高技术通讯 2010 年 第 20 卷 第 12 期:1211 ~ 1216

doi:10.3772/j.issn.1002-0470.2010.12.001

基于信誉评测机制的 WSN 安全路由协议研究①

杨 武② 马兴国 王 巍 苘大鹏 高光照

(哈尔滨工程大学信息安全研究中心 哈尔滨 150001)

摘 要 针对无线传感器网络(WSN)路由协议存在的安全问题,考虑到 WSN 节点能量低、资源有限的缺陷,提出了一种新型的 WSN 安全路由协议——VH-GEAR 协议。VH-GEAR 协议在地理位置能量感知路由(GEAR)协议的基础上引入了纵向(vertocal, V)和横向(horizontal, H)分析相结合的 WSN 节点信誉评测模型来提高路由协议的安全性,同时通过改进路由协议的信誉更新机制来减小能耗。基于 NS2 的仿真实验表明,VH-GEAR 路由协议能有效识别网络中的恶意节点,减小对合法节点的误判,降低网络能耗,从而加强了网络的安全性,延长了网络的生命周期,提高了网络的整体性能。

关键词 无线传感器网络(WSNs), 安全路由协议, 信誉评测模型, 信誉更新

0 引 言

无线传感器网络(wireless sensor networks, WSNs)是由不同区域内的传感器节点通过无线通信的方式组成的一种多跳自组织的网络系统,主要用来监视区域内图像、声音、气温、气压、湿度等物理环境的现场信息[1],目前在商业、工业和医疗等领域也都有了广泛的研究应用。WSN 安全路由协议是一个亟待解决的问题,因为其节点一般部署在环境恶劣区域、无人照看区域,甚至敌方区域,安全性直接影响其应用和推广。同时 WSN 节点能量低、存储资源少和计算能力弱也给安全路由协议的研究带来了困难。WSN 路由协议面临的安全威胁包括外部攻击和内部攻击。外部攻击由网络外节点发起,该类攻击可以通过密码安全机制进行有效防御;内部攻击由被俘获的内部节点引起,内部攻击无法通过密码安全机制进行防御,相对于外部攻击该类攻击威胁更大、防御更难。作为密码安全机制的有效补充,信誉机制在 WSN 防御内部攻击方面具有极大的优越性。

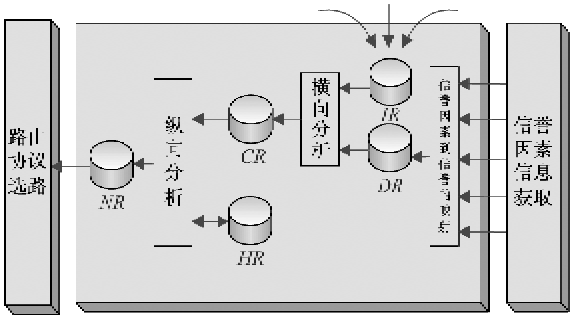
国内外许多研究人员都对 WSN 安全路由进行了深入研究,提出了一些协议,其中比较典型的是地理位置能量感知路由(geographic and energy aware routing, GEAR)协议,GEAR 协议本身具有较好的安全性,能够抵御槽洞攻击、虫洞攻击、Hello Flooding 等安全威胁[2]。但 GEAR 协议也具有一定的缺陷,它不能抵御虚假路由、女巫和选择性转发攻击。针对 GEAR 协议存在的安全问题,文献[3]提出了 GEAR 协议的改进安全路由协议(enhanced-GEAR, E-GEAR)。E-GEAR 在区域划分的基础上采用基于位置信息和二元 t 次多项式的密钥安全机制来抵御虚假路由攻击和女巫攻击,引入节点信誉评测模型来抵御选择性转发,识别发起内部攻击的恶意节点。但 E-GEAR 的信誉评测模型只是在横向上结合第三方节点对被评测节点进行信誉评价,而没有考虑被评测节点在整个生命周期中的全部记录和变化趋势,这种评价方式具有一定的片面性,会因为外界的瞬时干扰而导致合法节点的误判,从而造成评测不准确性问题。同时,在 E-GEAR 路由协议中每一次路由选路都要进行信誉更新,频繁的信誉计算加重了网络能耗的负担,减小了网络生命周期。针对以上问题,本文提出了一种新的基于信誉评价机制的 GEAR(Vertically & Horizontally GEAR, VH-GEAR)协议。VH-GEAR 协议通过引入纵向与横向相结合的 WSN 节点信誉评测模型来解决恶意节点误判的问题,同时通过改进信誉更新机制来减小网络能耗,最大限度地延长网络的生命周期。

