

文章编号:1001-9081(2015)03-732-04

doi:10.11772/j.issn.1001-9081.2015.03.732

无线传感器网络中基于路径序列检测的安全机制

陈 卓^{1,2*}, 谭志欢²

(1. 重庆理工大学 计算机科学与工程学院, 重庆 400054; 2. 通信抗干扰技术国家重点实验室(电子科技大学), 成都 611731)

(*通信作者电子邮箱 chenzhuo@cqu.edu.cn)

摘要:针对无线传感器网络(WSN)中容易受到的攻击的问题,提出一种新的基于路径序列检测的安全机制。该机制通过构建合理的路径序列并进行安全验证来实现数据包的路由规则检测及上一跳节点的身份认证,保证路由规则的正确性和数据的真实性。经过性能分析和仿真实验表明该机制在网络规模增加的情况下攻击检测失效的概率不会降低,所提策略能有效地检测出恶意篡改数据传输路径的路由攻击,提升无线传感器网络的安全性。

关键词:无线传感器网络;路由安全;路径序列检测;安全策略

中图分类号: TP393.03 **文献标志码:**A

Security mechanism based on path sequence detection in wireless sensor network

CHEN Zhuo^{1,2*}, TAN Zhihuan²

(1. College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China;
2. National Key Laboratory of Science and Technology on Communications (University of Electronic Science and Technology of China), Chengdu Sichuan 611731, China)

Abstract: To the problem of vulnerable to be attack in Wireless Sensor Network (WSN), a new security mechanism based on path sequence detection was proposed in this paper. This mechanism could detect the routing rule of packets and achieve the authentication of previous hop through constructing reasonable path sequence and sequence verification, then the correctness of routing rule and authenticity of data could be guaranteed. Performance analysis and simulation results show that the probability of the failure of data transmission path attacks detection will not decrease with the network scale. This result demonstrates that the proposed mechanism can effectively detect tampering of data transmission path attacks and can improve the security of the wireless sensor network.

Key words: Wireless Sensor Network (WSN); routing security; path sequence detection; security mechanism

0 引言

近年来,基于无线传感器网络的各类应用大量涌现。但受传感器节点成本和网络部署环境的限制,无线传感器网络在应用过程中仍存在一些亟待解决的问题^[1-2]。其中,由于该网络结构相对松散,极易受到各种网络攻击。使得安全问题成为需要重点关注和研究的热点^[3-4]。目前在无线传感器网络中已存在多种攻击方式,例如:消息注入攻击、路由欺骗攻击、重放攻击、选择转发攻击等。在典型的无线传感器网络攻击方式中,攻击节点除了通过产生虚假信息威胁网络安全外,还会恶意改变数据包的传输路径,使正常数据通过不安全的路径,经过恶意节点而无法保证数据的安全性。所以完善的安全机制除了要保证数据来自正常节点外,更重要的是要保证数据按既定的路由进行传输,并且要尽可能地减少节点耗电量,延长整个无线传感器网络的生命周期。而这在已有研究工作中比较少被关注。

基于现有研究的不足,本文提出了一种新的路径序列检测算法(Path Sequence Detection Algorithm, PSDA)。该算法利用路径序列对数据包的路由规则检测与上一跳节点的身份认证,保证数据的真实性与路由规则的正确性。该算法的优

势主要体现在以下几点。

- 1) 保证正确的路由规则。本文提出的算法不会影响数据按既定的路由进行正常传输。
- 2) 数据的真实性。本文提出的算法能够通过身份认证来保证数据的真实性,防止攻击者利用向网络中注入的虚假消息而产生的路由错误。
- 3) 计算开销小。与传统的身份认证安全手段不同的是,本文提出的算法不需要运行任何加密算法或者哈希运算,仅需根据与一条特定路径相符的并被在这条路径上合法节点所共享的路径序列信息来进行数据安全性的判断,能够最大限度地减少节点的计算开销。
- 4) 低时延和低能耗。得益于本文提出算法的计算复杂度较小,使得节点处对数据进行安全处理所消耗的时间就相比传统的认证机制短很多,这有效地提高了数据传输的效率。同样,也使得节点对数据包进行身份认证计算的CPU能耗降低。

