无线传感器网络低能耗树状路由安全性能

秦丹阳,贾爽,王尔馥,丁树春,甄佳奇,赵冰

黑龙江大学电子工程学院,哈尔滨 150080

摘要 安全可靠的无线传感器网络是现代通信系统的重要分支,是面向泛在通信的重要技术支撑。然而,大量的网络攻击导致数据安全受到威胁,严重影响网络可靠性,从而使无线传感器网络的使用价值大大降低。针对无线传感器网络的安全性问题,提出了以高效节能为前提的低能耗树状路由协议的安全模型LCTR模型。该模型利用报文鉴别码和数字签名技术实现鉴权和数据整合。通过采用常用报文鉴别码和数字签名技术作为参考对LCTR模型进行性能分析,仿真结果表明,LCTR模型下信息安全传输成功率最多可提高23%,网络生存时间最多可提高5%。

关键词 数据整合;能量使用率;鉴权;无线传感器网络

中图分类号 TN914.5 **文献标志码** A **doi** 10.3981/j.issn.1000-7857.2015.13.013

Low-energy consumption tree routing security for wireless sensor networks

QIN Danyang, JIA Shuang, WANG Erfu, DING Shuchun, ZHEN Jiaqi, ZHAO Bing

School of Electronics Engineering, Heilongjiang University, Harbin 150080, China

Abstract Safe and reliable wireless sensor network (WSN) is an important branch of modern communication systems, and is an important technical support for ubiquitous communication. However, a large number of network attacks will threaten data security, which will seriously affect network reliability and greatly reduce the use value of WSN. This paper proposes a security model for low-energy consumption tree routing protocols (LCTR), which achieves authentication and data integration using message authentication code (MAC) and digital signature (DS) techniques. Some common MACs and DSs have been taken as the reference to analyze the performance of LCTR. Simulating results show that with the model of LCTR, the safe transmitting rate of information is increased by 23% at most, and the network lifetime is increased by 5% at most.

Keywords data integration; energy efficiency; authentication; wireless sensor network

无线传感器网络是由大量静止或移动的传感器以自组织和多跳的方式构成的无线网络,协作地探测、处理和传输网络覆盖区域内感知对象的监测信息,并报告给用户[1,2]。无线传感器网络融合了逻辑上的信息世界与客观上的物理世界,改变了人类与自然界间的沟通方式。人们可以通过传感器网络来感知客观世界,这不仅提高了网络的应用性,也使得人们能更好地去感知认识世界。

随着无线传感器网络(wireless sensor networks,WSN)逐步应用于军事和商业领域,其安全性变得越来越重要。由于WSN特殊的应用环境,其安全问题尤为突出。关于WSN的网络攻击问题研究已取得很大进展,但往往是以损耗能量为代价提高网络的安全[3]。

WSN节点分布众多,并且需要进行监测、数据处理等活动,而节点一般用电池供电,可使用的电量非常有限,并且对于有成千上万节点的WSN来说,更换电池是不可能的,但要求WSN的生存时间长达数月甚至数年[4]。针对WSN的能耗

收稿日期:2015-03-18;修回日期:2015-05-18

基金项目:黑龙江省教育厅科学研究项目(12531480)

作者简介:秦丹阳,副教授,研究方向为无线泛在感知与多跳路由技术,电子信箱:qindanyang@hlju.edu.cn

引用格式:秦丹阳, 贾爽, 王尔馥, 等. 无线传感器网络低能耗树状路由安全性能[J]. 科技导报, 2015, 33(13): 76-83.

问题,建立低能耗树状路由协议的安全模型(security model for low-energy consumption tree routing,LCTR),用以提高网络平均生存时间,从而确保WSN的安全性。

1　树状路由协议概述

基于树状路由协议(tree routing,TR)是针对轻型网络设计的能量有效型路由协议[5]。制定TR协议的目的是减少冗余信息在节点中的传输,消除在路径搜索和表格更新过程中对能量产生的总开销。基于TR协议的路由选择过程主要取决于网络节点中树的结构,并由树的深度和子树个数两个参量进行控制。每构造一个树形结构就会为节点分配一个ID地址,分配的ID地址将会用来作为网络节点的逻辑地址。不同的控制报文用来控制树的结构进程,报文结构的变化取决于系统的规格。但一般而言将会有3种主要报文可以适用于任意一种TR协议。第1种为联合报文,即无论TR协议是否涉及这个报文,都要将附近的所有节点信息发送给发送者即父节点,让其接受子节点。第2种为联合回复,它会给联合报文发送一个回答,使父节点与子节点相结合。第3种为ID报文,即由父节点发送报文结合子节点的ID逻辑地址。一般来说,节点联合过程开始于树根即锚节点或者网络协调器,通过广播联合报文给邻居节点。发送者和接收者节点联合报文过程如图1所示。