1 WSN 的 VH-GEAR 安全路由协议

VH-GEAR 安全路由协议在 E-GEAR 协议的基

① 国家自然科学基金(60803144)资助项目。
② 男,1974 年生,博士,教授,博导;研究方向:计算机网络,信息安全;联系人,E-mail: gangwu@hrbeu.edu.cn
(收稿日期:2009-10-09)

础上进行了改进,引入纵向和横向相结合的 WSN 节点信誉评测模型来对节点行为进行信誉评价,有效识别网络中发起内部攻击的恶意节点。VH-GEAR 协议的选路算法以节点信誉为路由选路的一个主要参考标准,降低低信誉节点参与通信的概率,以此防御恶意节点对网络进行攻击。基于信誉评测的 VH-GEAR 安全路由协议的总体流程示意如图 1 所示。



DR:直接信誉;*IR*:间接信誉;*CR*:当前信誉;*HR*:历史信誉;*NR*:节点信誉

图 1 VH-GEAR 路由协议总体示意图

图 1 中信誉因素指节点的数据包转发和丢包行为,在 VH-GEAR 协议中信誉因素的获取通过多点确认机制来完成。*DR* 指直接信誉,是本地节点对被评测节点的信誉评价。*IR* 指间接信誉,是第三方节点对被评测节点的信誉评价。*CR* 指当前信誉,是由直接信誉和间接信誉横向分析而得到的对被评测节点的信誉评价。*HR* 指历史信誉,是本地节点存储的被评测节点的历史信誉。*NR* 指节点信誉,是由历史信誉和当前信誉经纵向分析后得到的对被评测节点的信誉评价。VH-GEAR 安全路由协议的选路基于多目标规划的最优性原理进行,其中 *NR* 作为路由协议选路的一个重要参考目标。

VH-GEAR 安全路由协议通过信誉评测模型对节点信誉的评价来识别恶意节点,而且结合纵向与横向信誉分析,从而降低了对合法节点的误判。VH-GEAR 协议安全效果示意图如图 2 所示。

1.1 纵向和横向分析相结合的节点信誉评测模型

1.1.1 直接信誉评价

VH-GEAR 安全路由协议通过信誉评测模型来防御选择性转发和自私节点等内部丢失性攻击,节点信誉主要在节点通信过程中产生,用来监测节点的通信性能,主要通过多点确认[4]的方法来获取,多点确认是通过多个节点对同一个数据包的确认来监测中间节点是否正常转发了该数据包,如果发包节点在限定时间内收到中间节点和其他节点对发出数据包的确认,则中间节点的节点信誉加 1,否则节点信誉减 1。

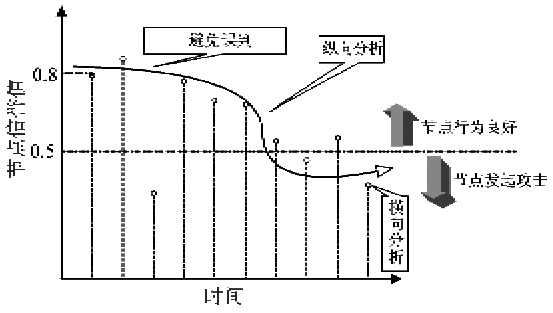


图 2 VH-GEAR 协议安全效果示意图

节点直接信誉评价以信誉因素为基础,其中信誉因素以被评测节点的通信行为为主,信誉因素的获取采用多点确认机制来完成。借鉴 BRSN 信誉评测模型[5]的思想,采用 Beta 分布描述节点的信誉分布。因此对 Beta 分布计算期望值可得到节点的信誉值。

定义 C_{ij}为节点 i 关于节点 j 的信誉分布,则

$$C_{ij} \sim \mathrm{Beta}(\alpha_{ij}+1,\ \beta_{ij}+1) \tag{1}$$

其中,α_{ij}表示节点 i 获得的关于节点 j 的正常行为次数;β_{ij}表示异常行为次数。

节点直接信誉 DR_{ij}是信誉分布的统计期望,即

$$DR_{ij} = E(C_{ij}) = E(\mathrm{Beta}(\alpha_{ij}+1,\beta_{ij}+1)) = \frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \tag{2}$$

