基于SPIN的无线传感器网络安全协议建模与分析

敬 超 常 亮 古天龙
(桂林电子科技大学计算机控制学院 桂林 541004)

摘 要 模型检验方法在有线网安全协议的分析和设计方面取得了巨大成功。无线传感器网络对安全协议同样具有严格的要求;与有线网相比,无线传感器网络在通信环境和网络节点等方面都更为脆弱,为相应的安全协议的分析和设计提出了挑战。提出了一种适用于无线传感器网络的安全协议形式化建模分析方法。它充分借鉴了传统有线网络安全协议的建模方法,在其基础上充分考察了无线传感器网络的通信环境以及网络节点,建立起一个全面并且直观的安全协议运行模型。以A. Perrig等人提出的SPINS安全协议为例,应用模型检验工具SPIN对其认证性和机密性等安全需求进行了分析验证,发现了该协议存在的漏洞。实例分析证实了模型检验方法在分析无线传感器网络安全协议时的有效性,从而推进了其在安全协议分析方面的应用范围。

关键词 无线传感器网络,模型检验,SPINS协议,SPIN工具,Promela
中图法分类号 TP311 **文献标识码** A

Using SPIN to Model and Analyze Security Protocol in Wireless Sensor Network

JING Chao CHANG Liang GU Tian-long
(School of Computer and Control of Guilin University of Electronic Technology, Guilin 541004, China)

Abstract Model checking has been successfully applied to design and analyze wired network security protocol. Compared with the wired network, wireless sensor network(WSN) also has the strict requirement on its security protocol. The vulnerabilities of WSN exist in communication environment and network node; those are great challenges for designing and analyzing a security protocol in WSN. This paper proposed an appropriate method to model and analyze security protocol in the WSN. Based on the method of wired network security protocol, with the thorough consideration of sensor network environmental factors and feature of sensor nodes, a general model was established and analyzed by our method. The paper took WSN SPINS security protocol as an example to model and analyze via SPIN tool. Through verifying the authentication and confidentiality of SPINS, we found flaws in the SPINS protocol. The work demonstrates the feasibility of using model checking to model and analyze security protocol in WSN, and expands the usage of model checking.

Keywords Wireless sensor network, Model checking, SPINS protocol, SPIN, Promela

WSN(Wireless Sensor Network,无线传感器网络)是一种集MEMS(Micro-Electro-Mechanism System,微电子机械系统)、计算机、通信、自动控制和人工智能等学科的新型测控网络。WSN有大量的、具有通信与计算能力的微小传感器节点,是密布在无人监控区域的、能够根据环境自主完成指定任务的"智能"自治测控网络系统。WSN最早用于军事方面,目前已经扩展到了其它许多领域,如空间探索、医疗和勘探等。由于WSN涉及的数据都具有高机密度和高敏感度等特点,因此为了保证数据不被泄漏,WSN的安全问题成为了当前热点研究的课题之一。除了具备传统有线网的安全特点外,WSN还应具有:(1)内容广泛性,即WSN面向特定应用收集网络信息,要求安全系统支持数据采集、处理和传输等更多网络功能;(2)需求多样性,不同的用户对网络的性能及其安全性需求呈多样化特点;(3)对抗性强,在军事中WSN是用于进攻和防御的工具,遇到的攻击者往往具备很高的专业能力和丰富的经验。针对WSN的这些安全特点,提出了许多经典的适用于WSN的安全协议,如TinySec[1],LEAP[1](Localized Encryption and Authentication Protocol),SPINS(Security Protocols for Sensor Networks)[2]以及MiniSec[5]等。

模型检验对于安全协议的分析已经取得了巨大成功[12]。它的基本思想是用有限状态机表示系统的状态转移结构,用时序逻辑表示设计的性质,通过遍历有限状态机来检验系统是否具有时序逻辑所表达的性质。如果不符合,模型检验工具可以给出一个反例。张玉清等人[4]采用模型检验方法对Needham-Schroeder公钥协议进行了建模分析,检验出了协议存在的漏洞;文献[8]使用SPIN工具对密码协议TMN做建

到稿日期:2008-11-14 返修日期:2009-01-21 本文受广西研究生教育创新项目(2007105950812M16)资助。

敬 超(1983—),男,硕士研究生,主要研究方向为无线传感器网络安全协议等,E-mail:cccjing@mails.guet.edu.cn;常 亮(1980—),男,博士,副教授,主要研究方向为描述逻辑、语义网、智能代理、形式化方法、安全协议;古天龙(1964—),男,博士,教授,主要研究方向为软件工程与形式化方法、离散事件/混杂系统、传感器网络与协议工程、知识工程与符号计算等。

