DZS-LEACH：一种动态的WSN层簇式跨区安全多跳路由协议

缪成蓓[1] 白光伟[1,2] 顾跃跃[1]
（南京工业大学计算机科学与技术系 南京 210009）[1]
（南京大学计算机软件新技术国家重点实验室 南京 210093）[2]

摘 要 主要研究传感器网络安全和能量高效的层簇式路由协议机制。在深入分析现有LEACH协议所面临的安全威胁的基础上，提出了一种动态的、基于分区自治的层簇式安全路由协议DZS-LEACH。其核心思想是，在多跳路由中融入动态密钥管理，使协议适应无线传感器网络动荡的拓扑结构，增强了协议的延展性；同时，DZS-LEACH通过分区自治避免远离基站的节点直接与汇聚节点通信，以均衡节点能耗。仿真实验表明，改进的路由协议DZS-LEACH大大减少了因网络攻击而造成的数据流失，增强了抗攻击能力，显著降低了网络能耗，延长了网络生存时间。

关键词 传感器网络，安全路由协议，分区自治，动态密钥，均衡能耗
中图法分类号 TP393.03 **文献标识码** A

DZS-LEACH: A Dynamic Cluster Based Zone-spanned Secure Multi-hop Routing Protocol in WSNs

MIAO Cheng-bei[1] BAI Guang-wei[1,2] GU Yue-yue[1]
(Department of Computer Science and Technology, Nanjing University of Technology, Nanjing 210009, China)[1]
(State Key Laboratory of Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

Abstract This paper focused on the performance enhancement of the typical LEACH protocol in security and energy efficiency in wireless sensor networks. Considering security threats faced by the existing LEACH protocol, we proposed a novel dynamic hierarchical cluster-based zone-spanned secure multi-hop routing protocol, so called DZS-LEACH. The main idea is to introduce a dynamic key management scheme in the multi-hop routing protocol to provide communication protection. The DZS-LEACH enables, on the one hand, the scalability of routing mechanism and adaptation to the dynamic network topology, on the other hand, balances energy consumption by means of partition autonomy and avoids long-distance communication between sensor nodes and sink node. Our simulation experiments demonstrate that the proposed DZS-LEACH may enhance defense ability and reduce data loss caused by network attacks. Meanwhile, the energy consumption is reduced significantly and the network lifetime is extended.

Keywords Wireless sensor networks, Secure routing, Partition autonomy, Dynamic keys, Balanced energy consumption

1 引言

无线传感器网络是由部署在监测区域内的大量微型、低成本、低功耗的传感器节点组成的多跳无线网络。其目的是协作地感知、采集和处理网络覆盖范围内监测对象的信息，并发送给观察者。与传统网络的路由协议相比，无线传感器网络路由协议需具备以下条件：能量高效、可扩展性，适应动态的网络拓扑结构、鲁棒性和快速收敛性。当前，能量高效已经成为无线传感器网络路由协议研究领域的一个关键性问题。

传感器网络的应用领域非常广泛，主要包括军事、环境监测和预报、健康护理、智能家居、建筑物状态监控、城市交通以及机场、大型工业园区的安全监测等领域。在这些应用中，传感器节点需要与基站进行实时通信以便采集及时有效的数据，由于部署的环境常常在无人监管的区域，传感器网络更容易受到恶意节点的攻击，更容易被捕获和破坏。因此，安全性已成为无线传感器研究领域一个重要研究课题。2002年Eschenauer和Gligor首次提出密钥预分配方法[1]；在此基础上，Anjum F等提出的对称密钥管理方案[2]引起了人们的广泛关注，其核心思想是在网络部署之前为每个传感器节点预先分配一个密钥，需要进行安全通信的任意两个节点之间创建出一个成对密钥来保护将要产生的报文信息。然而这种静态的密钥分配方式并不能完全适应无线传感器网络动态的随机拓扑环境。在传感器网络分簇结构和Exclusion Basis Systems (EBS)的基础上，Eltoweissy等人提出了动态密钥管理的概念[8]，其动态且高效的密钥管理方式在保证安全条件下，相比于静态密钥管理，大大节约了存储空间，提高了能量效率。如

本文受国家自然科学基金项目(60673185,61073197)，江苏省自然科学基金项目(BK2010548)，南京大学计算机软件新技术国家重点实验室开放课题(KFKT2010B08)资助。