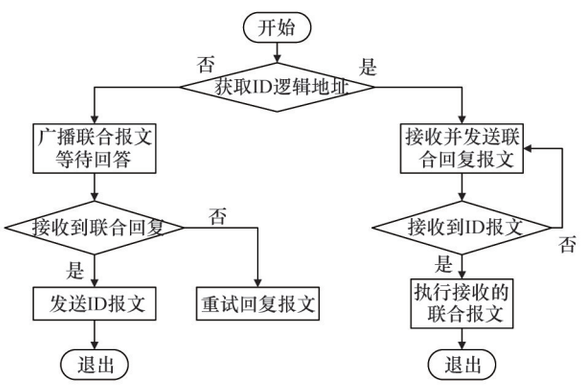


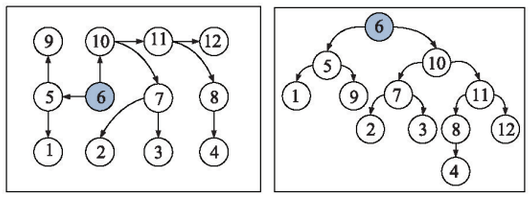
图1　节点联合过程流程图

Fig.1　Flow chart of node junction

图2给出两个逻辑树的典型结构。从图2可以比较清楚地看出在网络节点中逻辑ID的位置。

然而,TR协议中也存在一个弊端就是TR协议的路径过长、发送节点过深,使得到达根部的路径过长。此外,在TR协议中节点失效也可能是一个重要的威胁,因为它可能会引起节点分离。

为了弥补TR协议存在的缺陷,在原有协议基础上建立增强树的路由协议和改进树的路由协议,利用构造邻居节点表格寻找到达根部的最短路径的方式提高TR协议的效率。而针对于锚节点失效问题,通过建立一个容错路由协议便可以有效解决。



(a) 网络节点中的逻辑树　　(b) 树的逻辑观察

图2　逻辑树形结构举例

Fig. 2　Examples of logical tree structure

2　树状路由协议的安全模型

网络数据传输离不开路由协议,路由协议是其组网的基础。路由协议作为影响网络性能的一个重要因素,是确保WSN网络正常运行的关键。这里将设计一种基于树的路由协议的安全参考模型,用以抵御网络中常见的各种攻击,确保在网络节点中建立准确安全的拓扑模型用以保证数据的正确传输。

2.1　树状路由协议

树状路由协议控制消息用于管理节点联合与分离过程,当安全技术不被采用时,攻击者可以利用这些报文侵袭拓扑构造并且在节点中交换错误的拓扑信息。表1列举了可能出现的路由协议攻击,以及这些攻击可能产生的一些影响[6]。

表1　树状路由协议攻击

Table 1　Tree routing protocol attacks

路由选择过程	攻击	影响
节点联合与分离	1) 发送大量伪控制报文; 2) 窃听网络中的控制报文; 3) 修改网络控制报文内容	a) 在接收、加工和存储伪报文的过程中超出了传感器能量范畴; b) 在邻居节点制表中加入了敌对节点; c) 敌对节点获取网络拓扑结构; d) 传感器在制表中存储错误的拓扑信息; e) 传感器网络接收错误回复
数据传输	1) 发送伪数据包; 2) 窃听网络数据包; 3) 修改数据包内容; 4) 终止数据包	a) 发送鉴定数据时引起错误警报; b) 在转发、加工和存储伪报文的过程中超出了传感器能量范畴; c) 在非法路径中使用并读取网络数据; d) 传感器网络接收错误回复; e) 修改鉴定数据时引起错误警报; f) 阻碍重要数据在锚节点中被接收和加工

2.2 WSN的安全需求及方法

解决树的路由攻击的最好方法是在路由选择中采用安全防护技术,减少路由选择对网络产生的攻击。建立一个基于安全的拓扑模型,确保WSN在基于树的路由协议中可抵御常见的攻击[7]。并且要确保在构建阶段所参与的节点是WSN的节点而非敌对节点,为此需要实现对节点的鉴权。同时要确保数据的完整性及准确性即正确的拓扑信息。因此设计的LCTR模型需要实现鉴权和数据整合。

为实现鉴权和数据整合需要用到报文鉴别码(message authentication code,MAC)和数字签名技术(digital signature,DS)。MAC是基于哈希函数和分组密码建立的,DS利用公钥密码学签署要发送的报文。通过对MAC和DS的能耗评估,选出最优方案加入到模型中,在报文鉴别码中常用安全技术CBC-MAC、XMAC、CMAC,其处理过程基于分组密码完成的,而HMAC是基于哈希函数完成的。数字签名技术用到的安全技术有两种,其中RSA的处理过程是基于PKC进行的,ECDSA的处理过程是基于椭圆曲线密码学的PKC来完成的。

在基于MAC分组加密中,根据所要达到的安全等级使用不同的加密算法,并在表2中列出。对表2分析可以看出,密钥长度越长安全等级越好。

表2 各分组密码的安全强度

Table 2 Safety degree of different block keys

分组密钥方案	码组长度/bit	密钥长度/bit	安全等级
AES	128	128	*Rounds*=10
RC5	32	128	*Rounds*≥16
Skipjack	64	80	*Rounds*≤32
XXTEA	64	128	*Rounds*≥6

