

基于门限路由的源节点位置隐私保护协议

李 江¹, 刘学军¹, 章 玮²

(1. 南京工业大学电子与信息工程学院, 江苏 南京 211816)

(2. 中国人民解放军 73677 部队, 江苏 南京 210016)

[摘要] 近年来,随着无线传感器网络在军事和医疗等领域的应用越来越多,无线传感器网络的隐私保护研究受到了人们的广泛关注. 本文提出了一种门限路由的源节点位置隐私保护协议(Threshold Routing for Source-Location Privacy Protection, TR),与已存在的源位置隐私保护协议不同,该协议可以提供更高效的隐私保护能力和有效地降低能量的消耗. 应用 NS2 进行模拟仿真实验,结果表明与其他的隐私保护协议相比,门限路由协议在能耗和隐私保护方面具有更好的性能.

[关键词] 无线传感器网络,隐私保护,源位置,门限路由

[中图分类号] TP393 [文献标志码] A [文章编号] 1001-4616(2014)01-0117-06

Threshold Routing for Source-Location Privacy Protection in Wireless Sensor Networks

Li Jiang¹, Liu Xuejun¹, Zhang Wei²

(1. College of Electronics and Information Engineering, Nanjing Tech University, Nanjing 211816, China)

(2. 73677 PLA Troops, Nanjing 210016, China)

Abstract: In recent years, along with the wireless sensor network have more and more widely been applied in the field of military and medical treatment field and so on, the wireless sensor network privacy protection and research get more the public attention. We proposed a protocol of Threshold Routing for Source-Location Privacy Protection in Wireless Sensor Networks (here in after referred to as TR). Different from the past agreement of source-location privacy preservation, the protocol which we propose can ensure the privacy of source node cases, and effectively reduce energy consumption. We do the simulation experiments based on NS2. The results show that Threshold Routing in this paper has more efficient safety protection ability and less energy consumption.

Key words: wireless sensor network, privacy preservation, source location, threshold routing

无线传感器网络(Wireless Sensor Networks, WSN)作为物联网的重要技术之一,在众多领域受到广泛的关注. WSN 是一种大规模的分布式网络,主要用于在一些天气恶劣或无人维护的环境中,由一些价格低廉、能源有限、计算能力低的节点自组织而成. 每个节点收集周围环境中的信息,通过多跳路由将信息传给基站.

但是,这种 WSN 很多时候是一种开放式的网络,很容易受到外界的攻击. 为了在得到精确数据的同时也能保护数据信息的安全,人们开始研究 WSN 的隐私保护策略. 已有的无线传感器隐私保护主要分为两种:数据隐私保护和位置隐私保护. 数据隐私保护的主要目的是保护节点之间的传输数据,防止非法用户的窃听和扰乱,其隐私保护的策略主要有数据加密、数据融合、用户认证等. 文献[1]对近年来传感器网络中的数据隐私保护作了综述性的描述. 位置隐私保护的主要目的是保护节点地理位置的隐私,防止攻击者对监测的目标或节点进行破坏和抓捕. 不同于数据隐私保护,位置隐私保护要从全局考虑,节点的位置信息不仅不含在节点间的传输数据中,同时与网络中数据的传输方式以及流量有关. 位置隐私保护对于传感器网络具有重要的作用. 例如,在现代的信息技术战场上,一般会在敌区散布一些隐密的节点来检测敌人的动向. 如果没有位置隐私保护,节点就会很容易被敌人发现,从而被破坏. 在熊猫与猎人的模式中^[2],科

收稿日期:2013-08-10.