缪成蓓(1987－)，女，硕士生，主要研究方向为无线传感器网络安全路由协议等，E-mail：miaochengbei@163.com；**白光伟**(1961－)，男，博士，教授，博士生导师，CCF会员，主要研究方向为无线传感器网络、无线移动自组织网络、多媒体网络QoS、网络系统性能分析和评价等；**顾跃跃**(1985－)，男，硕士生，主要研究方向为无线传感器网络路由协议等。

何改进现有的层簇式路由协议使无线传感器网络面临的攻击威胁得到有效遏制，提高网络的安全性能是我们现阶段刻不容缓的研究工作。

本文在经典层簇式路由协议 LEACH 的基础上，一方面，依据能量模型，提出分区自治的概念，避免远离汇聚节点的传感器节点直接与汇聚节点通信，从而均衡了能量消耗；另一方面，改善 EBS 密钥管理方案，使其成功应用于这种新型的层簇式路由协议，将“区域”引申为“表格”，以“表格”为单位进行网络攻击后的恢复。实验仿真结果分析显示，这种新的安全路由协议提高了网路的安全性能，显著增加了网络的生存周期，降低了网络丢包率，大大提高了网络的能量效率。

本文第 2 节分析典型的分簇路由协议 LEACH 及其面临的威胁；第 3 节提出基于分簇的跨区动态安全多跳路由协议 DZS-LEACH；第 4 节对 DZS-LEACH 协议进行实验仿真，分析其性能；最后总结全文。

2 典型分簇路由协议及面临的威胁

在无线传感器网络中，传感器节点的无线通信模块即使在空闲状态下其能量消耗也与收发状态时相差无几，所以无线传感器网络引入了分簇算法来适当地关闭通信模块，降低节点的能量开销[3]。分簇网络中节点通常被分为簇头和普通节点两类。由于簇头需要协调普通节点的工作，负责数据的融合和转发，因此能量消耗相对较大。为此，分簇算法周期性地更换簇头来均衡网络能耗。

2.1 典型的分簇路由协议 LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) 是最早提出的一种基于分簇结构的无线传感器网络分簇算法[4]，基本思想是以随机方式选举簇头节点，非簇头节点将感知到的数据通过相应簇头传输到汇聚节点。为防止某节点长期担任簇头而耗能过多，LEACH 定义了“轮”的概念，通过轮循环将整个网络的能量负载平分到每个节点。每一轮由初始化和稳定工作两个阶段组成。初始化阶段，随机选择节点为簇头，成为簇头的节点向周围广播信息，其它节点根据接收到的广播信息的信号强度 RSSI (Received Signal Strength Indicator)来选择它所要加入的簇，并告知相应的簇头。当簇头收到所有簇成员发送的信息后，根据簇内节点的数量创建 TDMA(Time Division Multiple Access)时刻表答复每个节点何时开始传输数据。簇头直接与汇聚节点通信，而成员节点只能与所属聚簇中的簇头通信。稳定工作阶段，节点持续采集监测数据，传送到簇头，由簇头对数据进行必要的融合处理之后发送到汇聚节点。持续一段时间后，网络进入新一轮循环。下一轮工作周期重新选择簇头。

由此可见，LEACH 协议采用层次结构，节点不需要存储大量的路由信息，网络相对均衡地消耗能量。但通过研究发现 LEACH 协议也存在一些问题。簇头与汇聚节点直接通信，远离汇聚节点的簇头能耗较大，死亡较早，死亡分布不均匀；簇头选举由于随机数产生的不稳定性可能导致簇头分布不合理和个数偏离期望值；节点的通信范围有限，簇头与汇聚节点的单跳方式限制了网络覆盖范围，不适用大规模部署的网络。

2.2 传统 LEACH 协议面临的安全威胁

节点部署于开放环境和节点资源有限等特点使得传感器网络面临着各种严重的攻击威胁，安全路由的研究已经成为传感器网络研究的关键问题。

研究表明，传统 LEACH 协议主要面临以下四种攻击：

(1) 虚假的路由信息[5]：攻击者通过欺骗、更改和重发路由信息建立新的路由路径，形成虚假消息、网络分割、时延增加等。

(2) Sybil 攻击[6]：攻击者以多个身份出现在网络中，使其更容易成为路由路径中的节点，然后和其它攻击方法协同达到攻击的目的。

(3) Hello Flood 攻击[5]：攻击者通过以足够大的功率广播 Hello 包，收到 Hello 包的节点会误以为攻击者是它们的邻居，从而建立虚假的路由路径，向攻击者发送数据。

(4)共谋[7]：攻击者通过捕获节点获得节点存储空间中的全部数据，包括密钥。随着被捕获节点的增加，它们共享得到的密钥信息直至所有管理密钥均被捕获时，整个密钥系统完全丧失了安全性。