AES(advanced encryption standard)是美国联邦政府采用的一种分组加密标准。AES加密分组数据长度必须为128 bit,密钥长度可以为128、192、256 bit,AES加密有很多轮的重复和变换。RC5分组密码算法是参数可变的分组密码算法,3个可变的参数是:分组大小、密钥大小和加密轮数[8]。在此算法中使用了异或、加和循环3种运算。Skipjack算法是一种利用80 bit密码变量的64 bit电子密本。XXTEA分组加密算法使用128位的密钥,对32的倍数的分组信息进行操作,并保证每一轮加密都不相同,由于它具有低能耗的性能,因此十分适用于资源有限的环境。

CBC-MAC技术在基于分组加密算法上用来评估MAC的值。在CBC模式中利用分组密码算法对报文进行加密,从而创造一系列的分组。在最后的加密分组中得到的MAC值将会被写入到报文中。在这个过程中会用到两种不同的密钥,其中一种密钥用于分组加密算法,即在CBC模式中使用;另外一种密钥用于评估MAC的值。XMAC技术是在CBC-MAC技术的基础上提出的,可以用来操作密钥,同时支持可变长度的报文。CMAC技术也是在CBC-MAC技术的基础上提出的,并且它在评估过程中只需要一个密钥。值得注意的是,HMAC并不是基于分组密码对MAC的值进行估算,而是基于迭代加密哈希函数如MD5哈希函数[9],这是因为迭代加密哈希函数可以在固定大小的分组中对报文进行划分,压缩函数对它们进行迭代。

RSA算法和ECDSA算法都属于公开密钥密码体制,并且公开密钥密码体制又分为加密密钥和公开密钥两种形式[10]。当公共密钥核实签名信息时,公开密钥可以对报文进行签名。加密密钥安全程度虽高于公开密钥,但它更复杂一些。此外,它还需要确认公共密钥的准确性。

2.3 树状路由协议的安全模型

综上所述,需要设计低能耗树状路由协议的安全模型LCTR,用来解决无线传感器网络的能量损耗和安全问题。在设计安全模型过程中需要用到鉴权与数据整合技术,并要求在应用安全方案前,所有节点的密钥需达成一致。所以,设计安全模型时要考虑以下两点:首先所有用到的密钥需要预装载到网络传感器中;其次所有的传感器都要参与到安全实验过程中[11]。

所设计的安全模型由两个模块组成。第1个模块在节点联合过程中使用,目的是确保安全的拓扑模型,并保证节点中拓扑信息的准确性。第2个模块是在所有节点都被连接到网络的树中,并准备传送数据时使用。这个模型的目的是在可能出现的各种攻击中确保传输数据的准确性[12]。

对于模块1,在构造所需树形结构时,需要传输的控制报文将会被签名或者被嵌入到MAC中。当传感器接收到控制报文时,需核实报文是否由鉴权节点发送。如果发送者未被鉴权,所接受的报文将被忽略,否则在所构建的拓扑模型中的敌对节点将会被误当作正常节点。此外,接收者需要核实所接收的报文是否被修改,确保所建立拓扑模型的可靠性。

在模块2中添加模糊推理系统,此系统在传输数据包过程中判断是否需要采用安全保护技术。模块2是基于Mamdani模糊推理系统,Mamdani型的模糊推理方法是最常见的算法,最先将模糊集合的理论用于控制系统。添加模糊推理系统是基于3个因素考虑:传感器能耗、来自关联程序的时间和数据状态。模糊推理系统见图3。

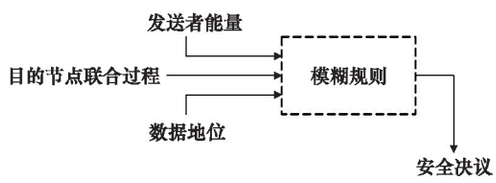


图3 模糊推理系统结构

Fig. 3 Structure of fuzzy inference

Mamdani模糊推理系统有3个输入端,分别为发送者能

量(sender energy,SE)、目的节点联合过程(time since last nodes association process,TLA)和数据地位(date status,DST)。与其他参数相比,SE有较高的优先级,这意味着当SE较低时不必采用安全保证,并且不需要考虑其他两个参量情况。此外,当数据低于安全标准时也不需要在数据包中采用安全保证。

模糊推理系统有一个输出端,其作用主要是用来判断在当前数据包中是否需要采用安全技术。模糊推理系统的隶属度函数为梯形函数或三角函数。梯形函数的4个顶点分别为$(a, 0)$、$(b, 1)$、$(c, 1)$和$(d, 0)$,三角函数的3个顶点分别为$(a, 0)$、$(b, 1)$和$(c, 0)$。并且公式表示分别为式(1)和式(2)。

$$\mu(x,a,b,c,d)=\begin{cases}0 & x<a,x>d\\ \dfrac{x-a}{b-a} & a\leqslant x\leqslant b\\ 1 & b<x<c\\ \dfrac{d-x}{d-c} & c\leqslant x\leqslant d\end{cases} \tag{1}$$

$$\mu(x,a,b,c)=\begin{cases}\dfrac{x-a}{b-a} & a\leqslant x\leqslant b\\ 0 & x<a,x>c\\ \dfrac{c-x}{c-b} & b\leqslant x\leqslant c\end{cases} \tag{2}$$

