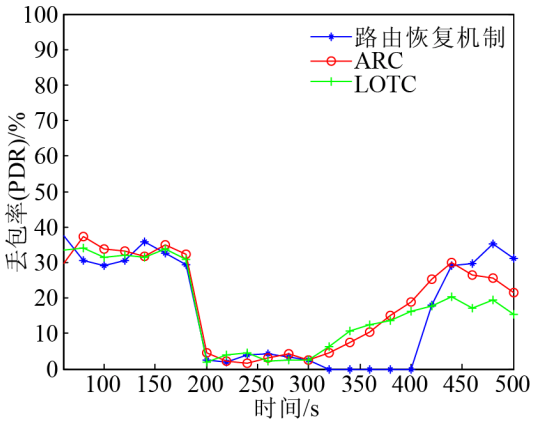
节点恢复方法	未受干扰攻击时 PDR	被干扰攻击时 PDR	被干扰攻击节点检测时 PDR	节点恢复后 PDR
路由恢复机制	15.87	83.61	无	15.33
ARC 方法	15.83	82.98	40.62	15.52
LOTC 方法	15.32	80.67	31.26	16.48

本文的路由恢复机制对被干扰攻击节点进行屏蔽，从图路由表中删除节点信息，使得节点 8，11 与 22 不与网络中节点进行通信，PDR 保持为 0，ARC 方法使得被干扰攻击节点逐步转入自适应速率通信中，LOTC 方法使被干扰攻击节点逐步转入低速率中继时隙信道，PDR 逐渐下降，结合表 3 可知，LOTC 相较于 ARC 转换到相应的通信方式速度更快，PDR 下降更快；在仿真时间 400~500 s 的被干扰攻击节点路由恢复阶段，被干扰攻击节点 8，11 与 22 的信息重新加入图路由表中，并且消除干扰攻击影响，与网络节点进行正常通信，ARC 与 LOTC 也已完成各自的通信方式转变，因此，PDR 趋于一定水平正常波动。

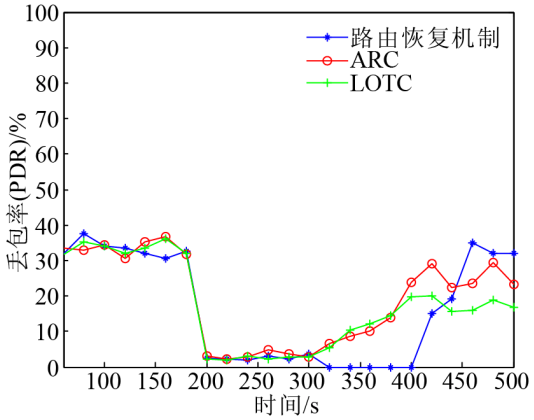
3.2 节点吞吐量对比

为详细对比观察被干扰攻击节点是否与工业无线传感器网络节点进行正常通信，以及路由恢复机制的性能，进一步通过 OPNET 对仿真通信各个阶段的吞吐量进行收集并分析，得到吞吐量变化仿真图如图 6 所示。干扰攻击下各种方法的网络节点各阶段的平均吞吐量如表 4 所示。

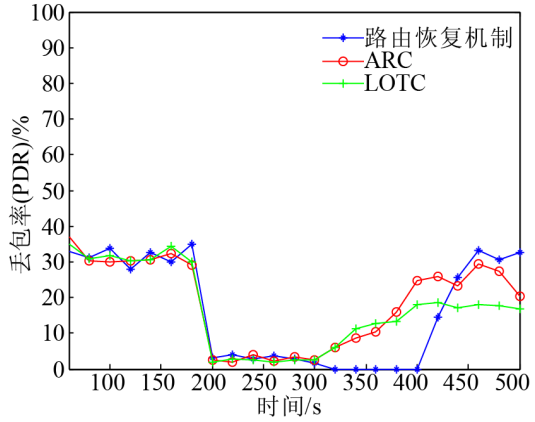
如图 6 所示，在仿真时间 60~180 s 的无干扰攻击阶段中，网络传感器节点只受到工业环境干扰情况下，保持着较高的吞吐量水平，然而在仿真时间 180~320 s 的有干扰攻击阶段中，网络传感器节点不仅受到环境干扰，还受到恶意节点的干扰攻击，节点 8，11 与 22 在干扰攻击下的吞吐量迅速降低，节点的通信受到限制。