我们可以将这四类归纳为两类，即把(1)－(3)归纳为节点欺骗，把(4)称之为节点侵占。对于静态密钥管理体系，即引言部分提到的密钥分配方案只能对第一类节点欺骗做出有效的防范，当传感器节点被攻击者捕获并获得节点的所有密钥，乃至形成共谋时，显然，静态密钥管理方案也已经被攻击者获知，针对这类攻击，我们采取动态的密钥管理分配方案，使得节点被捕获后网络动态生成新的密钥管理分配方案以恢复捕获节点，保证网络的安全性。

3 基于分区自治的层簇式安全路由协议 DZS-LEACH

本节研究一种新的多跳安全路由协议。首先，我们深入分析 EBS 密钥管理体系；其次，定义网络模型和能量模型，在此基础上，提出新的安全路由协议。本节分别从协议的簇首选举机制，利用动态密钥管理方案成簇及路径建立过程三个部分进行分析，最后针对网络安全问题提出协议的恢复机制。

3.1 EBS 密钥管理体系

2004 年 Eltoweissy 等人提出的 EBS 概念，是一种基于组合原理的密钥管理方法[8]。其中共有两种密钥：管理密钥和会话密钥。管理密钥用于 EBS 内部的密钥系统的建立和更新、会话密钥的生成、节点的驱逐等。会话密钥又称为通信密钥，用于组内或某些特殊节点之间的通信数据加密。

3.1.1 概念描述

定义 1 设 n,k,m 均为正整数，且 $1<k,m<n$。我们用 EBS(n,k,m)来描述集合 Υ，它是以集合$\{1,2,\cdots,n\}$的子集为元素的集合，对于任意 $t\in\{1,2,\cdots,n\}$，满足以下两个条件：

(1)t 最多出现在 Υ 的 k 个元素中；

(2)$\bigcup_{i=1}^{m}A_i=\{1,2,\cdots,n\}-\{t\}$即任何一个 t 都可以由恰好 m 个集合排斥掉。

定义 2 (EBS 矩阵$\binom{k+m}{k}$)：矩阵的列向量由 m 个 1，k 个 0 组成，且一共有 C_{k+m}^{k}个组成方式，即矩阵一共有 C_{k+m}^{k}个列向量。

3.1.2 密钥分配方案

n 表示节点数目，k 表示分配给每个节点的管理密钥个数，$k+m$ 表示管理密钥总数。

定理 1 当且仅当$\binom{k+m}{k}\geqslant n$时，$\binom{k+m}{k}$中的任意$n$个组合方式均可以构成EBS$(n,k,m)$，进而形成一个管理密钥的分配方案。

定理 2 通过广播最多m个数据包，可以取消并更新任意节点拥有的全部管理密钥，从而驱逐该节点。

3.2 能量模型

本文借鉴文献[9]中的能耗模型。该模型定义无线电路发送距离为dm的l bit消息消耗的能量为：

$$E_{Tx}(l,d)=E_{Tx\text{-}elec}(l,d)+E_{Tx\text{-}amp}(l,d)=\begin{cases}lE_{elec}+l\varepsilon_{fs}d^2, & d<d_0\\ lE_{elec}+l\varepsilon_{mp}d^4, & d\geqslant d_0\end{cases}\tag{1}$$

相应地，接收这些信息消耗的能量为：

$$E_{Rx}(l,d)=E_{Rx\text{-}elec}(l,d)=lE_{elec}\tag{2}$$

数据融合消耗的能量为：

$$E_{Gx}(l,d)=lE_{gather}\tag{3}$$

以上公式中，E_{elec}表示电路发送或接收1bit数据所消耗的能量；$\varepsilon_{fs}d^2$和$\varepsilon_{mp}d^4$为每放大1bit数据放大器消耗的能量；E_{gather}为每1bit数据融合处理消耗的能量；式(4)为将接收到的n个节点发送过来的$n\times l$ bit数据融合成l bit数据所消耗的能量。式(1)中的d_0由下面式子决定：

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}\tag{4}$$

式(1)表明合适的传输距离对于节点节省发送能量有很大帮助。

3.3 新的多跳安全路由协议实现步骤

3.3.1 网络初始化

设n个传感器节点随机部署在一个方形区域内。汇聚节点位于方形区域的右上角，S_i表示第i个节点，则节点集合为$N=\{S_1,S_2,S_3,\cdots,S_n\}$。所有的节点都有唯一的ID标识。在节点部署前，每个节点都有自身的密钥$K_i(i=1,2,\cdots,n)$，且K_i仅与基站共享。