1.1.2 节点信誉分析

信誉分析主要通过纵向与横向分析相结合来完成对节点的整体信誉评价。首先结合第三方节点的间接信誉 *IR* 对节点进行横向分析,得到节点的当前信誉 *CR*;然后结合 *CR* 和节点整个生命周期中的全部信誉进行纵向分析,纵向和横向分析相结合后便得到一个全面的节点信誉评价值 *NR*。

横向分析主要基于本地节点的直接信誉 *DR* 和第三方节点的间接信誉 *IR* 完成。为防止第三方节点的信誉欺骗,直接信誉的权重要高于间接信誉的权重,即直接信誉权重大于 0.5 且小于 1,横向分析后得到节点当前信誉 *CR*。

定义 CR_{ij}为节点 i 对节点 j 进行横向分析后得到的当前信誉,DR_{ij}为节点 i 对节点 j 的直接信誉,IR_{ij}为第三方节点 k 对节点 j 评价的间接信誉,ω_d 和 ω_i 分别表示直接信誉和间接信誉的权重,则

$$CR_{ij} = w_d \times DR_{ij} + w_i \times \frac{\sum_{k=1}^{n} IR_{kj}}{k} \quad (w_d + w_i = 1, w_d > w_i) \tag{3}$$

纵向分析结合 CR 和节点在整个生命周期中的全部信誉进行全面分析。纵向信誉分析采用指数加权移动平均(exponentially weighted moving average, EWMA)方法。

设节点的信誉序列为 y: $y \in \{y_0, y_1, \cdots, y_t, \cdots, y_n\}$,时间 t 的 EWMA 值为 $EWMA(t)$,时间 t 的信誉观测值为 y_t。当 $t \geqslant 2$ 时,结合时间 $t-1$ 的 $EWMA(t-1)$值可以求得 $EWMA(t)$:

$$EWMA(t) = \alpha \times y_t + (1 - \alpha) \times EWMA(t-1) \quad t \in \{2, 3, \cdots, n\} \tag{4}$$

其中,α 为当前信誉权重,y_t 为当前信誉 CR,$EWMA(t)$即为纵向和横向分析相结合后得到的节点信誉 NR。EWMA 方法以 $EWMA(t)$ 作为第 $t+1$ 时的预测值,即

$$\hat{y}_{t+1} = EWMA(t) \tag{5}$$

由此可以得到节点在下一时段信誉预测值的一般表达式为

$$\hat{y}_{t+1} = \alpha \times y_t + (1 - \alpha) \times \hat{y}_t \tag{6}$$

纵向和横向分析相结合的 WSN 节点信誉评测模型实现了对节点信誉的全面分析,弥补了简单的横向分析在不完全删除攻击下的检测缺陷,信誉评测模型中抚平短期波动的特性可以降低对合法节点的误判,显示长期趋势的特性也为有效识别网络中的恶意节点提供了保障。

1.2　周期性信誉更新机制

VH-GEAR 安全路由协议主要通过周期性信誉更新的机制来减少更新次数,降低网络能耗。在 E-GEAR 路由协议中每一次路由选路都要根据当前的节点信誉因素进行信誉计算,这大大加重了网络的能耗负担。在 VH-GEAR 安全路由协议中结合引入的信誉评测模型,对信誉更新机制进行了改进,信誉更新周期性进行,在每一次路由选路时直接获取当前的节点信誉值,而不是每次选路都要进行计算,这种更新方式弥补了信誉更新频繁,网络能耗负担重的问题,对网络整体性能的提升作用重大。

具体信誉更新过程由设置在邻居实体内的信誉更新定时器按设定周期定时触发,当每一个邻居节点被本地节点发现并添加时,都会为该邻居节点 neighbor 安装一个信誉更新定时器 updateTime,并自动启动,即 addTimer(updateTime,&(neighbor->repUpdateTimer_))。当定时器到达更新时间后,首先从邻居实体中获取信誉因素的最新信息,然后信誉对象根据当前信誉因素计算节点的直接信誉,随后相继进行纵向和横向分析,最终得到对该邻居的信誉评价,最后,信誉更新完成,定时器返回。定时器有 3 种返回状态可选择:定时器返回值 tc=0,更新周期不变继续定时;定时器返回值 tc>0,重设更新周期 updateTime=tc,继续定时更新;定时器返回值 tc<0,取消定时更新。改进后的周期性信誉更新如算法 1 所示。

```
void updateReputation( ){//周期性信誉更新算法
  RepUpdateTimer
  updateTime = REPUTATION_UPDATE_PERI;
  // 设置信誉更新周期
  TimerCallback    tc = 0;          // 定时器返回值
  addTimer(updateTime,&(neighbor->repUpdateTimer_));
  //在路由中启动邻居节点的信誉更新定时器
  while(updateTime->expire()){   //定时器到达更新时间
    computeReputation();          //计算信誉
    tc = newValue;          //设置定时器返回值
    if(tc   <   0){ //取消定时,直接返回
      return;
    }else if(tc >   0){    //重设信誉周期,继续定时
      updateTime = tc;       //重设信誉周期
    }else if(tc  =  =   0){          ;          //周期不变继续定时
    }
    继续等待更新;
  }
}
```