(a) 节点 8 的吞吐量变化图



(b) 节点 11 的吞吐量变化图



(c) 节点 22 的吞吐量变化图

图 6 3 个网络节点吞吐量变化图
Fig. 6 Three node throughput change graph

表 4 网络节点各阶段的平均吞吐量
Tab. 4 Average throughput at each stage of network node /(kb/s)

节点恢复方法	未受干扰攻击时吞吐量	被干扰攻击时吞吐量	被干扰攻击节点检测时吞吐量	节点恢复后吞吐量
路由恢复机制	32.66	3.25	无	32.58
ARC 方法	32.94	3.81	12.23	26.45
LOTC 方法	32.18	3.17	13.94	18.89

在仿真时间 320~400 s 的被干扰攻击节点检测阶段中，干扰攻击检测方法检测出节点 8，11 与 22 处于被干扰攻击状态，对其进行屏蔽，使得节点 8，11 与 22 的吞吐量为 0，文献[8]在检测出节点 8，11 与 22 处于被干扰攻击状态后，将节点采用 ARC 方法通信，文献[9]在检测出节点 8，11 与 22 处于被干扰攻击状态后，将节点转入 LOTC 方法通信，吞吐量均不断保持上升。

在仿真时间 400~500 s 的被干扰攻击节点恢复阶段，被干扰攻击节点 8，11 与 22 在重新加入图路由表过程中，吞吐量持续上升，当被干扰攻击节点加入网络路由完成后，吞吐量到达较高水平波动，ARC 方法中被干扰攻击节点完成转入自适应速率通信，LOTC 方法中被干扰攻击节点完成低速率中继时隙信道转换，但 ARC 与 LOTC 方法中被干扰攻击节点并未彻底摆脱干扰攻击，导致吞吐量相对于本章的路由恢复机制吞吐量较低。

综上所述，在智能型干扰攻击下，被干扰攻击节点在通过路由恢复机制后，PDR 与吞吐量恢复到未受干扰攻击时正常的水平波动，即被干扰攻击节点能够成功恢复到工业无线传感器网络中。

4 结论

本文得出一种基于 WirelessHART 图路由的被干扰攻击节点路由恢复机制，其中非协调跳频扩频生成跳频序列，提高跳频序列生成的可靠性；将路由代价引入到 WirelessHART 图路由算法中，均衡网络消耗；干扰攻击模型验证了该路由恢复机制能成功使被干扰攻击节点消除干扰攻击影响，并重新加入到网络中。在今后将对方法进行实际工厂环境测试分析，进一步检验路由恢复机制的实用性，以便开发其它节点恢复机制，此外，将被干扰攻击节点路由恢复机制与其它干扰攻击检测方法结合，提高可靠性。

参考文献:

[1] Salam H A, Khan B M. IWSN-Standards, Challenges and Future[J]. IEEE Potentials (S0278-6648), 2016, 35(2): 9-16.

[2] 陈柯雨, 林荫宇, 肖智超, 等. 一种能耗均衡的无线传感器网络路由算法[J]. 电讯技术, 2017, 57(11): 1240-1245.
Chen Keyu, Lin Yinyu, Xiao Zhichao, et al. A wireless sensor network routing algorithm with balanced energy consumption[J]. Telecommunications Technology, 2017, 57(11): 1240-1245.

[3] Jin X, Kong F, Kong L, et al. Reliability and Temporality Optimization for Multiple Coexisting WirelessHART Networks in Industrial Environments[J]. IEEE Transactions on Industrial Electronics (S0278-0046), 2017: 1-1.

[4] Sasikala E, Rengarajan N. An Intelligent Technique to Detect Jamming Attack in Wireless Sensor Networks (WSNs)[J]. International Journal of Fuzzy Systems (S1562-2479), 2015, 17(1): 76-83.