每一个隶属度函数需要调整的最佳值是通过表3表示。并且a、b、c和d的值并不是固定不变的,它们根据当前应用情况或者WSN所提供的服务信息情况进行修改。

表3　a、b、c和d在每一个模糊推理系统中的参数值

Table 3　Parameter values of a, b, c and d in each fuzzy inference system

模糊变量	隶属函数	函数类型	隶属函数参数智能
SE	低	梯形函数	a=0、b=0、c=0.2、d=0.4,x=当前SE值
	中	三角函数	a=0.3、b=0.5、c=0.7,x=当前SE值
	高	梯形函数	a=0.6、b=0.8、c=1、d=1,x=当前SE值
TLA	短	梯形函数	a=0、b=0、c=0.2、d=0.4,x=当前TLA值
	中	三角函数	a=0.3、b=0.5、c=0.7,x=当前TLA值
	长	梯形函数	a=0.6、b=0.8、c=1、d=1,x=当前TLA值
DST	较低鉴定	三角函数	a=0、b=0、c=0.3、d=0.6,x=当前DST值
	较高鉴定	梯形函数	a=0.4、b=0.8、c=1、d=1,x=当前DST值
决议(输出端)	不采用安全保证	梯形函数	a=0、b=0、c=0.3、d=0.6,x=当前输出端的值
	采用安全保证	梯形函数	a=0.4、b=0.8、c=1、d=1,x=当前输出端的值

3　LCTR模型开销分析

主要分析该安全模型构架的能量开销。在此安全模型中需要采用安全技术,这个过程会损耗传感器的一部分能量。

3.1　通信开销分析

在基于树的路由协议中传感器在执行发送和接收报文时会产生大量的能量消耗,并且大部分能量消耗主要产生在通信运营过程中。表4列出了在方程式中出现的所有缩写及所代表的含义。

表4　缩写列表

Table 4　Abbreviations

缩写	含义
N	节点数
k	报文大小,以比特为单位
d	发送端到接收端之间的距离
n	节点i的邻居节点数
TCC	树形结构通信开销
BC	分组开销,取决于所使用的安全机构
BS	分组大小,取决于所使用的安全机构
AS_i	第i个联合报文的大小
ARS_i	第i个联合回复报文的大小
IDS_i	第i个ID报文的大小

测量通信开销时需了解报文大小和发送距离。根据式(3)和式(4)利用通信代价中发送和接收k比特报文,可计算出到达目标地点的距离d。

$$Sending\_Cost(k,d)=Eelec\cdot k+Eamp\cdot kd^2 \tag{3}$$

$$Receiving\_Cost(k,d)=Eelec\cdot k \tag{4}$$

在网络节点中建立一个树的路由模型需要测量通信开销,需要知道在该阶段中发送和接收报文的总数。通过对接收端和发送端联合过程的推断,所需发送报文数量为$2N+\sum_{i=1}^{n}n_i$,接收端报文数量为$N+2\times\sum_{i=1}^{n}n_i$。通信电源能量可以根据式(5)计算得到

$$\begin{aligned}TCC=&Sending\_Cost(k,d)\cdot\left(2N+\sum_{i=1}^{n}n_i\right)\\&+Receiving\_Cost(k)\cdot\left(N+2\times\sum_{i=1}^{n}n_i\right)\end{aligned} \tag{5}$$

3.2　处理成本开销分析

当采用安全技术时将会消耗传感器的部分能量,关于在启用一个控制报文所需能耗可根据式(6)计算得出。

$$MessageCost=NumofBlocks\cdot BC, \tag{6}$$

式中,$NumofBlocks$为节点数,且满足$NumofBlocks=\left[\dfrac{k}{BS}\right]$。

通过了解在联合过程中的网络节点之间交换的报文数,可计算出处理这些报文所需要的能量开销。由式(7)和式(8)分别计算出在发送和接收报文中所需的处理成本开销。

安全模型LCTR模型中,节点在联合过程中处理发送报文所消耗能量SC的最大值为

$$SC=\sum_{i=1}^{n}\left(\left\lceil AS_i/BS\right\rceil+\left\lceil IDS_i/BS\right\rceil\right)+\sum_{i=1}^{n}\left(n_i\left\lceil ARS_i/BS\right\rceil\right)BC \quad (7)$$

式中,发送的联合报文数为N,基于此可以推出所有联合报文所需分组数为$\sum_{i=1}^{n}n_i\left(\left\lceil AS_i/BS\right\rceil\right)$。同理,可以推出联合回复报文和ID报文所需分组数分别为$\sum_{i=1}^{n}n_i\left(n_i+\left\lceil ARS_i/BS\right\rceil\right)$和$\sum_{i=1}^{n}n_i\left(\left\lceil IDS_i/BS\right\rceil\right)$。