网络节点部署完毕，汇聚节点向所有传感节点广播一个控制信息，各节点根据接收到的信号强度估计与汇聚节点的距离，判断并标识自己所属区域D。这里我们提出了一个“区域”的概念，它不同于簇，是特指以汇聚节点为圆心，以多个不同长度为半径的相邻圆周线之间围成的各个圆环带。对于区域半径的选择是基于能量模型中的距离阈值d_0，具体见上文能量模型。根据仿真场景，文中采用三区制，如图1所示，从汇聚节点由近及远依次划分为A区、B区和C区，分别记为D_1,D_2,D_3。

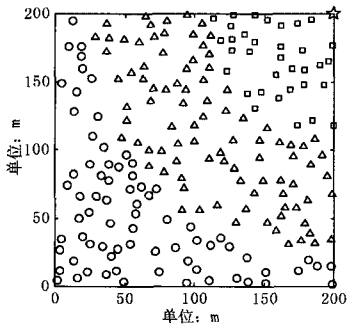

图1 MATLAB随机生成网络节点拓扑图

3.3.2 簇首选举及成簇

在LEACH协议中，每个存活节点会产生一个介于0～1之间的随机数，如果此随机数小于阈值$T(n)$，则此节点为簇首，并发布自己是簇头的公告消息。$T(n)$表示为：

$$T(n)=\begin{cases}\dfrac{P}{1-P[r\bmod(1/P)]}, & n\in G\\ 0, & n\notin G\end{cases}\tag{5}$$

式中，P为簇首节点占网络中所有节点的百分比，r为当前轮数，$r\bmod(1/p)$为这一轮循环中当选过簇头的节点个数，G是本轮循环中未当选簇首的集合。如果节点已成为簇头，则将$T(n)$设为0，这样该节点就不会在本轮再次当选簇头。

簇头选举结束，非簇头节点检测接收到的簇头公告消息，判断自己区域里是否有簇头存在，如果没有，则自动成为簇头，并广播消息。如果有，则分别计算与同区域的所有簇头之间的距离H，最后选择最近的簇头加入。

3.3.3 路径建立

我们以“表格”为单位进行簇间路由建立，这里的“表格”对应于“区域”，同一区域的簇建立一张表格，同一表格中的簇头不进行通信，选择相邻表格中的簇头进行多跳路径传输，这样做的目的是为了减少簇头的负担，以免簇头因负荷太重造成能量的过早流失。同样建立过程用簇头密钥进行加密。

3.3.4 建立动态密钥管理方案

网络分簇结构建立之后，簇内的节点向它们的簇头进行安全初始化，这个过程我们称之为安全注册阶段，即簇内节点广播一个注册报文$\{ID_{S_i},K_i,d_i\}$，报文用S_i的密钥加密，并包含节点S_i的ID和S_i距离基站的距离。簇头节点向基站进行安全注册。首先向基站发送申请报文$\{ID_{CH},ID_{S_i},K_{CH},d_i\}$，$K_{CH}$为基站用于和该簇头共享的密钥，基站生成一个注册种子S_1[7]，由K_{CH}加密发送给簇头，簇头节点在簇内广播S_1，簇内节点根据单向F函数得到注册密钥$K_{S_1}=f(S_1)$，加密后发送注册报文$\{ID_{CH},ID_{S_i},K_i,K_{S_1},d_i\}$给簇头，簇头节点根据$F$函数和种子确认簇内节点的合法身份并记录簇内节点$S_i$的ID和$d$。然后簇头节点利用自己与基站共享的密钥加密注册报文向基站进行安全注册$\{ID_{CH},\{ID_{S_i},d_i\},K_{CH}\}$。

至此，簇头节点已经得到了本簇内所有簇内节点的数目n，根据n选择合适的EBS参数k,m，并保证$\binom{k+m}{k}\geqslant n$。簇头设定好EBS结构之后，在簇内选择密钥生成节点S_k。文献[7]提供了一个密钥生成节点，主要生成管理密钥和共谋恢复密钥，目的是为了将密钥分配和密钥生成两个功能分配给不同的节点完成，以防止簇头被捕获导致整个密钥体系被破解。我们的密钥体系中同样加入这样一个节点，根据簇内节点的剩余能量来选择S_k。选择簇头节点与密钥生成节点之间的通信过程可以描述为：首先簇头向基站发送报文$\{ID_{CH},K_{CH}\}$，基站记录报文并生成种子S_2，并发送报文$\{ID_{CH},K_{CH},K_{S_2}\}$回簇头；然后簇头再发送报文$\{K_{S_2},k\}$给$S_k$，$S_k$生成管理密钥，并发送这些密钥给簇头。