[5] Henna K. Patiala K. Jamming Attack Detection and Isolation to Increase Efficiency of the Network in Mobile Ad-hoc Network[J]. International Research Journal of Engineering and Technology (S2395-0072), 2015, 2(4):

https://dc-china-simulation.researchcommons.org/journal/vol32/iss5/14
DOI: 10.16182/j.issn1004731x.joss.18-0638

第 32 卷第 5 期 系统仿真学报 Vol. 32 No. 5
2020 年 5 月 Journal of System Simulation May, 2020

510-516.

[6] Kaur J, Bansal K. An Improved LEDIR Technique Using LEDIR For Failure Node Recovery In WSN[J]. International Journal of Engineering And Computer Science (S2319-7242), 2015, 4(10): 14551-14558.

[7] 胡浩, 黄雄锋, 杨明月, 等. 工业无线传感器网络节点通信中的瞬时故障恢复[J]. 软件, 2011, 32(9): 12-15.
Hu Hao, Huang Xiongfeng, Yang Mingyue, et al. Instantaneous fault recovery in industrial wireless sensor network node communication[J]. Software, 2011, 32(9): 12-15.

[8] 吕绍和, 廖林冰, 李雯, 等. 无线网络抗干扰攻击的自适应无速率通信[J]. 计算机工程与科学, 2015, 37(3): 479-485.
Lü Shaohe, Liao Linbing, Li Wen, et al. Adaptive rateless communication for wireless network anti-jamming attacks[J]. Computer Engineering and Science, 2015, 37(3): 479-485.

[9] Xu W, Trappe W, Zhang Y. Anti-jamming timing channels for wireless networks[C]// ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April. New York, NY, United States: DBLP, 2008: 203-213.

[10] Strasser M. Efficient uncoordinated FHSS anti-jamming communication[C]// Tenth ACM International Symposium on Mobile Ad Hoc NETWORKING and Computing. New York, NY, United States: ACM, 2009: 207-218.

[11] Jemili I, Tekaya G, Belghith A. A Fast Multipath Routing Protocol for wireless sensor networks[C]// IEEE/ACS, International Conference on Computer Systems and Applications. Doha, Qatar: IEEE, 2014: 747-754.

[12] Modekurthy V P, Saifullah A, Madria S. Distributed Graph Routing for WirelessHART Networks[C]// In Proceedings of 19th International Conference on Distributed Computing and Networking. Varanasi, India: ACM, 2018: 1-10.

[13] 李世兴, 王宏, 周桂平. 适用于 WirelessHART 网络中实现图路由机制的 R-Dijkstra 算法[J]. 仪表技术与传感器, 2015(6): 131-134.
Li Shixing, Wang Hong, Zhou Guiping. R-Dijkstra algorithm for implementing graph routing mechanism in WirelessHART network[J]. Instrument Technology and Sensors, 2015(6): 131-134.

[14] 张志东, 孙雨耕, 刘洋,等. 无线传感器网络能量模型[J]. 天津大学学报:自然科学与工程技术版, 2007, 40(9): 1029-1034.
Zhang Zhidong, Sun Yugeng, Liu Yang, et al. Wireless sensor network energy model[J]. Journal of Tianjin University: Natural Science and Engineering Technology Edition, 2007, 40(9): 1029-1034.

[15] 徐宜敏, 孙子文. 工业无线传感器网络中干扰攻击的入侵检测[J]. 传感技术学报, 2017, 29(7): 1049-1055.
Xu Yimin, Sun Ziwen. Intrusion Detection of Interference Attacks in Industrial Wireless Sensor Networks[J]. Journal of Sensing Technology, 2017, 29(7): 1049-1055.

[16] 高文欢. 扩频通信技术浅析[J]. 中国无线电, 2015(8): 40-41.
Gao Wenhuan. Analysis of Spread Spectrum Communication Technology[J]. Chinese radio, 2015(8): 40-41.

[17] Strasser M, Pöpper C, Capkun S, et al. Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping[C]// 2008 IEEE Symposium on Security and Privacy. Oakland, California, USA: IEEE, 2008: 64-78.

[18] Yang S, He R, Wang Y, et al. OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p[C]// International Conference on Systems and Informatics. Shanghai, China: IEEE, 2015: 536-541.