1 相关研究工作

国内外学者针对无线传感器网络所面临的安全问题进行了系统的研究^[1,5],Deng 等^[6]给出了一种通过数据分段来防

收稿日期:2014-10-15;修回日期:2014-12-03。 基金项目:国家自然科学基金重点项目(60833002);重庆市基础与前沿研究计划项目(cstc2013jcyjA40024);重庆市教委科技项目(KJ1400918)。

作者简介:陈卓(1980-),男,重庆人,副教授,博士,主要研究方向:无线传感器网络、多媒体通信; 谭志欢(1992-),男,湖南郴州人,硕士研究生,主要研究方向:无线传感器网络、云计算。

止数据被攻击节点俘获的方案。传感器节点将一个消息分割成若干固定长度的数据放入不同数据包中,通过不同的路由路径经过不同的传感器节点传输到数据汇聚点,数据汇聚点将收到的分组进行重组恢复出原始消息。但该手段会导致节点能量开销过大。加密保证了数据的机密性。由于传感器节点计算能力与电池能量受限,无线传感器网络中不适合采用计算复杂的加密方法,如:公钥加密,目前大多数应用于无线传感器网络的加密方法采用对称密钥加密。然而,采用对称加密方法需要重点研究如何在无线传感器网络中合理、有效而安全地进行密钥分配、密钥管理。另外,认证机制能够有效地防止网络中来自非法攻击节点的数据包污染,保证数据的完整性和数据来源的可靠性。传统的认证方法大致分为两种,对称密钥方法和非对称密钥方法(数字签名)^[7]。由于传感器计算能力有限,若计算量增大,则节点响应的能力下降,因此无线传感器网络不宜使用计算复杂度较高的非对称密钥方法。认证的实现方法主要通过发送节点在发送数据时附加上消息认证码^[8],在接收节点对消息重新计算并与从数据包中提取的消息认证码进行对比,如果相同则通过认证,否则可能是数据被篡改或者数据来自非法节点。信任管理需要构造出具体的信任模型,通过监测邻节点的行为来增加、减少对该节点的信任值,传感器节点选择信任值最高的节点作为下一跳。该机制能够使得数据的路由路径避免经过有可能是攻击节点的传感器节点。在信任管理领域中比较为人熟知的例子就是watch dog的应用^[9]。随着无线传感器网络发展与广泛应用,越来越多的无线传感器网络的安全技术研究致力于解决无线传感器网络中常见的威胁,极大可能地消除潜在危险节点以及保护网络中的数据,达到在不同应用环境下由实际安全需求制定出的一系列安全目标。

到目前为止,仍然没有一种安全机制能够完全地应对无线传感器网络中的所有问题,由于传感器节点简单的计算能力与受限的电池能量限制,在任何应用环境中都应该根据实际情况对网络安全需求和节点性能进行折中考虑,选择最合适的安全机制来应对网络威胁。

2 路径序列检测算法

2.1 算法运作机制概述

本节介绍新的路径序列检测算法,说明如何利用路径序列来进行路由规则检测与身份认证,使中间转发节点或接收节点可以利用路径序列判断对应数据包的安全性。路径序列检测算法的实施过程可以分为3个阶段,包括路由建立、生成路径序列和安全处理。具体的流程如图1所示。

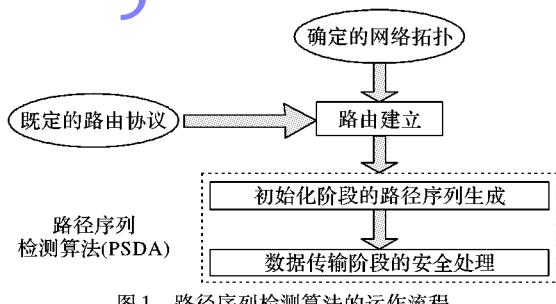


图1 路径序列检测算法的运作流程

无线传感器网络会在一个事先确定好的路由协议上开始运行,通常的路由协议会根据最小跳数搜寻到达汇聚节点

(sink)的最优路径。在路由建立好以后的初始化阶段,需要生成全网所有路径的路径序列,并且在每一个传感器节点上都存储经过该点的路径的序列。最后在数据传输阶段,每一个节点通过验证接收到的数据包上所携带的路径序列来进行路由规则检测与身份认证,保证数据包路由规则的正确性与数据真实性。