安全模型LCTR模型中,节点在联合过程中处理接收报文所消耗能量的最大值RC为

$$RC=\sum_{i=1}^{n}\left(\left\lceil IDS_i/BS\right\rceil\right)+\sum_{i=1}^{n}\left(n_i\left\lceil AS_i/BS\right\rceil\left\lceil ARS_i/BS\right\rceil\right)BC。 \quad (8)$$

式中,发送的联合报文数为$\sum_{i=1}^{n}n_i$,基于此可以推出所有联合报文所需分组数为$\sum_{i=1}^{n}n_i\left(\left\lceil AS_i/BS\right\rceil\right)$。同理,可以推出联合回复报文和ID报文所需分组数分别为$\sum_{i=1}^{n}\left(n_i\left\lceil ARS_i/BS\right\rceil\right)$和$\sum_{i=1}^{n}\left\lceil IDS_i/BS\right\rceil$。

4 安全模型评估与仿真结果

对于所构造安全模型性能的仿真将采用QualNet网络模拟器实现。

4.1 安全技术评估及能量开销分析

仿真过程中所需参数如表5列出。各种安全技术能量开销评估见表6~表8[13]。

表5 仿真参数

Table 5 Simulation parameters

仿真参数	参数值
网络规模	多达30个节点
移动性	无
接收器数量	1
地形面积/m^2	1500×1500
无线传感器射程/m	250
初始能量/J	1000

表6 分组密码技术能量开销评估

Table 6 Evaluation on energy cost for different block keys

单位:μJ

安全技术	MicaZ	TelosB
AES	146.6	425.49
bRC5	137.92	58.26
Skipjack	27.58	13.3
XXTEA	124.64	38.7

表7 MAC技术能量开销评估

Table 7 Evaluation on energy cost for different MACs

单位:μJ

安全技术	MicaZ				TelosB			
	AES	RC5	Skipjack	XXTEA	AES	RC5	Skipjack	XXTEA
CBC-MAC	160.39	178.78	123.61	172.14	112.2	98.45	75.97	88.97
XMAC	264.59	282.98	227.81	276.34	176.44	162.69	140.21	152.91
XMACHMAC	387.19	405.58	350.41	398.94	250.39	236.64	214.16	226.86
HMAC	278.39	278.39	278.39	278.39	57.37	57.37	57.37	57.37

表8 数字签名技术能量开销评估

Table 8 Evaluation on energy cost for different DSs

单位:mJ

安全技术	MicaZ		TelosB	
	签名	核实	签名	核实
RSA-1024	359.87	14.05	68.97	2.7
ECDSA-160	26.96	53.42	6.26	12.41

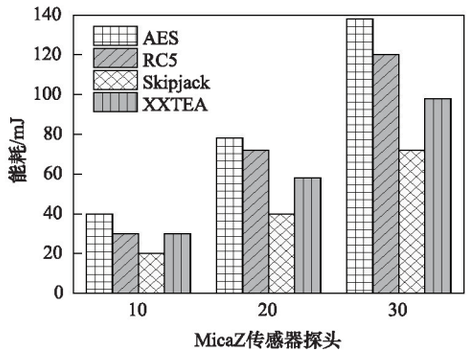
在TR协议中采用不同MAC算法时,所得功率效率不同。基于MAC技术的密码性能主要取决于分组密码,可用来计算MAC值。这里将分别在MicaZ传感器探头和TelosB传感器探头中采用安全技术。MicaZ和TelosB是两个熟知的传感器探头,它们之间最大的区别是记忆空间大小和能量有效利用率不同。其中,MicaZ传感器探头的RAM为4 KB,ROM为128 KB;TelosB传感器探头的RAM为10 KB,ROM为48 KB。依据能量有效率原则TelosB能量有效率要高于MicaZ。

4.1.1 分组密码评估

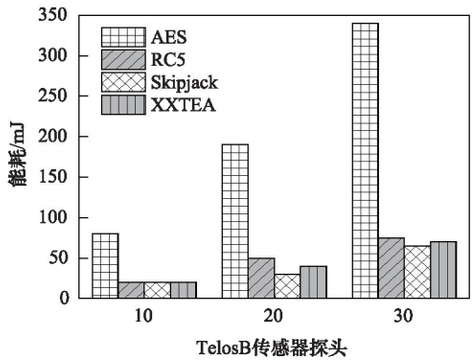
在基于AES、RC5、Skipjack加密算法和XXTEA在传感器探头中进行评估研究。在MicaZ传感器探头和TelosB传感器探头中,每个分组密码进行加密、解密所产生的能量消耗的仿真结果分别如图4(a)、(b)所示。

评估主要在TR协议中进行,并根据加密算法的特点采用符合它们自身特点的最佳方案进行评估,测量在不同的网络规模中所产生的能量消耗。根据图4仿真结果可看出,能量消耗随着节点数的增加而增加。此外,在TelosB传感器探头中除AES加密算法外,分组密码方案相比较而言更节省能