模分析，成功地将模型检验方法运用到了密码协议的分析上；文献[9-11]采用模型检验方法分别对互联网密钥交换协议、电子合同签订协议和公平非否认协议(即 Zhou Gollmann 协议)进行了建模和分析，验证结果扩展了模型检验方法的使用范围。但是，对于 WSN 下的安全协议，采用形式化方法去分析的工作还很少。它面临的挑战性问题主要是：①WSN 的外界环境。传感器节点往往被安置在极其恶劣的环境下，且带宽有限、稳定性差、时延长、传播范围广、通信距离较远等；②传感器自身特点。传感器节点容量有限，计算能力差，节点能量都受到了很大的限制，易损坏、丢失等。这些问题使得传感器节点在执行协议中被迫中断，通信方不得不放弃协议的执行。

WSN 的特点为 WSN 安全协议的建模分析提出了挑战。文献[3]采用 AVISPA 模型检验工具对 WSN 的 LEAP+TinySec 进行了形式化建模和分析，详细描述了使用高级形式化语言 HLPSL 的建模分析过程；通过分析发现了协议存在的漏洞，最后提出了解决方案。但是在分析过程中没有充分考虑 WSN 环境和自身带来的挑战问题。

针对这些挑战，本文在借鉴已有的有线和无线网络安全协议形式化建模和分析方法的基础上，充分考虑 WSN 的环境和传感器自身的特点，以一个经典的 WSN 安全协议 SPINS 为例，给出了一种适用于 WSN 的模型检验建模分析方法；在此基础上，本文采用 LTL(Linear Temporal Logic，线性时态逻辑)对协议的机密性和认证性进行刻画，进而使用模型检验工具 SPIN 对协议进行了分析。分析结果显示了 SPINS 协议存在的漏洞，同时证明了本文方法的有效性。

1 SPINS 协议简介

SPINS 安全协议是一种适用于 WSN 的安全架构，该架构包括 SNEP(Secure Network Encryption Protocol，网络安全加密协议)和 μTESLA(micro Timed，Efficient，Streaming，Loss-tolerant Authentication Protocol，基于时间的、高效的、容忍丢包的流认证协议)两个部分。SNEP 用以实现通信的机密性、完整性、新鲜性和点到点的认证；μTESLA 用以实现点到多点的广播认证。该协议曾经是美国加州大学贝克利分校的 Smart Dust 项目，用此协议成功地构建了 WSN 安全通信平台。此后，巴西学者 A. C. Ferreira 等人[13]将 SPINS 架构用于保证一种 WSN 簇结构的通信协议的安全性。

在此主要对 SPINS 中的 SNEP 协议进行建模和分析。SNEP 协议是一种低通信开销的、实现了数据机密性、数据认证、完整性保护、新鲜性保证的简单高效的安全通信协议。它采用预共享主密钥 Kmaster(master key)的安全引导模型，假设每个节点都和基站之间共享一对主密钥，其它的密钥都是从主密钥衍生出来的。SNEP 协议的各种安全机制都是通过信任基站完成的。根据 SNEP 协议，当两个节点要进行通信的时候，因为之前没有共享的秘密，所以决定通过彼此之间信任的基站来协助建立安全通道。假设 A 和 B 都与基站 S 存在共享密钥 K_{AS} 和 K_{BS}，具体通信过程如下：

(1)$A \rightarrow B: N_A, A$

(2)$B \rightarrow S: N_A, N_B, A, B, MAC(K_{BS}, N_A | N_B | A | B)$

(3)$S \rightarrow A: \{SK_{AB}\}K_{AS}, MAC(K_{AS}, N_A | B | \{SK_{AB}\}K_{AS})$

(4)$S \rightarrow B: \{SK_{AB}\}K_{BS}, MAC(K_{BS}, N_B | A | \{SK_{AB}\}K_{BS})$