通讯联系人:李江,硕士研究生,研究方向:传感器网络. E-mail:15251899213@yeah.net

学家通过传感器节点来观察熊猫的生活习性,但是猎人可以通过逆向追踪找到源节点的位置,这样熊猫的安全就受到了极大的威胁。

本文的研究内容是位置隐私保护,并提出了一种基于距离门限的路由协议(Threshold Routing for Source-Location Privacy Protection, TR), TR 路由协议将网络节点构建成一个基于距离门限的虚拟树状结构路由,同时在路由组建过程每个节点将通信范围内的节点分为两类:幻象节点和路由节点。TR 协议将数据转发过程分为两个阶段: h 跳有向数据转发和沿路由树转发。当目标移动到源节点感知范围内时,源节点选取满足条件幻想节点作为转发节点,以 h 跳有向路由转发感知数据。当 h 跳有向路由转发结束后,幻想节点再沿着路由树向 sink 转发。通过与过去协议的实验对比,本文提出的 TR 协议有效地延长了安全时间,大大增加了源节点位置的安全性。

1 相关研究工作

近几年,源位置隐私保护得到了广泛关注,人们提出了很多解决方案。在过去相关文献的研究中,可以将攻击者分为两类:全局流量攻击者和局部流量攻击者。全局流量攻击者通过对整个网络进行流量分析推测出源节点的位置,因为源节点位置周围的数据流量要比其他地方更密集,所以攻击者在监测全局流量时可以很容易地定位源节点的位置。最近文献[3]提出了有效防御这种攻击者的策略,通过向网络中植入虚假流量使得网络中的流量在被统计时保持一致。该策略有效地掩盖了源节点周围的传输流量,保护了源节点的位置隐私。由于对整个网络进行全局流量分析,需要大量设备和时间来收集足够多的数据,同时又容易被有效地防御,所以这种攻击方式并不是很常见。

局部流量攻击者通过监测部分区域内的流量,以逆向追踪的方式来寻找数据源节点。防御这种攻击方式,数据传输路由需要具有一定的随机性。Ozturk 等人^[4]最先提出了幻象路由协议,将数据传输路由通过两个阶段来实现。首先数据包从源节点开始随机 h 跳到达一个幻象节点,然后再由幻象节点按照最短路径路由向基站转发。幻象节点离源节点越远,隐私保护能力就越强。而经过简单的随机 h 跳转发后,幻象节点离源节点的位置并不足够远。姚剑波等人^[5]又提出了定向随机步发送方式,中继节点把收到的分组以等概率的方式转发给它的父节点。每个分组都以定向随机步的方式从信源节点转发到基站。但是以这种方式产生的幻象节点会集中某一特定区域,对于源节点的隐私保护效果不佳。文献[6]还提出源节点可视区的概念,攻击者一旦进入源节点的可视区,则认为源节点暴露。如果数据包由幻象节点向基站发送时经过源节点的可视区,那么攻击者在逆向追踪的过程中很容易发现源节点,幻象节点没有达到保护源节点的作用,称之为“失效路径”。Wang 等人^[6]提出了一种基于角度的源位置隐私保护协议,该协议有效地降低了失效路径的产生,但是角度的计算带来了节点额外的计算开支,同时也没有达到完全避免“失效路径”的效果。文献[7]中陈娟等人又提出了 PUSBRF 协议和 EPUSBRF 协议,通过源节点洪泛标记出可视区内的节点,在基站建立路由的时候避开这些可视区内的节点。该协议虽然一定程度上避免了“失效路径”,却在实际应用中存在一些问题:首先路由的建立是在源节点洪泛之后,对于监测移动的目标,这种方式的能耗很大;其次源节点可视区域内的洪泛带来了额外的通信开销。文献[8]提出了一种对于移动节点的位置隐私保护。文献[9]提出了一种可以同时抵御局部流量攻击者和全局流量攻击者的源位置隐私保护策略。

本文提出的 TR 协议是应用于静态网络中抵御局部流量攻击者的路由策略。在 TR 路由中考虑了“失效路径”的问题,同时解决了上述协议的不足,在避免产生“失效路径”的同时省去源节点的洪泛过程。不仅提高了对源位置的隐私保护能力,而且有效地降低了能量的消耗。通过与文献[6]提出的 PRLA 协议和文献[7]提出 PUSBRF、EPUSBRF 协议的实验对比,结果表明本文提出的 TR 路由协议可以更有效地保护了源节点位置的隐私,而且在减少能量消耗方面也要优于其他协议。

2 网络模型和攻击模型

本文假设网络模型中只包含一个 sink 节点和大量的普通节点。sink 节点的信息是公开的,每个节点通过多跳的方式将信息传输给 sink 节点。节点在检测到目标后变成源节点,在一段时间内,源节点会周期地将数据包发送给 sink 节点。

对于攻击模型,本文假设数据内容都经过加密处理,攻击者只可以偷听数据的传输。参考“熊猫一猎

人”博弈模型^[2],对攻击者做如下假设:

(1)攻击者具有优良的设备,可以逆向追踪数据包定位节点的地理位置,并且记录每一个经过的节点.