量开销。无论是在MicaZ传感器探头中,还是在TelosB传感器探头中,AES加密算法都会产生较大能量消耗,而Skipjack加密算法相比较而言更节省能量。



(a) MicaZ传感器探头仿真结果



(b) TelosB传感器探头仿真结果

图4　分组密码中不同的网络规格所产生的能耗

Fig. 4　Energy consumption from different network specifications in block cipher

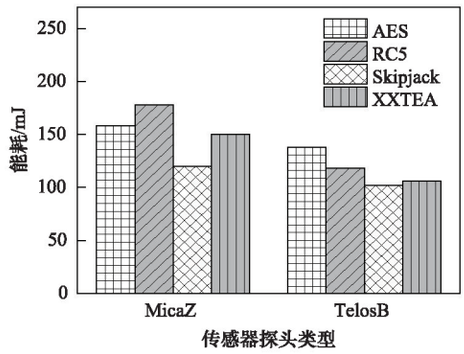
4.1.2　MAC技术评估

主要针对4种MAC技术进行评估,即CBC-MAC、XMAC、CMAC和HMAC技术。并且前3项安全技术是基于分组密码,并对MAC的参数值进行估算。在TR协议中分别采用这4个安全算法,通过对其分组密码的研究来评估这些算法的安全性能。并通过图5将CBC-MAC、XMAC和CMAC算法的仿真结果表示出来。

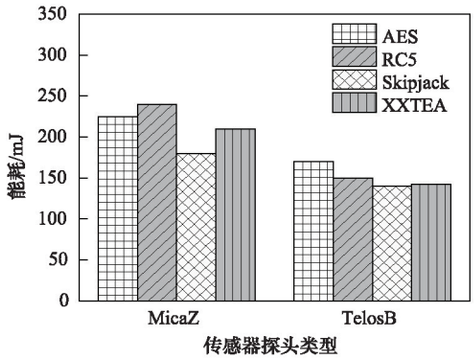
由图5的仿真结果可以看出,采用CBC-MAC方法时,不论采用MicaZ还是TelosB探头,能耗相比于XMAC和CMAC均较低,因此,CBC-MAC的能量利用率更高。由于HMAC算法需要通过哈希函数对MAC的值进行估算,因此难以应用于分组密码中。分别采用MicaZ和TelosB传感器探头利用HMAC算法所产生的能量消耗情况如图6所示。

4.1.3　数字签名技术评估

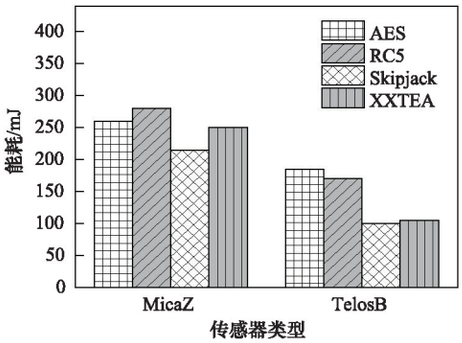
对无线传感器网络中采用的基于PKC的两种WSN数字签名技术RSA与ECDSA进行性能评价,仿真结果见图7。



(a) CBC-MAC算法



(b) XMAC算法



(c) CMAC算法

图5　使用不同分组密码的能量损耗

Fig. 5　Energy consumption of using different block cipher

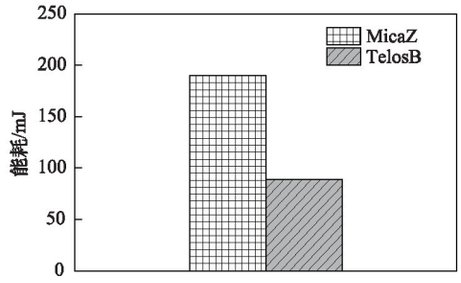


图6　HMAC算法中不同传感器探头的能量损耗

Fig. 6　Energy consumption of different sensor probe in HMAC algorithm

由图7可见,无论采用MicaZ传感器探头还是TelosB传感器探头,由于采用了椭圆曲线密码体制(elliptic curve cryptography,ECC),ECDSA数字签名技术的能量使用效率都要高于RSA数字签名技术。此外,与其他基于PKC方案相比,ECDSA结构简单,更适用于无线传感器网络的LCTR模型。

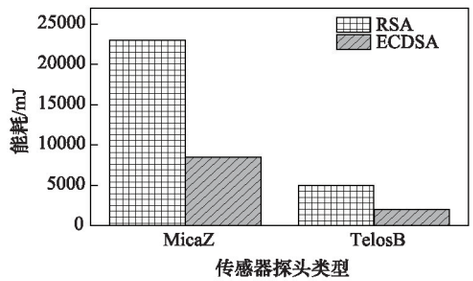


图7 DS方案中不同传感器探头的能量损耗

Fig. 7 Energy consumption of different sensor probe in DS scheme

4.2 LCTR模型评估及仿真结果

主要针对于LCTR模型的两个设计模块进行评估,选出最优方案。首先对模块1进行评估,即对树形结构进行评估,分别在传感器探头中使用MAC技术和DS技术,仿真结果如图8所示。