首先，WSN 中的节点 A 要与 B 进行通信。A 通过广播的方式寻找节点 B，并将自己与 B 通信的请求和 N_A 发给节点 B(N_A 为强新鲜性认证的 Nonce 随机数，保证数据的新鲜性)。接着，节点 B 收到了 A 的请求后，B 将和 A 的通信的请求以及 N_A，N_B 采用 MAC(Message Authentication Code，消息认证码)方式发送给基站 S，即将发送的消息用自己与基站共享的密钥 KBS 和 CTR(COUNTER，计数值)模式下计数器产生的计数值加密后发送给 S。基站在接收到了 B 的请求后，通过验证，将临时共享密钥 SK_{AB} 分别采用同样的 MAC 方式分配给节点 A 和 B。最后，节点 A 和 B 分别验证了基站 S 发来的消息，采纳密钥 SK_{AB} 后，A，B 两节点才能建立信道，进行安全的通信。若需要再次通信，可以重新协商新的密钥。

2 SPINS 协议建模

针对协议涉及的初始方、响应方、服务方和入侵方，本节分别采用有限自动机的方式刻画出协议在运行时可能出现的状态。

2.1 协议诚实主体的建模

在 SPINS 中，诚实主体主要是发起方、响应方和服务器方。对于发起方 A，用有限状态机来刻画其执行协议时的状态过程。图 1 所示是发起方想与 WSN 中某个 B 节点进行安全通信时的整个状态转换过程。A 自动从初始状态 idle 跳转到 Sa1 状态，选择 B，生成消息 1，开始执行协议；在向 B 发送了消息 1 后进入 Sa2 状态，等待消息 2 的到来；在接到消息 2 后，判断消息 2 是否符合要求；如果符合要求，进入 Sa3 状态；最后进入 finish 状态，完成一次协议的执行。此后，A 可以重新进入初始状态 idle，开始另外一次协议的执行。这里需要注意的是，为了模拟协议运行在 WSN 环境，假设在 A 处于 Sa2 状态等待消息 2 到来时，除了正常接收到消息 2 进入 Sa3 外，还会出现两种情况：(1)无线传感器网络下的环境因素，从而使 A 被迫中断协议执行。如网络的带宽、可靠性、延时以及稳定性等，都会导致消息丢失或者无限地延迟下去。在此引入一个计时器，当收到消息 2 为超时，A 进入 Abort 状态，被迫放弃协议执行。说明 A 由于 WSN 环境的因素，导致无法收到消息 2；(2)传感器自身的特点，如传感器容量有限、能量低、易耗尽以及计算能力差等因素，导致 A 被迫中断协议的执行。此时设置了一个 Energy 的 bool 变量来标记由于传感器本身产生的故障。若 Energy=1，说明传感器节点出现故障，A 进入了 Abort 状态，中断了此次协议的执行。

对于响应方，用有限状态机刻画，如图 2 所示。

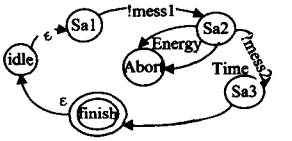


图 1 发起方 A 执行协议时的状态转换图

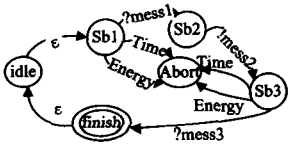


图 2 响应方 B 执行协议时的状态转换图

当有节点要与 B 进行通信时，B 自动进入了 Sb1 状态，等待接收消息 1；在接收到消息 1 后进入 Sb2 状态，生成消息 2；在发送消息 2 之后进入 Sb3 等待状态，等待消息 3 的到来；接到了消息 3 后进入 finish 状态，完成一次协议执行。此后，B 可以重新进入初始状态 idle。与 A 相同，在进入状态 Sb1

和 Sb3 状态时，同样考察了 WSN 的环境和传感器本身的因素。

对于服务器方的有限状态刻画，如图 3 所示。

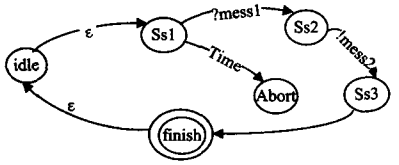


图 3　服务器方 S 执行协议时的状态转换图

当有节点发出了请求后，S 自动进入状态 Ss1，等待接收消息 1；在接收到了消息 1 后进入 Ss2 状态，生成消息 2；在发送了消息 2 后，直接进入状态 Ss3；最后进入 finish 状态，完成一次协议的执行。此后，S 可以重新进入初始状态。在这里，与 A 和 B 不同的是，由于服务器采用的是固定的装置设备，相比小的传感器而言，基站服务器自身不容易出现故障。因此，在 S 进 Ss2 状态时，没有考虑设备本身带来的影响，只考察了 WSN 环境的因素，导致 S 进入了 Abort 状态，被迫放弃协议。