(2)攻击者的监听半径有限,只能从传输信息中获得下一跳节点的位置,不能直接进行多跳追踪.

(3)攻击者不会通过其他方式来攻击网络,如篡改数据包、破坏节点等,因为这些攻击方式可以被有效地防御.

sink 的信息是公开的,攻击者一开始位于 sink 节点处,监测 sink 与邻居节点之间的通信.一旦检测到有向 sink 发送的数据包,攻击者就开始向发送数据包的节点移动.以往的攻击模型可以分为两种:耐心攻击者和谨慎攻击者.前者攻击者会在一个节点处一直等待数据包;而后者如果在一段时间内没有接收到数据包,会回到上一个节点.根据文献[6]中的讨论,耐心攻击者比谨慎攻击者更具有危险性,所以本文只讨论耐心攻击者.

3 TR 协议描述

3.1 路由树和幻象节点表的生成

本文提出的 TR 路由是一种基于距离门限的虚拟树状路由.路由树组建仅发生在初始阶段,一旦路由树组建完毕,今后的数据传输不再需要重构路由树,除非网络的结构发生改变.

首先基站载入非对称密钥,每个节点也载入与基站共享的公匙,然后由 sink 节点开始广播信息 BM,建立树状路由. BM 由 BMO、D、Hop、Parents 组成,即 $BM = \{BMO, D, Hop, Parents\}$. 其中, BMO 为广播信息标识; D 表示距离门限值,其值根据隐私保护的要求人为设定; Hop 表示消息的跳数计数,初始为 0; Parents 表示广播信息从 sink 节点出发所经过的节点集合. 每个节点中都保存信息 hop、parents、phantoms, hop 表示节点沿着路由树到达 sink 的跳数,初始值为无穷大; parents 表示节点按照虚拟路由树向 sink 发送数据所经过的所有节点集合,即节点的祖先节点表,初始为空; phantoms 表示节点的幻象节点集合,即幻象节点表,初始为空; parents 和 phantoms 两张表在树状路由生成阶段同时生成.

当节点 n_i 接收到邻居节点 n_j 转发的广播消息 BM 后,当前节点 n_i 通过公式 $P_r = P_t(c_1/d)^n$ ^[10] 计算与邻节点的距离 d . 其中, n 和 c_1 为常数,一般取 $n=2, c_1 = \frac{\sqrt{GTGR\lambda}}{4\pi}$, GT 为发射增益、 GR 为接收增益、 λ 为载波波波长. P_t 为邻节点 n_j 发送数据时的功率, P_r 为当前节点 n_i 接收数据时的功率. 如果 $d > D$, 将转发节点 ID 存入当前节点的幻象节点表 n_i . phantoms 中, 成为当前节点 n_i 的幻象节点; 如果 $d \leq D$, 分两种情况考虑:

(1) BM 信息中的 Hop < 当前节点的 n_i . hop, 则将转发节点 n_j 设为路由树中当前节点的父节点, 并更新当前节点的 n_i . hop 和 n_i . parents, 即 n_i . hop = Hop、 n_i . parents = Parents, 同时更新 BM, 将 Hop+1, 当前节点 ID 加入到 parents 中, 转发广播信息 BM;

(2) BM 信息中的 Hop \geq 当前节点的 n_i . hop, 则丢弃广播信息 BM.

以此类推,直到整个网络中的所有节点都加入这个虚拟路由树.路由建立完成以后,每个节点都得到了距离源节点的最小跳数、所有的祖先节点和幻象节点,同时每个节点也得到其周围邻节点的这些信息.