簇头向簇内节点广播EBS矩阵，使得所有簇内节点都知道自己的密钥分配方案。然后簇头将S_k生成的全部管理密钥在簇内广播，最后销毁这些管理密钥。簇内节点收到管理密钥后根据EBS矩阵得到属于自己的k个管理密钥，并销毁EBS矩阵。具体报文形式的过程类似于上述注册与生成管理密钥的过程。

会话密钥主要用于簇内的数据通信，在本协议中，我们为每个簇分配唯一会话密钥，与成簇过程同时进行，簇头用管理密钥加密后在簇内广播，簇内节点解密后得到会话密钥。

3.3.5 节点捕获的恢复机制

本文中的攻击检测由 IDS 入侵检测系统检测，采用基于标志的检测技术：先定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。

(1)簇内节点被捕获

a)簇内被捕获节点数目未构成共谋的情况

根据定理 2，簇头节点广播 m 个数据包更新簇内被捕获节点的 k 个管理密钥。簇头向 S_k 发送更新密钥请求数据包，S_k 收到后生成新的管理密钥 K'_{s_2}，利用现有的 K_{S_2} 和单向函数 F 计算新的 $K'_{s_2}=f(K_{S_2})$，并将这些新的管理密钥打包发送给簇头。由于簇头已经销毁了函数 F，因此不能解密得到新的管理密钥，只能逐一在簇内广播，簇内节点解密得到属于自己的新管理密钥。被捕获的节点由于没有被分配到这 m 个数据包，因此不能解密得到新的密钥，从而被驱逐出了网络。更新会话密钥与此类似。

b) 簇内节点被捕获数达到共谋的情况

文献[7]引出了一个共谋恢复密钥的概念，在不同距离的簇内节点和簇首之间建立唯一的密钥，该密钥被称为共谋恢复密钥 K_r，它由 S_k 产生，且用会话密钥加密后发送给簇首，簇首为 d_i 相同的一组簇内节点转发相应的 K_r，并将这些共谋恢复密钥发送给基站。在本协议中，我们研究出更适用于本协议运行环境的共谋恢复方法。共谋发生后，我们根据 K_r 可以得到被捕获的所有节点的集合，集合中包括了节点的 ID 和 d，由此得到它们所属的“表格”，“表格”中未被捕获的节点恢复被捕获的节点，相当于(1)中的情况。

(2)簇头节点被捕获

基站根据与簇内节点共享的密钥 K_i 来更新被捕获的簇头所在簇内的所有节点的 ID 和 F 函数，并重新选举新簇头，新簇头按照 3.3 节重新建立新的密钥分配方案。

4 实验仿真及性能分析

本文通过 Matlab 仿真的方法对 DZS-LEACH 协议的性能进行分析与评价。我们采用典型的传感器网络分布场景，通过一系列的仿真实验分析在节点被捕获乃至形成共谋后 DZS-LEACH 协议的恢复能力、网络生命周期及总能耗等方面的性能，并与现有的 LEACH 算法进行比较。

4.1 网络分布

假设网络中有 200 个节点，均匀分布在 200m×200m 的正方形区域内，汇聚节点(基站)位于该正方形区域的右上角。仿真实验的参数如表 1 所列。

假设网络运行轮循环周期为 20s，普通节点每 2s 收集一次数据，并转发给簇头，即每周期普通节点发送 10 次数据，簇头节点融合和发送 10 次数据。设定 LEACH 和 DZS-LEACH 的网络节点初始能量、拓扑结构相同，当网络中 80% 的节点无法工作即认为该网络不可用。

根据式(4)可得 d_0 约为 87.7m。由式(1)可知，为达到节能效果，以汇聚节点为圆心的 A 区半径值应小于 d_0。为在实际仿真时方便计算，取 A 区半径为 90m。B 区要基本保证在一般情况下相邻区域的簇头间距在 d_0 范围以内，所以取 180m。C 区半径考虑覆盖整个网络，所以取 270m。网络中节点被捕获如图 2 所示，其中菱形为被捕获的节点，取而代之的是恶意节点。网络被分为三个区域，如图 1 所示。