2.2　入侵者模型

入侵者模型是最难、最复杂的一部分。根据 Dolev-Yao[7] 的模型，假设协议执行过程被入侵者所控制。基于这种假设所得到的通信模型如图 4 所示。

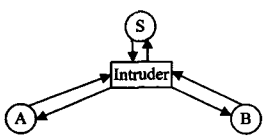


图 4　协议通信模型图

其中入侵者具有以下的能力：

(1)可以在任何通信主体间截获消息或者转发消息；

(2)可以以自己的身份冒充 A，B 和 S；

(3)根据获取的消息增长自己的知识，产生新的消息；

(4)解密已知密钥加密的消息(完美加密假设：入侵者对不知道密钥加密的消息无法解密)。

入侵者进程的 Promela 实现，主要分为两大部分：一是从通道中截取消息，包括存储不能解密的消息和解密已知密钥的消息来获取知识；二是发送消息到通道中，随机转发截取的消息，或者发送根据获取知识产生的新消息。具体如下：

```
/*—Intruder model——*/
Proctype Intruder()
{
do
/*——part I:intercept and storage the message——*/
.....
/*——part II: transmit intercept message, or send new message due to already known knowledge——*/
.....
od
}
```

入侵者的行为是非确定的，它的执行实际上是无限循环的(do…od)，且包括所有可能的状态，以达到对协议整个状态的搜索。

3　协议性质的 LTL 描述

采用时态逻辑中的线性时态逻辑 LTL 对协议所需满足的属性进行规格验证，并且对需要满足的性质进行描述。

3.1　LTL 简介

线性时态逻辑 LTL 是一种采用线性、离散且与自然数同构的时间结构，以路径(状态序列)作为命题的论断对象。线性时态逻辑公式是在状态序列上解释其真值的[14]。线性时态逻辑被广泛地用于有限状态系统的行为描述，它的语法可递归定义如下：

①命题常量{true，false}和原子命题变元($p,q,r,\cdots$)是线性时态逻辑公式；

②如果 p,q 是线性时态逻辑公式，则$\neg p, p\wedge p, p\vee q, p\,U q$ 也是线性时态逻辑公式；Gp, Fp, Xp 也是线性时态逻辑公式；

③每个线性时态逻辑公式均可通过有限次应用如上构造获得。

时态算子 G，F，X，U 分别表示 Globally，Future，neXt time，Until。表 1 给出了在 SPIN(见 4.1 节)中描述 LTL 使用的时态和逻辑操作符。

表 1　LTL 的时态和逻辑操作符

一、二元操作符	含义
[]	时态操作符“一直”(always)
<>	时态操作符“最终”(eventually)
!	布尔操作符“否定”(negation)
U	时态操作符“直到”(until)
&&，∧	布尔操作符“与”(and)
||，∨	布尔操作符“或”(or)
−>	布尔操作符“蕴含”(implication)

LTL 模型检测的常用方法是将所要检测的性质即 LTL 公式的补(否、非)转换成 Büchi 自动机，然后求其与表示系统的自动机的交。如果交为空，则说明系统满足所要检测的性质；否则生成对应反例，说明不满足的原因。

3.2　LTL 性质描述

对于 SPINS 协议，采用 LTL 对认证性和机密性进行规格描述。

(1)认证性。是指能够确认对方的真实身份后，保证对方的真实身份与协议消息中所声称的身份相一致。分析 SPINS 协议时，采用了文献[6]的方法进行检测。即若初始者 I 发起了一次会话与响应方 R，则响应方 R 必须也和 I 进行一次会话；若初始方 I 确信自己已经完成了与响应方 R 的一次协议运行，则 R 必须开始与 I 的协议执行。因此得到了以下 4 个变量，分别表示为：

bit Init_A=0；当 A 向 B 发起一次会话，置 1；

bit Init_B=0；当 B 向 S 发起一次会话，置 1；

bit End_B=0；当 B 完成了与 S 的最后执行，置 1；

bit Init_S=0；当 S 响应了 B 的会话，置 1；

bit End_S_a=0；当 S 完成了与 A 的最后执行，置 1；

bit End_S_b=0；当 S 完成了与 B 的最后执行，置 1；

因此，得到的 LTL 公式表示如下：

G1：[]((! End_S_a)||(! End_S_a U Init_A))