3.2 源节点的转发机制

源节点是随机触发的,每个节点都可能成为源节点.当目标移动到某一节点感知范围内时,该节点变成源节点,向 sink 节点转发检测数据.数据包先从源节点进行 h 跳后到达一个幻象节点,再由幻象节点沿着建立的路由树向 sink 转发. h 值根据隐私保护要求确定, h 值越大,幻象节点离源节点越远,隐私保护能力就越强.

TR 协议的数据转发机制分为 2 个步骤,分别如下:

Step 1: 感知数据的 h 跳有向路由. 当检测到目标在感知范围之内时,源节点 S 感知数据,进行数据转发,同时将源节点 S 的位置坐标也包含在数据包中. 首先,在源节点的幻象节点表 S . phantoms 中选取一个幻象节点 M ,将感知数据转发给节点 M . 接着,节点 M 从它的幻象节点表 M . phantoms 中选取一个幻象节点 K ,将数据转发给节点 K . 以此类推,进行 h 跳转发,数据包达到一个幻象节点 L . 在 h 跳有向路由过程中,在幻象节点表中选取的幻象节点必须满足:(1)祖先节点表 parents 中不包含源节点 S ;(2)到源节点距

离较大. 条件(2)保证了数据包每次都尽可能朝着远离源节点的方向转发,避免了随机转发的环路问题.

Step 2:沿路由树转发数据. 当 h 跳数据转发结束后,最后的幻象节点 L 将接收到的数据包沿路由树向 sink 转发,同时基于安全考虑将包含在数据包中的源节点位置坐标抛弃. 这样能确保数据包在经过最小跳数到达基站.

整个转发过程如图1所示.

节点转发感知数据包的代码实现如下.

```

case DATA:      //源节点的数据转发
1  if  $h > 0$ 
2    在当前节点幻象节点表  $phantoms$  中随机选取一个节点  $M$ 
3    while  $M.parents$  包含源节点  $S$ 
4      do 将数据转发给  $M$ 
5     $h = h - 1$ 
6  end if
7  while ( $h > 0$ )
8    最后幻象节点沿着路由树向 sink 转发数据

```

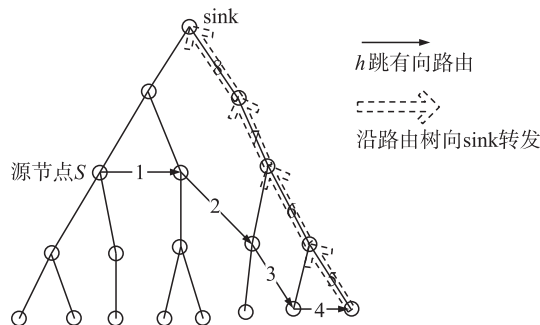


图1 源节点数据转发示意图

Fig. 1 Data forward diagram of Source node

4 TR 协议分析

4.1 幻象节点位置的多样性分析

由文献[7]的定理1可知,假设 sink 的第 i 个圆是以基站为圆心, $i \times R$ 为半径的圆, R 为节点的通信半径,如图2所示. 节点 N 距离 sink 的最小跳数为 H , 由于是基于最短路径路由协议,因此节点 N 位于 sink 的第 H 个圆与第 $H-1$ 个圆组成的环之间. 节点 N 简单地以基于邻节点距离 sink 的最小跳数进行 h 跳数据转发,最后数据包到达的幻象节点到 sink 的跳数为 $H+h$ 或者 $H-h$, 那么幻象节点的位置将集中在圆弧 $R_2R_1R_3$ 或者圆弧 $R_4R_6R_5$ 上.

但是 TR 路由在建立过程中,每个节点到 sink 的跳数 hop 都是基于门限值 D 的最小跳数,节点与父节点之间的距离小于门限值 D . 而在 h 跳有向路由阶段,每一跳选取的幻象节点与当前节点的距离大于门限值 D , 所以 h 跳数据转发结束后,数据包到达的幻象节点到 sink 的跳数不能确定为 $H+h$ 或者 $H-h$, 那么幻象节点就不会集中在上述所说的圆弧上,即满足了幻象节点地理位置的多样性.