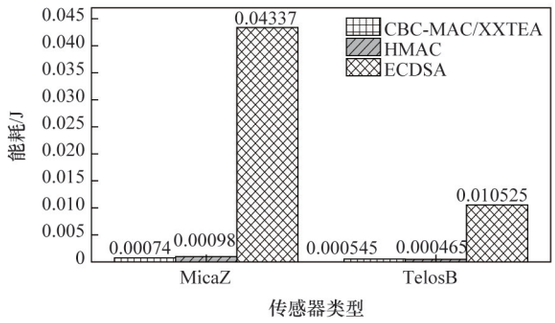
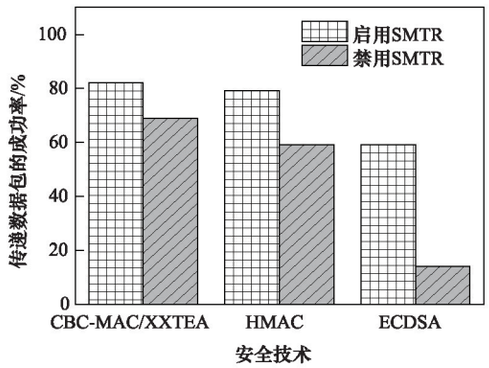


图8 模块1中MAC技术和DS技术在不同传感器探头中的能量消耗

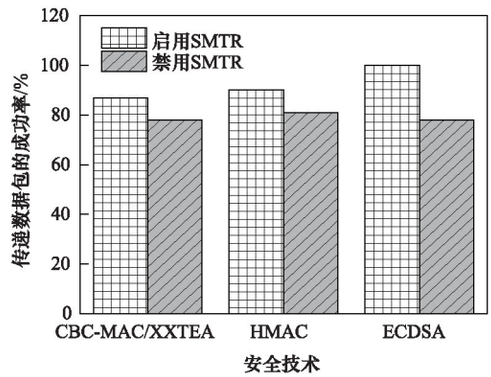
Fig. 8 Eergy consumption of MAC technology and DS technology in different sensor probes in module I

分组密码是基于MAC方案,并且CBC-MAC/XXTEA和AES或RC5比较能耗较低,且与Skipjack算法相比有较高的安全优势,所以选择CBC-MAC/XXTEA。此外,还选择在MicaZ和TelosB传感器探头中对HMAC和ECDSA进行参数比较。通常在传感器网络中并不推荐使用PKC方案,这是因为它是基于不对称的处理模式,相对于对称模式处理更为复杂。

图9是LCTR模型中的SMTR模块启用或禁用时传递数据包的成功率的仿真结果。由图9(a)所示,在MicaZ传感器探头中若在LCTR模型的第2个模块中使用CBC-MAC/XXTEA、HMAC和ECDSA安全技术时,成功率分别提升约为14.5%、20%和45%。图9(b)结果显示,在TelosB传感器探头中若在LCTR模型的第2个模块中使用CBC-MAC/XXTEA、HMAC和ECDSA安全技术时,成功率分别提升约为8%、6.5%和23%。



(a) MicaZ传感器探头



(b) TelosB传感器探头

图9 启用或禁用模块2时采用不同安全技术的成功率

Fig. 9 Success rate of applying different security technologies with module II enabled or disabled

图10是对在不同传感器探头中采用安全协议时总体网络成功率提升的比较。可以看出,MicaZ传感器探头安全性能要优于TelosB传感器探头。

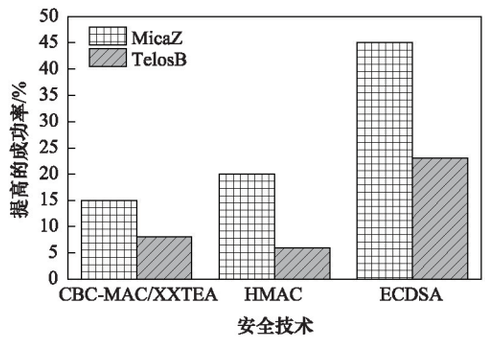
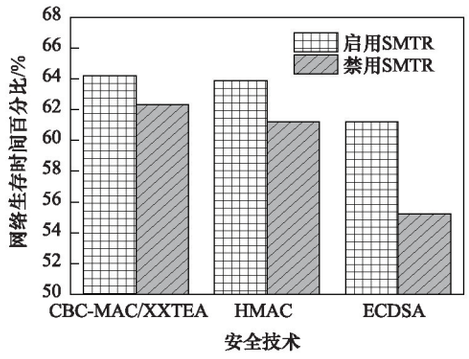


图10 启用模块2时不同传感器探头所提高的成功率

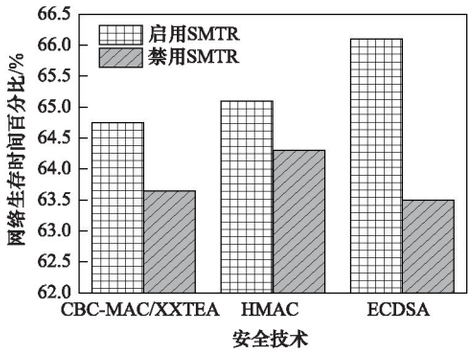
Fig. 10 Improved success rate of using different sensor probes in module II