算法 1　VH-GEAR 协议的周期性信誉更新算法

1.3　VH-GEAR 选路算法

VH-GEAR 安全路由协议选路算法基于多目标规划最优性原理进行选路,综合考虑信誉、距离、能量等多个目标的最优。考虑 WSN 节点能量受限、计算能力弱的缺陷,为节省求解能耗,采用多属性效用法进行多目标规划求解,多属性效用法即给每个目标一定的优先级即权重,通过优先级构成综合目标,以此来评价各可行方案的优劣。在 VH-GEAR 选路算法中,综合目标是节点到目标区域的代价最小,代价公式为

$$c(N, R) = \alpha \times d(N, R)/d(S, R) + \beta \times e(N)/i(N) + (1 - \alpha - \beta) \times r(N) \tag{7}$$

其中,$c(N, R)$ 为邻居节点 N 到目标区域 R 的估计代价,α 为距离权重,β 为能量权重,$(1-\alpha-\beta)$ 为

信誉权重，$d(N, R)$ 为邻居节点 N 到目标区域 R 的距离，$d(S, R)$ 为源节点 S 到目标区域 R 的距离，这里使用归一化的距离 $d(N, R)/d(S, R)$，$e(N)$ 为节点 N 的剩余能量，$i(N)$ 为节点 N 的初始化能量，这里使用归一化的能量 $\beta e(N)/i(N)$，$r(N)$ 为邻居节点 N 在纵向和横向分析后计算得到的节点信誉 NR。

式(7)表示邻居节点的可用性，选路算法在所有可用节点中选择最优下一跳节点，即在可用邻居列表中选择到目标区域代价最小的邻居节点作为路由的下一跳节点。选路时，如果节点能量或信誉低于设定阈值，则该节点不可用，全网广播能量低或信誉低警告信息，并跳过该节点继续查找下一个邻居节点。否则计算节点到目标区域的代价。如果该节点到目标区域代价小于最小代价，则将该代价作为最小代价，并修改最小代价节点 ID 为当前节点 ID，否则计算下一邻居节点。最后返回最小代价节点 ID，即路由的下一跳节点。由此可得选路算法如算法 2 所示。

```
int findNextHop( ){//VH-GEAR 选路算法，选择下一跳节点
  if(邻居列表空)
    return -1;
  while(存在下一邻居节点){
    选择邻居节点;
    if(邻居节点能量低于阈值){//能量低
      广播节点能量低警告信息;
      Continue;
    }
    if(邻居节点信誉低于阈值)  {//信誉低
      广播节点信誉低警告信息;
      Continue;
    }
    计算节点到目标区域代价;
    if(代价 < 最小代价){//节点到目标区域代价最小
      更新最小代价;
      更新最小代价 ID;
    }
  }
  返回最小代价节点 ID; //选路算法选择下一跳节点
}
```

算法 2　VH-GEAR 协议的选路算法

2　仿真试验与结果分析

本文采用 NS2 仿真平台对 VH-GEAR 安全路由协议进行试验验证。为有效对比协议改进前后的性能，仿真试验采用了如下的参数指标：

(1)误判率(misjudgment rate)：对比分析协议改进前后将非攻击节点判定为攻击节点的数目与网络中非攻击节点总数的比率。

(2)识别率(judgement rate)：对比分析协议改进前后识别出的攻击节点的个数与设定的攻击节点总数的比率。

(3)能耗率(energy consumption rate)：对比分析协议改进前后网络中所有节点消耗的总能量与初始化总能量的比率。

仿真实验中使用的网络场景由 Setdest 随机生成，为达到较佳的实验效果，对个别节点做了适当调整，网络覆盖面积 800 × 800，网络中设置了 100 个 WSN 节点，生成的网络拓扑图，如图 3 所示。