2.2 网络模型

无线传感器网络的簇通常由一个 sink 节点和多个部署在探测区域的传感器节点组成。路由协议,如:面向低功耗及易丢包网络的路由协议(Routing Protocol for Low power and lossy network, RPL)^[10],以最小跳数寻找到达 sink 节点的最优路径,实现数据从多点到一点的汇聚。在这样的情况下网络拓扑可以看作是一个有向无环图。因此本文考虑一个简单无环图 G,如图2所示。sink 节点有较强的计算能力,能量限制不严格;传感器节点计算能力和能量受限,负责收集传输环境数据。每一个传感器节点通过在同一个簇中的其他传感器节点根据某个既定的路由规则一跳一跳地将自己感知到的环境数据传输汇聚到 sink 节点,然后由 sink 节点把数据发送给基站。

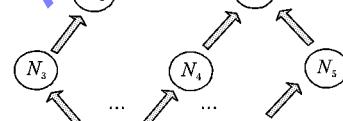


图2 有向无环传感器网络模型

在一个网络簇规模为 n 个节点的无线网络环境中,每个节点 $N_i (i = 1, 2, \dots, n)$ 周期性地感知环境数据并向单一的数据汇聚点 sink 发送消息数据 $M_i^j (j = 1, 2, \dots, n)$ (表示节点 N_i 发送的第 j 条消息);数据汇聚点 sink 在第 j 个 generation 需要接收来自整个网络的 n 条消息 $(M_1^j, M_2^j, \dots, M_n^j) (j = 1, 2, \dots, n)$ 。图 G 的每一条边 e 都可以传输数据,但同一时刻只能传输一个数据。对于任意节点,当有数据通过边 e 传输到 N_i 时, N_i 需要根据本方案中设计的安全机制对数据包的安全性进行判断:若符合安全要求则将数据包按既定的路由继续进行转发;否则发出危险警告并丢弃数据包。一个正常运作的无线传感器网络最终将在 sink 节点上实现对所有数据 $M_i^j (i = 1, 2, \dots, n, j = 1, 2, \dots, n)$ 的汇聚。

在有向无环图 G 中,按照节点的度数可以将节点分为两类,叶子节点 N_l 和非叶子节点 N_p 。 N_p 指度大于 0,有子节点的传感器节点;而 N_l 是指度为 0,即没有子节点的传感器节点。令 $\{0, 1\}^q$ 表示长度为 q b 的所有二进制串的集合。在网络簇规模为 n 个节点的传感器网络中,令:

$$b = \begin{cases} 2, & n \in [1, 2^8) \\ 4, & n \in [2^8, 2^{16}) ; k = 8 * b \\ N, & n \in [2^k, 2^{k+1}) \end{cases} \quad (1)$$

其中: k 表示在对网络节点进行路由信息表初始化时,每一个 N_i 都需要生成一段全 0 原始序列 $A_{init} \in \{0\}^k$,而该序列的长度为 k b。本文在第 3 章中介绍。因此本文需要区分网络中的叶子节点和非叶子节点。例如,每个传感器节点可以通过监听邻居节点的路由控制报文中的信息来统计子节点的个数,子

节点个数为 0 的节点即为 N_i 。

假设无线传感器网络运行于事先约定的路由协议之上,不失一般性在本文中的方案仿真中采用 RPL 路由协议。并且假设无线传感器网络在初始的路由建立阶段与路径序列信息交互阶段是绝对安全的,没有攻击节点参与。当网络运行稳定处于消息传输阶段时,多种攻击可能出现在网络中。