4.2 “失效路径”的分析

文献[6]提出了“可视区”的概念,认为攻击者一旦追踪到源节点的可视区内,则源节点被发现的概率大大增加,因此 Wang 等人^[3]定义了在最短路经路由阶段经过数据包可视区的路径为“失效路径”. 在本文提出的 TR 协议中,网络基于门限值建立了最小跳数的路由树. 网络中的每个节点发送给 sink 的数据包都是沿着路由树转发,与文献[8]的网络模型不同,所以“可视区”概念在 TR 协议中并不适用. 本文重新定义“失效路径”为在幻象节点沿路由树向 sink 发送数据包的过程中经过源节点的幻象路径.

在 TR 路由协议中,每个节点中都保存 $parents$, $parents$ 表示节点按照虚拟路由树向 sink 发送数据所经过的所有节点,即节点的祖先节点集合. 利用节点存储的 $parents$ 信息,TR 路由在 h 跳有向路由阶段,每一跳在幻象节点表中选取的幻象节点必须满足祖先节点表 $parents$ 中不包含源节点 S . 经过 h 跳数据转发后幻象节点的祖先节点表也不会包含源节点,那么当幻象节点沿路由树向 sink 传送数据的时候就能有效地避开源节点,防止了“失效路径”的产生.

此外,不管是文献[6]提出的 PRLA 协议还是文献[7]提出的 PUSBRF、EPUSBRF 协议都需要源节点在 h 跳有向路由阶段前进行一次洪泛,将 h 跳内的所有节点都标识出来,以达到避免失效路径以及幻象节点位置多样性的要求. 但是对于移动的检测目标,所到过的节点越多,洪泛的次数就越多,带来的通信开销

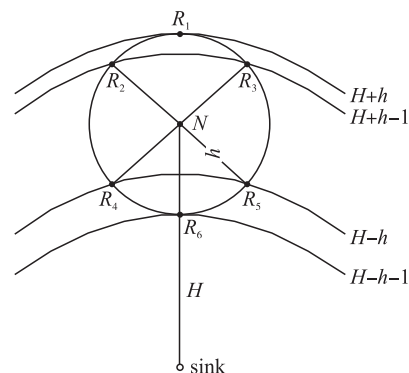


图2 基于距离基站的最小跳数的幻象节点分布

Fig. 2 Phantoms node distribution based on the minimum hop count from sink node

就越大.但是 TR 协议在虚拟路由树建立的同时,利用门限值 D 将节点的邻节点分为幻象节点和路由节点,源节点在 h 跳有向路由阶段可以直接在幻象节点表中选取节点进行 h 跳数据转发,最后到达的幻象节点能够有效地实现位置的多样性和避免“失效路径”的产生.基于 TR 协议的数据转发机制,避免源节点的洪泛过程,有效地降低了节点的通信开销.

5 实验结果分析

文本在 Ubuntu12.04 的平台上,利用 NS2 模拟仿真软件构建了一个简单无线传感器网络.实验过程中,将本文提出的 TR 协议分别与 $PRLA$ 协议^[6]和 $PUSBRF$ 、 $EPUSBRF$ 协议^[7]进行对比,从两个方面来衡量协议的性能:通信开销和安全时间.节点的能量消耗主要用于转发数据包,因此,本文将节点转发数据包的次数作为通信开销.安全时间是衡量网络安全性能的一个重要指标,本文定义安全时间为源节点被攻击者捕获前发送数据包的个数(源节点在一段时间内周期性地向 sink 发送数据包).

为了便于实验结果对比,本文使用与文献[7]相同的环境配置,在一个 $6\,000\text{ m} \times 6\,000\text{ m}$ 的区域内随机部署 $10\,000$ 个传感器节点,每个节点的通信半径为 100 m ,门限值 D 取通信半径的 $4/5$,即 80 m .sink 的位置固定不变,源节点通过事件触发,攻击者的监听半径等于节点的通信半径,攻击者一开始在 sink 位置等待.本文的实验结果是经过多次实验所得的平均值.