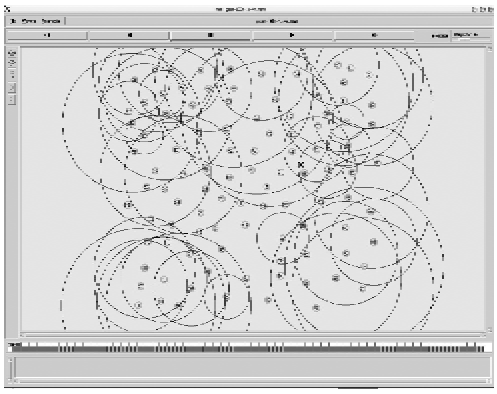


图 3　网络拓扑图

2.1　误判率

对比 VH-GEAR 路由协议和 E-GEAR 路由协议对意外丢包节点的误判率。仿真时长 1600s，发送节点个数 1，接收节点个数 4，信誉更新周期 100s，恶意节点个数 5，意外丢包节点个数[0,3,6,…,27,30]，意外丢包节点丢包率 80%，意外丢包时长 200s(丢包开始时间不定)，VH-GEAR 协议纵向分析的当前信誉权重 0.618 和 0.8。仿真后两种协议对意外丢包节点的误判率如图 4 所示。

从图 4 误判率对比图可以看出，VH-GEAR 协议从整体上降低了对意外丢包节点的误判率，可以提高网络安全性和生命周期。VH-GEAR 路由协议中误判率降低的主要原因是信誉评测模型中引入了纵向分析，抚平了短期波动，其中影响误判率的主要因素是纵向分析的权重 α，α 值越低对信誉的平稳效果越好，误判率越低。当 α 值接近 1 时，VH-GEAR 协议对历史信誉的参考接近于零，此时 VH-GEAR 协议和 E-GEAR 协议的信誉评测模型相当。

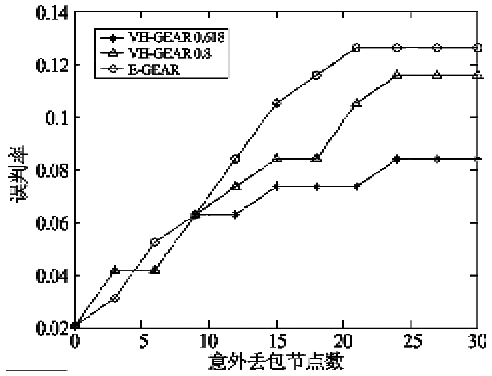


图 4　误判率比较

2.2　识别率

对比 VH-GEAR 路由协议和 E-GEAR 路由协议对恶意节点的识别率。实验仿真时长 1600s,发送节点个数 1,接收节点个数 4,信誉更新周期 100s,恶意节点的个数[3,6,…,21,24],恶意节点丢包率 80%,VH-GEAR 协议纵向分析的当前信誉权重 0.618 和 0.58。仿真后两种协议对恶意节点的识别率如图 5 所示。

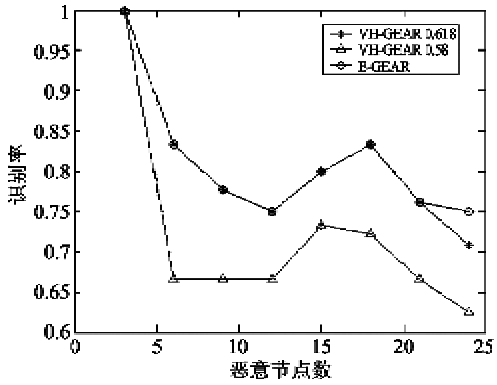


图 5　识别率比较

从图 5 可以看出,当 VH-GEAR 路由协议纵向分析的当前信誉权重 α 为 0.618 时,对恶意节点的识别率与 E-GEAR 协议相当,当 α 值降低为 0.58 时,对恶意节点的识别会有一定程度的影响。VH-GEAR 路由协议中影响识别率的主要因素是纵向分析中的当前信誉权重 α。当前信誉权重 α 越高对识别率的影响就越小,反之则对识别率的影响就越大。除 α 值外,对 VH-GEAR 路由协议和 E-GEAR 路由协议的识别都有影响的因素还有恶意节点丢包率和恶意节点分布。恶意节点丢包率和恶意节点分布都会对识别率产生影响:当恶意节点丢包率比较低时,信誉变化速度减缓,延长了识别恶意节点所需要的时间;当恶意节点不在关键路径上时,它们几乎不参与通信,信誉评测模型无法获得有效信誉因素,因此也无法进行有效的识别。虽然这些节点不能被识别,但因为它们并不在通信路径中,因此不会对网络造成大的影响。