3 基于路径序列的安全机制

路径序列的产生关系着安全机制的有效性,因此路径序列选择要求满足:1)路径序列需要在网络中的每个节点中存储路由信息;2)路径序列需要根据网络拓扑结构变化进行适当调整;3)为了使攻击检测失效的概率适当降低,路径序列的长度需要合理设计。这里本文将介绍如何生成全网路径的路径序列并且初始化每个节点的路由信息表(Routing Table, RT)。一个无线传感器网络根据既定的路由协议建立好路由之后,首先本文要在环境数据传输开始前在全网中进行路径序列的生成与告知,使得在每一个节点上都存储一张初始化好的 RT。在一个网络簇规模为 n 个节点的无线传感器网络中,令:

$$T_i = t_{k-1}t_{k-2}\cdots t_1t_0 \in \{0,1\}; i = 1, 2, \dots, d \quad (2)$$

则某个特定的节点上的路由信息表的 k 条表项($(R_1, R_2, \dots, R_k) \in RT$)分别表示经过该节点的 k 条路由的路径序列,这些路径序列用于在接下来的数据传输过程中对经过该节点的数据包进行路由规则检测与身份认证。

如图 3 所示,首先网络中被识别的叶节点初始化生成一段长为 k 比特的全 0 原始序列:

$$Q_{\text{init}} = F_{\text{init}}L_{\text{init}} = q_{k-1}q_{k-2}\cdots q_1q_0 \quad (3)$$

其中: $F_{\text{init}} = q_{2\tau-1}q_{2\tau-2}\cdots q_{\tau+1}q_\tau \in \{0\}^\tau$, $L_{\text{init}} = q_{\tau-1}q_{\tau-2}\cdots q_1q_0 \in \{0\}^\tau$, $k = 2\tau$ 。

令 $Q_j \in \{0,1\}^k (j = 2, 3, \dots)$, 表示对 Q_{init} 的第 j 次记录修改序列。在一个网络簇为 n 个节点的无线传感器网络中,假设本文在一个节点 ID 为 x 的节点上得到了 d 条路径序列表项($(T_1, T_2, T_3, \dots, T_d) \in RT$)。每个序列 $T_i (i = 1, 2, 3, \dots, d)$ 的长度为 b 字节。路由信息表的初始化过程如图 4 所示。

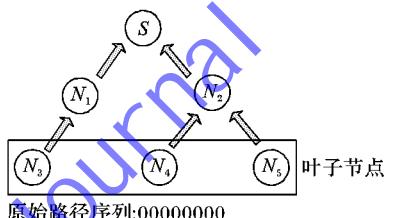


图 3 叶子节点初始生成全 0 原始序列示例

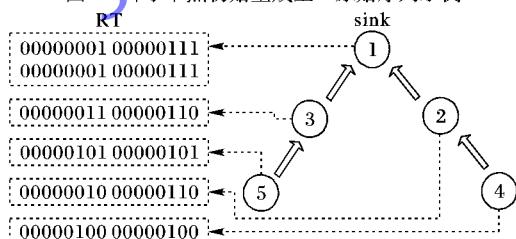


图 4 路由信息表的初始化过程示例

继续对在数据传输阶段进行安全处理的运作过程进行描述。路由建立完并在每个节点上的路由信息表被初始化好以后,就该进行环境数据的收集和消息的传输。当整个无线传

感器网络开始进行正常的运作时,节点周期性地感知环境并发送数据,sink 节点采集汇聚来自全网络中的环境数据。假设此时网络攻击可能会出现在网络中。该方案中每个传感器节点上存储的路径序列上记录着正常情况下数据包在到达该节点之前所经历的路径信息。在这个阶段各个传感器节点就利用这些路径序列对数据进行安全处理,实现对网络中每个数据包的路由规则检测以及身份认证。下面分别给出节点在数据发送过程和数据转发过程中的操作流程。