表 1 仿真参数

参数类型	参数值
传感器个数	200
传感器坐标范围(单位:m)	(0,0) ～ (200,200)
数据包长度	4000 bit
控制包长度	100 bit
电子发射消耗能量 E_{Tx}	50 nJ/bit
电子接收消耗能量 E_{Rx}	50 nJ/bit
近距离发射放大器参数 ε_{fs}	10 pJ/bit/m^2
远距离发射放大器参数 ϵ_{mp}	0.0013 pJ/bit/m^4
数据整合能量 E_{DA}	5 nJ/bit/signal
簇的最佳个数 k_{opt}	5 %
传感器初始能量 E_0	1J
A 区半径	90m
B 区半径	180m
C 区半径	270m

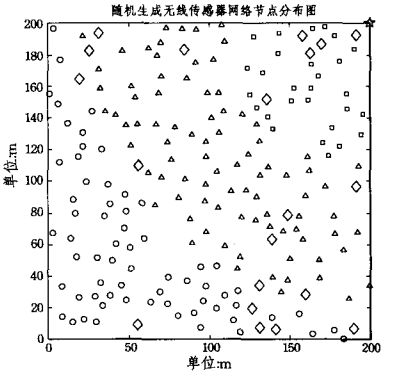

图 2 网络中节点被捕获时的分布图

仿真主要针对网络被攻击的情况下，即恶意节点捕获正常节点，并获得其中的密钥管理方案，取而代之。在这种情况下，我们分析 DZS-LEACH 的恢复能力，并与 LEACH 协议相比，分析丢包率、网络寿命及网络能耗。

4.2 DZS-LEACH 协议的网络恢复能力

网络中节点被恶意节点捕获，恶意节点通过获知其中的密钥管理方案来获得网络中相关密钥信息及消息报文，此时，DZS-LEACH 协议的动态密钥管理方案会使得当前网络重新分配节点并更新网络中的密钥管理方案，而 LEACH 协议由于没有相应的恢复功能，导致节点消息被捕获从而造成能量的浪费，节点过早死亡。

图 3 和图 4 分别为两种协议在网络运行 200 轮后死亡节点分布图，其中，黑色实心点代表死亡的节点。

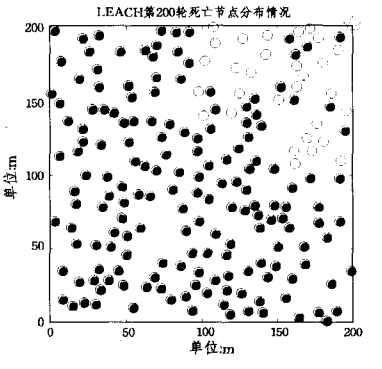

图 3 LEACH200 轮后死亡节点分布情况

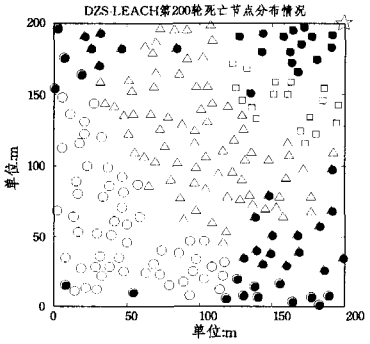

图 4　DZS-LEACH 死亡节点分布情况

以上两图比较可以看出，节点被捕获后，LEACH 协议的大部分节点都已经死亡，而改进后的协议中加入了动态密钥管理方案，协议在受到攻击之后可以自动更新密钥管理方案，从而减少了节点能量的浪费，在抵御攻击的程度上有显著的提高。网络运行 200 轮后，改进后的协议比 LEACH 协议的死亡节点大大减少，进一步证明了抵御攻击的强能力。

4.3　网络的生存时间

无线传感器网络工作时，能量的消耗主要来自两个方面：计算和通信。而射频通信消耗的能量占主要部分。层簇式路由协议虽然相比其它拓扑结构的路由协议节约能量，但容易造成能量消耗不均衡，降低网络的存活时间。本文引入分区自治思想，建立表格采用动态密钥管理方案，不仅能有效进行节点被捕获后网络的恢复，而且能提高网络的存活时间，更能很好地保持能耗均衡。图 5 和图 6 分别是两种协议在各轮次的存活节点数目和网络总能耗曲线图。