5.1 通信开销对比和分析

不管是本文提出的 TR 协议,还是 $PUSBRF$ 、 $EPUSBRF$ 协议和 $PRLA$ 协议,主要思想基本一致:首先源节点通过某种方式产生幻象节点,再由幻象节点向 sink 转发数据包.所以通信开销应该包括 3 个部分:广播,源节点 h 跳有向路由,数据包由幻象节点向 sink 转发. TR 协议中的广播仅出现在路由树组建阶段,路由树组建是一次性事件.在 $EPUSBRF$ 协议中,广播过程在源节点洪泛结束以后进行,对于不同的源节点,都要进行广播,因此,随着源节点的增加整个网络的通信开销也会随之成倍增加.其他协议的广播过程的通信开销趋于相同.在正常数据传输阶段, TR 协议不存在广播开销,所以本文在实验中没有进行这方面的比较.

图 3 为源节点距离基站的跳数 $H=60$,对于不同有向路由跳数 h 进行的实验结果对比,其中横坐标为有向路由的跳数,纵坐标为通信开销(用数据包转发的数量表示).如图所示,通信开销随着源节点进行有向路由跳数 h 的增加而增加.其中 $EPUSBRF$ 的通信开销最大,而 TR 协议与 $PRLA$ 基本相当.

图 4 为 $h=15$,对于不同的源节点距离 sink 的跳数 H 进行的通信开销对比.如图所示,通信开销则随着 H 的增加而增加.

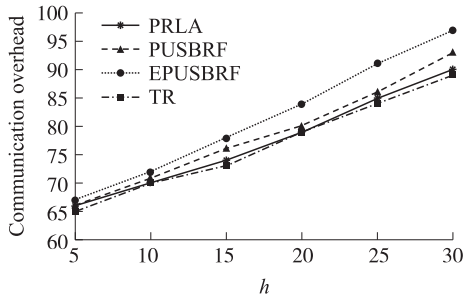


图 3 h 跳有向路由的通信开销对比

Fig. 3 Communication overhead compared with h which is the hop count in the directed routing

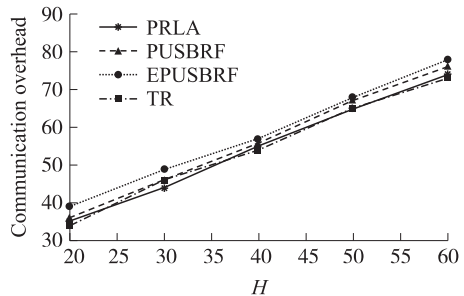


图 4 通信开销与源节点距离 sink 的跳数 H 关系

Fig. 4 Communication overhead compared with H which is the hop count from source node to sink node

由上述实验结果对比可知,4 种协议的通信开销相差不超过 10%,但是本文提出的 TR 协议与其他 3 种协议不同的是, TR 协议没有源节点洪泛过程,所以当监测目标在多个节点之间移动时, TR 协议的通信开销将远远小于其他协议.

5.2 安全时间对比和分析

图 5 为 $H=60$,对于不同的 h 进行的安全时间对比,其中横坐标为有向路由的跳数,纵坐标为安全时间(用源节点被捕获前发送的数据包个数表示).由图可知,随着 h 的增加安全时间也在增加.这是因为 h 越大,源节点产生的幻象节点随机性也越大,攻击者就越难捕获源节点. TR 路由协议的安全时间与 $PRLA$ 相比有着明显的提升,与 $PUSBRF$ 、 $EPUSBRF$ 相比也有略微的提升,因为 TR 路由中引入了门限值 D ,使得

h 跳有向路由中的每一跳都足够远,让攻击者更难捕捉到源节点的真实位置.

图6为 $h=15$,对于不同的 H 进行的安全时间对比.由图可知,随着源节点距离基站的跳数 H 增加,平均安全时间也随之增加.其中TR协议相对于其他3种路由协议还是有着明显的提升.