- 数据发送过程 源节点 $N_i (i = 1, 2, \dots, n)$ 。
 步骤 1 采集环境数据,生成消息包 $M_i^j (j = 1, 2, \dots)$ 。
 步骤 2 选择 $T_s \in RT_{Ni} = \{T_1, T_2, \dots, T_k\}_{Ni}$ (若 $k > 1$, 则任选其一) 并生成包 $T_s + M_i^j$ 。
 步骤 3 将 $T_s + M_i^j$ 发送出去。
 数据转发过程 转发节点 $N_v (v = 1, 2, \dots, n, v \neq i)$ 。
 步骤 1 从 $T_s + M_i^j$ 中分别提取出路径序列 T_s 和环境数据 M_i^j 。
 步骤 2 节点将自己的 ID 号赋给 F_s' , 把 L_s 与自己的节点 ID 号相异或生成 L_s' , 将 F_s' 与 L_s' 结合生成 T_s' 。
 步骤 3 在 RT_{Nv} 中检索:如果 $T_s' \in \{T_1, T_2, \dots, T_k\}_{Nv}$, 继续步骤 4;否则,丢弃该包并发出警报。
 步骤 4 重新生成 $T_s' + M_i^j$ 。
 步骤 5 将 $T_s' + M_i^j$ 按路由转发给下一跳。

特别说明:当恶意节点获知序列并产生恶意数据时,可能导致本文提出的攻击检测策略失效,但如 4.1 节所分析的,本文的策略可以尽可能地保证失效概率较低。

4 安全性分析及仿真实验

4.1 可证安全性分析

假设无线传感器网络在 RT 初始化完成后网络进入稳定运行阶段时,非法攻击节点加入该网络。非法攻击节点可能向网络中发送污染包或者更改了数据的传输路径时,数据包需要在每一个转发节点上进行基于路径序列的路由规则检测和身份认证。由于在原来已建立好路由的路径上的特定路径序列除了该路径经过的所有节点知道以外,后来新加入的非法节点是不知道的,因此污染节点需随机地伪造一段路径序列,携带在自己发送的污染包中,企图在下一个合法转发节点上进行路径序列验证时能够蒙混过关。

路径序列的长短取决于该网络的规模大小,假设网络中有 n 个节点,则路径序列的长度为 $bB, k b$ 。假设接收到该数据包的中间转发节点的 RT 表项有 d 项,由于 PSDA 采取的是单跳节点 ID 异或操作来生成路径序列,存储在节点的 RT 表项中的路径序列就有可能出现相同的情况,具体示例如图 5 所示。

如图 5,经过路径序列检测算法可以得到在节点 1 所存储的 RT 都为 00000001 00000111。由此可以看出,PSDA 检测伪造路径序列的概率与该中间节点的子节点数 x 有关($x \leq d$)。则对于一个携带了一段 $k b$ 的伪造路径序列的危险数据包,PSDA 能够成功检测出数据异常的概率 P_{det} 为 $1 - (1 - 1/2^x)^{\tau}$, $\tau = k/2$,也就是说本文所提出的机制在攻击检测中失效的概率 P_{inv} 仅为 $1 - (1 - 1/2^x)^{\tau} (x \leq d, \tau = k/2)$ 。为了使攻击检测失效的概率适当降低,路径序列的长度需要合理

设计。因此本文设计的路径序列长度为 b B, 其中 n 为无线传感器网络簇中的节点个数。随着网络规模的不断增大, 参数 $1/2^x$ 的减小速度快于同一节点下的子节点数 x 的增长, 因此攻击检测失效的概率 $1 - (1 - 1/2^x)^n$ 会变得越来越小, 该机制在网络规模较大时应用的安全性是极高的。

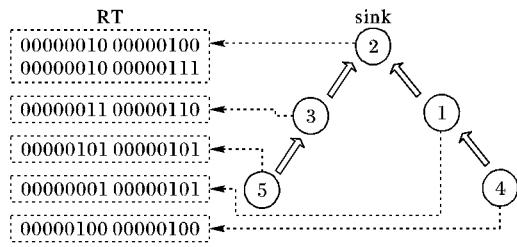


图 5 路径序列相同时的示例

为了解网络规模大小对 PSDA 安全性的具体影响, 进一步根据该机制在不同规模的网络中进行攻击检测失效的概率与任意中间节点 T 的子节点数量可得到如图 6 所示的关系。