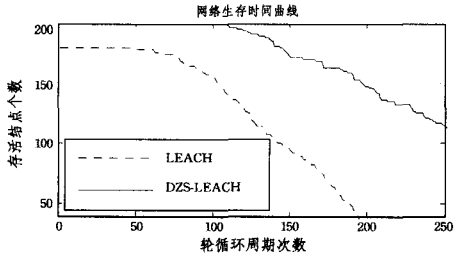

图 5　网络的生存时间

图 5 中，DZS-LEACH 分区自治使得簇头均匀分布，簇间多跳使得能耗均匀。另外，在节点被捕获的网络环境下，网络中的 IDS 系统检测功能自动检测出异常节点，由于 LEACH 协议的单跳模式没有安全机制，网络的起始阶段就有节点被 IDS 隔离。而 DZS-LEACH 协议中我们加入了动态安全机制使得在循环中节点不受攻击的挟持，网络重新分配密钥方案使得节点的存活率大大提高，从而节约了网络能耗。曲线的走势说明 DZS-LEACH 的有效存活期比 LEACH 更加集中，网络出现大面积监控盲区的时间短，这较直观地反映在了表 2 中。

表 2　两种协议的节点死亡状况统计

协议	发生第一个节点死亡	20%节点死亡	50%节点死亡	80%节点死亡
LEACH（仿真轮数）	0	2	144	191
DZS-LEACH（仿真轮数）	116	141	266	317

4.4　网络的总能耗

图 6 是网络总能耗的累计曲线图，随着轮次增加，DZS-LEACH 曲线渐渐靠近 LEACH 曲线。这是由于 DZS-LEACH 协议增加了路由控制信息以及动态安全机制，在网络生存的后期，各节点能量所剩无几，这些控制信息会明显增加能耗，加快节点死亡。

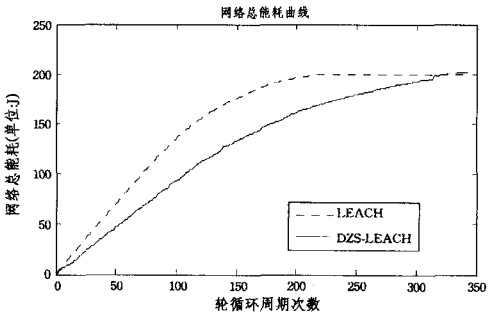

图 6　网络的总能耗

从图 6 可以看出，DZS-LEACH 总能耗变化率比 LEACH 变化小，说明 DZS-LEACH 每轮能耗更加均衡。

表 3 为仿真环境下汇聚节点（基站）收到的数据包数目的统计。采用 LEACH 协议，汇聚节点收到的数据包数远远少于 DZS-LEACH 协议。这是因为，LEACH 协议簇头直接跟汇聚节点通信的单跳通信模式使得簇头节点在被捕获后，密钥系统也被窃取，产生路径的误导，数据包无法及时有效地被传送，从而造成数据包的丢失，改进后的路由协议 DZS-LEACH 中加入了动态密钥管理方案，使得节点在被捕获后，系统自动添加节点，并重新分配密钥方案，没有分配到密钥的攻击节点被自动驱逐出网络，保证了报文能及时传送，正确到达汇聚节点。

表 3　基站收到的数据包和控制信息统计

协议名称	数据包数
LEACH	274930
DZS-LEACH	452260

结束语　本文在 LEACH 协议的研究基础上提出了一种新的多跳跨区安全路由协议，主要目的是消除节点被捕获乃至形成共谋的情况下 LEACH 协议存在的安全隐患。在能耗问题上，我们采用跨区路由思想，在加入动态安全机制的同时也均衡整个网络的能量消耗。实验表明，DZS-LEACH 协议能有效抵御恶意节点的攻击，显著延长网络的存活时间，均匀死亡节点的分布，提高能量利用率。

参 考 文 献

[1] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. New York, NY, USA, 2002: 41-47

[2] Anjum F, Mouchtaris P. Security for Wireless Ad-hoc Networks [M]. John Wiley Publications, 2007

[3] 孙利民，李建中，陈渝，等. 无线传感器网络[M]. 北京：清华大学出版社，2006

[4] Heinzelman W R, Chandrakasan A P, et al. Energy efficient communication protocol for wireless microsensor networks [C]// Proceedings of Hawaii International Conference on System Sciences. Hawaii, USA, 2000: 3005-3014

（下转第 393 页）

5 应用

在组网中，出现单通的情况常见于互相用双绞线（或光纤）连接的端口。如图1所示，从设备B上的TX端口至设备A上RX方向的链路出现了故障，导致设备B只能收报文不能发报文的情况，设备B与设备A之间的链路就是单向链路。