2.3　能耗率

对比 VH-GEAR 路由协议、E-GEAR 路由协议和 GEAR 路由协议在一定时间内的网络整体能耗率。实验仿真时长 850s,发送节点个数 1,接收节点个数 4,初始化能量 100,节点传输能耗 0.660,节点接收能耗 0.395,节点闲置能耗 0.035,节点睡眠能耗 0.001,信誉更新周期 100s,恶意节点的个数 5,恶意节点的丢包率 80%。仿真后 3 种路由协议的能耗率如图 6 所示。

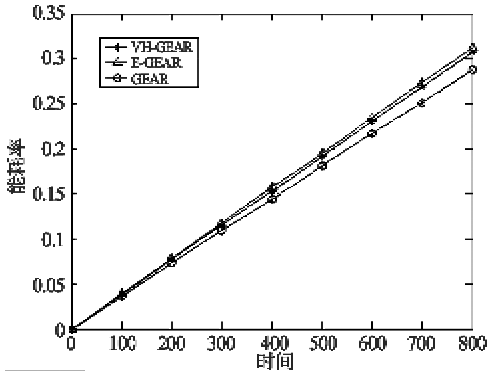


图 6　能耗率比较

从能耗率对比图可以看出,改进后的 VH-GEAR 路由协议比改进前的路由协议能耗更低。能耗降低的主要原因是信誉模型对节点的信誉计算是周期性进行的,选路协议在选择下一跳时直接获取节点信誉,减小了信誉计算次数;而改进前路由协议每次路由选路都需要根据信誉因素进行信誉计算,这大大加重了节点能耗负担。因此,虽然 VH-GEAR 协议在信誉模型中加强了信誉分析,但因为信誉周期性更新,减小了信誉计算次数,计算次数减小降低的能耗远远超过了附加分析所累加的能耗,从而从整体上降低了网络的能耗。

3　结　论

本文提出了一种新型的 WSN 安全路由协议 VH-GEAR 协议,VH-GEAR 协议以防御 WSN 路由协议存在的安全威胁为目的,在 GEAR 协议的基础上引入了纵向分析和横向分析相结合的 WSN 节点信誉评测模型来解决节点误判的问题,提高了路由协

议的安全性,同时,结合引入的信誉评测模型对信誉更新机制进行了改进,改进后降低了网络能耗,最大限度地延长了网络生命周期。最后通过 NS2 仿真实验表明,VH-GEAR 安全路由协议在安全性和能耗上都有很大的改进,对网络整体性能的提高作用明显。

参考文献

[1] Romer K, Mattern F. The Design Space of Wireless Sensor Networks. *IEEE Wireless Communications*, 2004(6): 54-61

[2] Yu Y, Estrin D, Govindan R. Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks. UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, 2001.1-11

[3] 杨光. 无线传感器网络安全路由协议研究:[博士学位论文]. 哈尔滨:哈尔滨工程大学.2009.23-33

[4] 俞波,杨珉,王治等. 选择传递攻击中的异常丢包检测. 计算机学报, 2006(29): 1542-1551

[5] Ganerival S, Balzano L K, Srivastava M B. Reputation-based Framework for High Integrity Sensor Networks. In: Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), washington, D.C., USA, 2004.66-77

Research on a security routing protocol based on reputation evaluation mechanism for WSNs

Yang Wu, Ma Xingguo, Wang Wei, Man Dapeng, Gao Guangzhao

(Information Security Research Center, Harbin Engineering University, Harbin 150001)

Abstract

In consideration of the security problems existing in present routing protocols for wireless sensor networks (WSNs) and WSN nodes, shortcomings of low energy and limited resource, the paper proposes the VH-GEAR protocol, a novel security routing protocol for WSNs. Based on the geographical and energy aware routing (GEAR) protocol, the VH-GEAR protocol introduces a WSN node reputation evaluation model based on Vertical & Horizontal analysis to obtain its preferable safety performance, and then improves the reputation update mechanism to obtain its preferable energy performance. The results of the simulation experiments on the NS2 show that the proposed VH-GEAR protocol can identify vicious nodes effectively and decrease both node misjudgment and node energy consumption, as a result, can improve the safety performance, the life cycle and the overall performance of WSNs.

Key words: wireless sensor networks (WSNs), security routing protocol, reputation evaluation model, reputation update