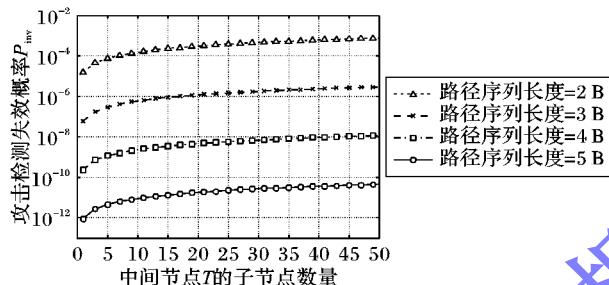


图 6 PSDA 攻击检测失效的概率与子节点数关系

取路径序列的长度为 2、3、4 和 5 字节, 分别对应于网络规模为最多为 $2^{16}, 2^{24}, 2^{32}, 2^{40}$ 的无线传感器网络, 因此该安全机制的网络可扩展性良好。从图 6 可以看出, 对于一个规模大小固定的网络, 经过一个节点的子节点数 x 越多, 安全性也就越低。另外随着网络规模的增大, 路径序列的比特长度 k 也会相应地增长, $1 - (1 - 1/(2^{k^2}))^n$ 的值理论上会大幅下降。因此正如图 6 中四条曲线的对比, 在网络规模越大路径序列越长的无线传感器网络中, 该机制进行攻击检测时失效的可能性会显著地降低。

4.2 仿真实验验证

本节通过系统仿真来检测并验证该机制在攻击检测方面的有效性。本文提出的 PSDA 机制在 Contiki 操作系统^[11]中实现, 利用 Cooja^[11]仿真器中的 Sky 平台进行仿真测试, 在仿真中本文采用 RPL 路由协议^[10,12]。本文在仿真平台上实现网络节点的路由信息表项的初始化生成。这里主要针对构造虚假最优路径的路由攻击场景以及发布虚假路由控制信息的路由攻击场景来验证本文提出算法的正确性。

如图 7 所示的网络场景, 传感器网络中正常节点 5 发送的数据包, 原本需经过 4 跳沿路径“5-1-2-3-4”到达 sink 节点 4, 攻击节点 6 进入网络后, 形成一条只需要经过 3 跳沿路径“5-6-3-4”到达 sink 节点 4 的虚假最优路径, 以此来改变数据的传播路径。图 8 中的仿真结果显示, 节点 5 的数据包传输路径被攻击节点 6 修改后, 节点 3 能够根据对路径序列的验证有效地检测出该攻击, 发现出不正确的路由, 发出警告信息并丢弃掉来自不规则路由的数据包。

另外, 本文构建了如图 9 所示的网络场景, 假设在网络稳定后的正常运行阶段, 新加入的攻击节点 6 可以通过发布虚

假的路由控制信息让它周围的节点改变优先父节点, 选择攻击节点 6 作为路由的下一跳, 以此改变数据包的传输路径。运行于 RPL 路由协议之上的无线传感器网络的节点之间相互监听公告的 DIO, 节点会根据邻居节点发来的 DIO 信息中的 etx 值来计算优先父节点, 以建立按最优路径的路由。

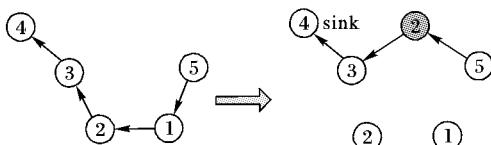


图 7 模拟加入构造虚假最优路径的攻击节点

ID:5 sending msg: <Hello 6 from the [node 5]>
ID:6 attacker received data, modify and relay
ID:3 [Warning]: illegal identification or irregular route ----- drop!