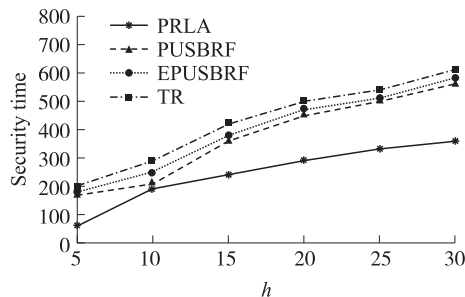


图5 h 跳有向路由的安全时间对比

Fig.5 Security time compared with h which is the hop count in the directed routing

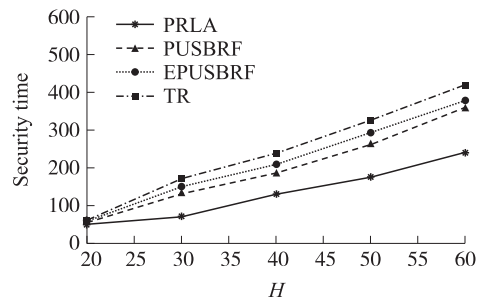


图6 安全时间与源节点距离 sink 的跳数关系

Fig.6 Security time compared with H which is the hop count from source node to sink node

根据上述可知,随着 h 和 H 的增加,安全时间也会随之增加,但是图3和图4显示, h 和 H 的增加也会带来通信开销的增加,那么就需要在安全性能和通信开销之间寻找一个平衡点.由图5可知,当 $H=60$, h 从10增到15时,安全时间增长最快, $h>20$ 后,安全时间增长比较缓慢;图6又显示,当 $h=15$ 时, $H>40$ 后安全时间增长幅度较大.因此,为了平衡通信开销和网络的安全性能,一般取 $1/5 \leq h/H \leq 1/3$,具体可以根据安全需求来调整 h 的大小.

6 结语

对于用于目标检测的无线传感器网络,本文总结了过去协议存在的一些问题,在此基础上提出了TR路由协议.与以往存在的路由不同的是,TR协议引入了节点门限值和路由树概念,不仅避免了源节点的洪泛过程,而且有效地避免“失效路径”的产生和满足了幻象节点地理位置的多样性,从而提高了对源位置的隐私保护能力,同时降低了能量的消耗.在模拟仿真实验中,本文将TR路由协议的通信开销和安全时间分别与PUSBRF、EPUSBRF和PRLA相比较,结果表明TR路由协议在保持高效的安全性能的同时,减少了整个网络的通信开销.

[参考文献]

- [1] 范永健,陈红,张晓莹.无线传感器网络数据隐私保护技术[J].计算机学报,2012,35(6):1 132-1 146.
- [2] Kamat P,Zhang Y,Trappe W,et al. Enhancing source-location privacy in sensor net routing[C]//Proceedings of the 25th International Conference on Distributed Computing Systems(ICDCS). Ohio,2005:599-608.
- [3] Silvija Kokalj-Filipovic, Fabrice Le Fessant, Predrag Spasojevic. Trade-offs of source location protection in globally attacked sensor networks;a case analysis[C]//2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. Salt Lake City,2011:323-331.
- [4] Ozturk C,Zhang Y,Trappe W. Source-location privacy in energy constrained sensor networks routing[C]//Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN). Washing DC,2004:88-93.
- [5] 姚剑波,郝晓青,文光俊.无线传感器网络中的位置隐私保护[J].传感技术学报,2008,21(8):1 437-1 441.
- [6] Wang W P,Chen L,Wang J X. A source-location privacy protocol in WSN based on locational angle[C]//Proceedings of the IEEE International Conference on Communications(ICC). Beijing,2008:1 630-1 634.
- [7] 陈娟,方滨兴,殷丽华,等.传感器网络中基于源节点有限洪泛的源位置隐私保护协议[J].计算机学报,2010,33(9):1 737-1 747.
- [8] Edith C H Ngai, Ioana Rodhe. On providing location privacy for mobile sinks in wireless sensor networks[J]. Wireless Networks,2013,19(1):115-130.
- [9] Yao Lin, Kang Lin, Deng Fangyu, et al. Protecting source-location privacy based on multirings in wireless sensor networks [EB/OL]. [2013-06-21] DOI:10. 1002/cpe. 3075.
- [10] 马朝,斌贾晋,康张立军. Ad hoc 网络中广播风暴的抑制方案[J].中国数据通信,2005(3):35-39.

[责任编辑:丁 蓉]