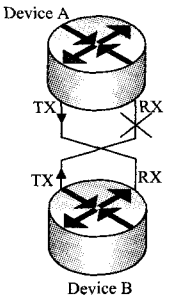

图1

UDLD检测单向链路的过程如下。

5.1 状况一：Device A与Device B双向连通（见图2）

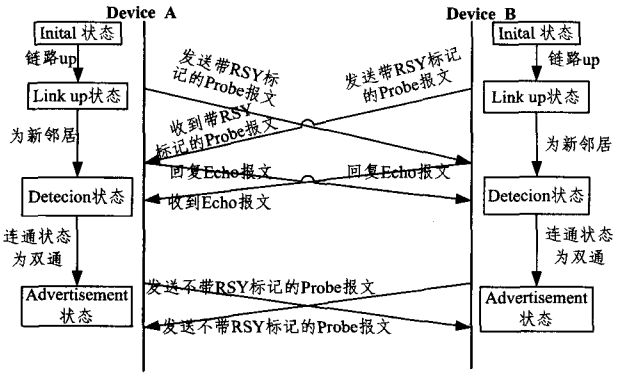

图2 UDLD工作过程

5.2 Device A先启动、Device B后启动，出现单通情况，Device A只能收不能发（见图3）

5.3 Device A与Device B在双通后，出现单通情况，Device A只能收不能发（见图4）

结束语 网络是最怕环路，当在一个中大型的网络中出现环路特别是Layer 2环路，所产生的广播风暴会在瞬间十几秒内淹没整个网络。单向链路故障就会导致STP环路等，UDLD协议的诞生正是为了避免这个问题，UDLD可以检测出设备之间存在的单通链路，并及时地关闭相应的端口，从而保证网络的正常运行。

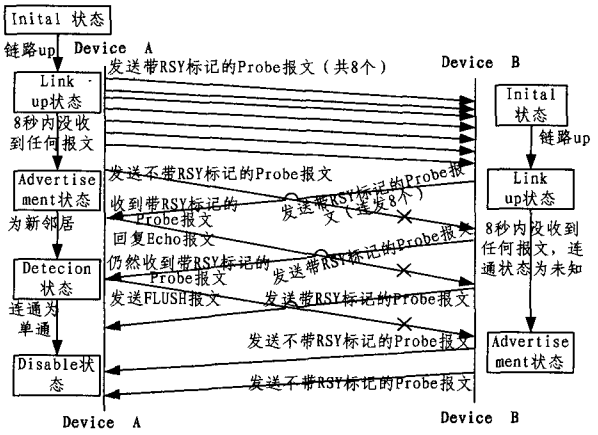

图3 UDLD工作过程

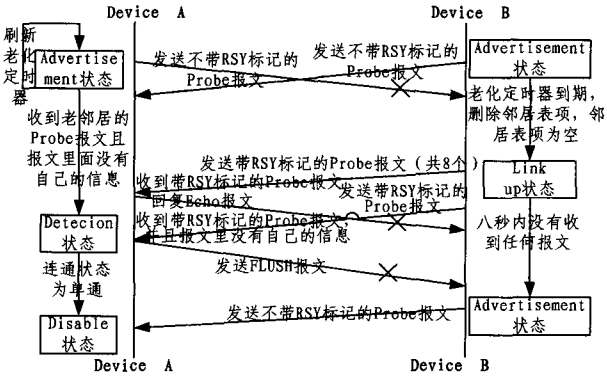

图4 UDLD工作过程

参考文献

[1] IEEE 802.1D-2004 Standard - - Media access control (MAC) Bridges

[2] IEEE 802.3-2002 IEEE Standard — Local and metropolitan area networks Specific requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications

[3] Katz D, Ward D. Bidirectional Forwarding Detection[Z]. Work in Progress, March 2008

[4] IETF STD 62, RFC 5171, V Cisco Systems UniDirectional Link Detection (UDLD) Protocol

（上接第363页）

[5] Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures [C] // Proceedings of IEEE International Workshop on Sensor Network Protocols and applications. Anchorage, USA, 2003: 113-127

[6] Zhang Q H, Wang P, Douglas S. Defending against Sybil Attacks in Sensor Networks [C] // Proceedings of IEEE International Conference on Distributed Computing Systems Workshops. Columbus, USA, June 2005: 185-191

[7] 孔繁瑞，李春文，等. 无线传感器网络动态密钥管理方法[J]. 软件学报，2010，21(7)：1679-1691

[8] Eltoweissy M, Heydari H, Morales L, et al. Combinatorial Optimization of Group Key Management[J]. Journal of Network and Systems Management, 2004, 12(1): 33-50

[9] Heinzelman W B, Chandrakasan A P, et al. An application specific protocol architecture for wireless microsensor networks [J]. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670