图 8 在虚假最优路径路由攻击下的仿真结果

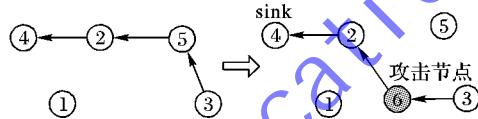


图 9 模拟加入发布虚假路由控制信息的攻击节点

攻击节点 6 周期性地发布虚假的 icmp 报文向周围节点公告错误的 etx 值(小 etx 值), 干扰周围节点对优先父节点的计算, 选择节点 6 作为数据包传输的下一跳。图 10 中的仿真结果显示, 节点 3 发出的数据被攻击节点 6 改变了路径后, 在到达网络正常节点 2 时被成功地检测出来, 发出警告信息并及时地丢弃这个途经了恶意攻击节点的危险数据包。

ID:5 sending msg: <Hello 3 from the [node 3]>
ID:6 attacker received data, modify and relay
ID:2 [Warning]: illegal identification or irregular route ----- drop!

图 10 在发布虚假路由控制信息攻击下的仿真结果

5 结语

本文针对无线传感器网络面临的常见网络攻击, 对传感器网络的安全机制进行了研究, 设计了一种基于路径序列检测的安全机制。通过安全性分析和仿真验证表明, 该机制能够有效地检测出非法攻击节点造成的消息注入攻击和恶意改变数据传输路径的路由攻击, 能够实现身份认证和路由规则检测。针对构造虚假最优路径的路由攻击和发布虚假路由控制攻击, 该机制通过对路径序列的验证来实现对数据包的路由规则检测与上一跳节点的身份认证, 保证了路由规则的正确性与数据的真实性。

参考文献:

- ZHOU Y, FANG Y, ZHANG Y. Securing wireless sensor networks: a survey [J]. IEEE Communications Surveys and Tutorials, 2008, 10(3): 6–28.
- HAO J, ZHANG B, MOUFTAH H T. Routing protocols for duty cycled wireless sensor networks: a survey [J]. IEEE Communications Magazine, 2012, 50(12): 116–123.
- AHMAD SALEHI S, RAZZAQUE M A, NARAEI P, et al. Security in wireless sensor networks: issues and challenges [C]// Proceedings of the 2013 IEEE International Conference on Space Science and Communication. Piscataway: IEEE, 2013: 356–360.
- ABDELHAKIM M, LIGHTFOOT L E, REN J, et al. Distributed detection in mobile access wireless sensor networks under Byzantine attacks [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(4): 950–959.

(下转第 740 页)

6 结语

无线传感器网络的安全性日益成为研究的热点。本文按照节点类型的不同,给予不同的检测任务,并且充分考虑了节点的安全性需求,对于各类节点进行不同的安全检测,有效提高了系统的安全检测率。同时本文着重考虑了网络的能耗问题,通过引入移动代理技术和代理节点,网络的整体能耗和簇头平均能耗得到了较大的降低,延长了网络的生存周期。由于无线传感器网络自身的复杂性,本文目前停留在仿真实验环境下,在实际应用中需深入研究,继续对其进行完善和改进。

参考文献:

- [1] SUN B, SHAN X, WU K. Anomaly detection based secure in-network aggregation for wireless sensor networks [J]. IEEE Systems Journal, 2013, 7(1): 13–25.
- [2] SU M, YANG X, WEI L, et al. Key management scheme in WSN based on property of circle [C]// Proceedings of the 2010 International Conference on Computational Intelligence and Software Engineering, Piscataway: IEEE, 2010: 1–4.
- [3] REN K, ZENG K, LOU W, et al. On broadcast authentication in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2007, 6(11): 4136–4144.
- [4] BAO F, CHEN I R, CHANG M, et al. Hierarchical trust management for wireless sensor networks and its applications to trust based routing and intrusion detection [J]. IEEE Transactions on Network and Service Management, 2012, 9(2): 169–183.
- [5] LIU A, ZHENG Z, ZHANG C, et al. Secure and energy-efficient disjoint multipath routing for WSNs [J]. IEEE Transactions on Vehicular Technology, 2012, 61(7): 3255–3265.
- [6] SU C-C, CHANG K-M, KUO Y-H, et al. The new intrusion prevention and detection approaches for clustering-based sensor networks [C]// Proceedings of the 2005 IEEE Wireless Communications and Networking Conference. Piscataway: IEEE, 2005, 4: 1927–1932.
- [7] NGAI E C H. Intrusion detection for wireless sensor networks [D]. Hong Kong: The Chinese University of Hong Kong, 2005.
- [8] ABDUVALIYEV A, LEE S, LEE Y-K. Energy efficient hybrid intrusion detection system for wireless sensor networks [C]// Proceedings of the 2010 International Conference on Electronics and Informa-
- [9] ESTIRI M, KHADEMZADEH A. A game-theoretical model for intrusion detection in wireless sensor networks [C]// Proceedings of the 2010 23rd Canadian Conference on Electrical and Computer Engineering, Piscataway: IEEE, 2010: 25–29.
- [10] HU H, YANG Z. Mobile-Agent-based adaptive data fusion routing algorithm in wireless sensor networks [J]. Journal of Electronics and Information Technology, 2008, 30(9): 2254–2258. (胡海峰, 杨震. 无线传感器网络中基于移动代理的自适应数据融合路由算法[J]. 电子与信息学报, 2008, 30(9): 2254–2258.)
- [11] PANTAZIS N A, NIKOLIDAKIS S A, VERGADOS D D. Energy-efficient routing protocols in wireless sensor networks: a survey [J]. IEEE Transactions on Communications Surveys and Tutorials, 2013, 15(2): 551–591.
- [12] CHEN M, YANG L T, KWON T, et al. Itinerary planning for energy-efficient Agent communication in wireless sensor networks [J]. IEEE Transactions on Vehicular Technology, 2011, 60(7): 3290–3299.
- [13] ADEEL M, LATIF A, MUAZ M, et al. Energy gain enhancement by ECC coded data in wireless sensor networks [C]// Proceedings of the 2012 10th International Conference on Frontiers of Information Technology. Washington, DC: IEEE Computer Society, 2012: 13–17.
- [14] CHANG Q, ZHANG Y, QIN L. A node authentication protocol based on ECC in WSN [C]// Proceedings of the 2010 International Conference on Computer Design and Applications. Piscataway: IEEE, 2010: 606–609.
- [15] MASADEH S R, ALJAWARNEH S, TURAB N, et al. A comparison of data encryption algorithms with the proposed algorithm: wireless security [C]// Proceedings of the 2010 6th International Conference on Networked Computing and Advanced Information Management. Washington, DC: IEEE Computer Society, 2010: 341–345.
- [16] VERMA O P, AGARWAL R, DAFOUTI D, et al. Performance analysis of data encryption algorithms [C]// Proceedings of the 2011 3rd International Conference on Electronics Computer Technology. Piscataway: IEEE, 2011, 5: 399–403.

(上接第 735 页)

- [5] MARTINS D, GUYENNET H. Wireless sensor network attacks and security mechanisms: a short survey [C]// Proceedings of the 2010 13th International Conference on Network-based Information Systems. Piscataway: IEEE, 2010: 313–320.
- [6] DENG J, HAN R, MISHRA S. Countermeasures against traffic analysis attacks in wireless sensor networks [C]// Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks. Piscataway: IEEE, 2005: 113–126.
- [7] LOCKE G, GALLAGHER P. Digital Signature Standard (DSS) [EB/OL].[2014-10-05]. <http://www.docin.com/p-434165217.html>.
- [8] BLACK J R. Message authentication codes [D]. Davis: University of California at Davis, 2000.
- [9] ROMAN R, ZHOU J, LOPEZ J. Applying intrusion detection systems to wireless sensor networks [C]// Proceedings of the 2006 3rd IEEE Consumer Communications and Networking Conference. Piscataway: IEEE, 2006: 640–644.
- [10] VASSEUR J P, AGARWAL N, HUI J, et al. RPL: the IP routing protocol designed for low power and lossy networks [J]. IPSO Alliance, 2011, 13(6): 120–127.
- [11] VASSEUR J-P, DUNKELS A. Interconnecting smart objects with IP: the next Internet [M]. San Francisco: Morgan Kaufmann, 2010: 112–120.
- [12] CASADO L, TSIGAS P. Contikisec: a secure network layer for wireless sensor networks under the contiki operating system [EB/OL].[2014-08-06]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.6598&rep=rep1&type=pdf>.