在启用CBC-MAC/XXTEA、HMAC和ECDSA安全技术时，MicaZ传感器探头成功率分别高于TelosB传感器探头6.5%、13.5%和22%。

图11是启用或禁用模块2时，在两个传感器探头中分别采用CBC-MAC/XXTEA、HMAC和ECDSA安全技术所得网络平均生存时间的对比。



(a) MicaZ传感器探头



(b) TelosB传感器探头

图11　启用或禁用模块2时采用不同安全技术下网络生存时间仿真对比

Fig. 11　Comparison of network lifetime simulation applying different security technologies with module II enabled or disabled

网络生存时间即网络开始运营直到第一个网络传感器消耗完所有能量所需的时间。由图11可以看出，启用模块2可整体延长网络生存时间。模块2之所以提高了成功率和网络生存时间，是因为它在数据包传输过程中启用了模糊推理系统，由模糊推理系统的决策输出按需启用安全技术模块，这样可以减少不必要的能量损耗，从而延长网络生存时间，并且确保传感器网络可抵御常见攻击，提高了网络的安全性能。

5　结论

无线传感器网络是现代通信系统的重要组成，而其网络的安全性是数据传输成功率的重要保证，因此，对于网络安全性的研究十分重要。本文设计了拟面向基于TR协议建立的能量有效的安全模型LCTR，并在模型构造中利用了报文鉴别码和数字签名技术实现鉴权和数据整合，同时比较了抵御网络攻击的各项安全技术的仿真结果，选出CBC-MAC/XXTEA、HMAC和ECDSA3种安全技术应用于LCTR模型的参数比较。研究表明，启用模块2同时使用安全技术可以整体提高数据传输成功率和网络生存时间，使网络更加可靠、稳定；而在启用模块2时，在所选用的3种安全技术中，MicaZ传感器探头使用ECDSA技术成功率提升22%，网络生存时间的百分比增大约5%，TelosB传感器探头使用ECDSA技术成功率提升23%，网络生存时间的百分比增大约3%，其效果最为显著。未来研究中，将进一步总结各种安全技术的特点，建立符合泛在组网形态的安全模型，为后续研究抵御各种攻击的最佳方法和泛在路由提供新的思路。

参考文献(References)

[1] 张金辉, 郭晓彪, 符鑫. AES加密算法分析及其在信息安全中的应用[J]. 通信学报, 2011, 28(5): 23-29.
Zhang Jinhui, Guo Xiaobiao, Fu Xin. AES encryption algorithm and its application in information security[J]. Journal of Communications, 2011. 28(5): 23-29.

[2] Prabhakaran B. On suppoting reliable QoS in multi-hop multi-rate mobile ad hoc networks[J]. Wireless Networks, 2010, 11(3): 106-109.

[3] Maconea D, Oddib G, Pietrabissab A. MQ-Routing: Mobility, GPS and energy-ware routing protocol in MANETs for disaster relief scenarios [J]. Ad Hoc Networks, 2012, 8(9): 2-4.

[4] Kaaniche H, Kamoun F. Mobility prediction in wireless ad hoc networks using neural networks[J]. Journal of Telecommunications, 2010, 8(1): 95-97.

[5] 吕九一, 陈楠. 无线传感器网络的应用与发展概述[J]. 科技广场, 2011, 11(3): 1-4.
Lü Jiuyi, Chen Nan. Application and development overview of wireless sensor networks[J]. Technology Square, 2011, 11(3): 1-4.

[6] 陈正宇, 杨庚, 陈蕾. 无线传感器网络数据融合研究综述[J]. 计算机应用研究, 2011, 10(5): 6-8.
Chen Zhengyu, Yang Geng, Chen Lei. Summary of wireless sensor network data fusion research[J]. Application Research of Computers, 2011, 10(5): 6-8.

[7] Mekkaoui K, Rahmoun A. Analysis of hops length in wireless sensor networks[J]. Wireless Sensor Network, 2014, 6(5): 109-117.

[8] Torkestani J A. Mobility prediction in mobile wireless networks[J]. Joural of Network and Computer Applications, 2012, 8(5): 1633-1635.

[9] 蒋莹, 吴蒙. WSN基于网络编码数据传输可靠性研究[J]. 计算机技术与发展, 2013, 37(4): 12-14.
Jiang Ying, Wu Meng. Reliability research of WSN code-based data transmission network[J]. Computer Technology and Development, 2013, 37(4): 12-14.

[10] Lucas D, Joel J. A survey on cross-layer solutions for wireless sensor networks[J]. IEICE Transactions on Journal of Network and Computer Applications, 2011, 5(34): 523-534.

[11] Egemen K C, Dan B, Amit D. Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: a simulation-based approach[J]. Telecommunication Systems. 2013, 2(6): 751-768.

[12] Kaaniche H, Kamoun F. Mobility prediction in wireless ad hoc networks using neural network [J]. Journal of Telecommunications, 2010, 8(1): 95-97.

[13] Habib M, Ammari B. On the problem of k-coverage in mission-oriented mobile wireless sensor networks[J]. Computer Networks, 2012, 6(1): 7-9.

(责任编辑　吴晓丽)