G2：[]((! End_B)||(! End_B U Init_B))

G3：[]((! End_S_b)||(! End_S_b U Init_S))

[]表示一直(always)，U 表示直到(until)。若 G1 不满足，说明有入侵者冒充 A 与 B 通信；若 G2 不满足，说明有入侵者冒充 B 与 S 通信；若 $G3$ 不满足，说明有入侵者冒充 S 与

B 通信。

(2)机密性。保证需要保密的协议消息内容在传送过程中不被非法窃取。对于 SPINS,其机密性必须满足语义安全的特性,即相同的数据信息在不同的时间、不同的上下文,经过相同的密钥和加密算法产生不同的密文。在这里,通信双方共享同一个密钥,通过使用计数器模式 CTR 来实现语义安全。通信双方共享一个计数器,计数器值作为每次通信加密的初始化向量。这样,每次计数值不同,则必定产生不同的密文。这样就保证了传送内容的机密性,不容易被入侵方获取,而消息内容的身份也需要保密。因此,在我们的入侵者模型中相应地加入了三个变量来获取其 ID:

bit known_A=0; 当能够解密消息,并且在消息中包含了 A 的身份,置 1;

bit known_B=0; 当能够解密消息,并且在消息中包含了 B 的身份,置 1;

bit known_S=0; 当能够解密消息,并且在消息中包含了 S 的身份,置 1;

所以得到的机密性的 LTL 描述公式如下:

G4:[](! known_A&&! known_B&&! known_S)

4 实验结果与分析

本节采用模型检验工具 SPIN 的 Promela 语言对模型的过程进行描述,并对协议所需满足的性质进行验证,检验协议在受到攻击的情况下,是否满足其基本性质。

4.1 检验工具 SPIN

SPIN(Simple Promela INterpreter)是一种适合于并行系统尤其是协议一致性的辅助分析验证工具。它以 PROMELA(PROcess Meta LAnguage)为输入语言,可以对网络协议设计中规格的逻辑一致性进行检验,检测一个有限状态系统是否满足线性时态逻辑 LTL 公式及其它一些性质。SPIN 模拟和检验的基本过程如图 5 所示。

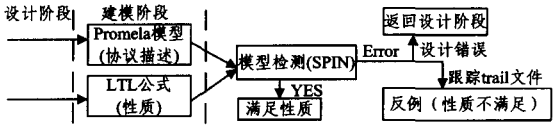


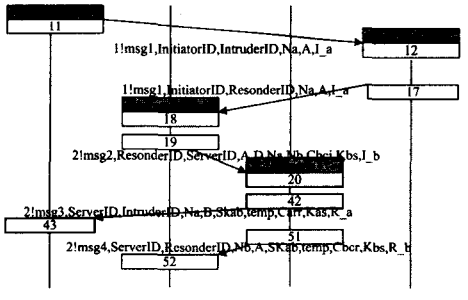
图 5 SPIN 的工作流程

4.2 结果分析

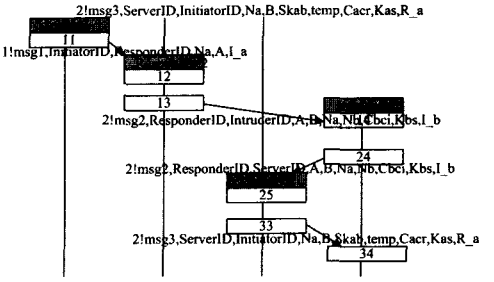
使用 SPIN 验证了第 3 节模型描述的 LTL 属性,结果表明,认证性中的 $G1$,$G2$ 和 $G3$,以及机密性的 $G4$ 性质均不满足,检测过程如下:

(1)认证性

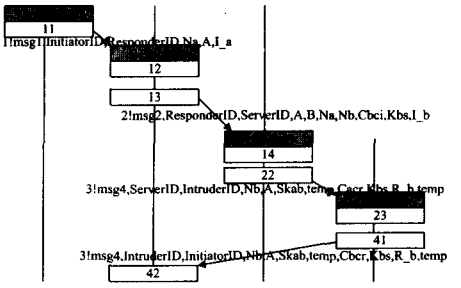
$G1$,$G2$ 和 $G3$:受到的攻击轨迹如图 6 所示。



(a)G1 受到的攻击轨迹



(b)G2 受到的攻击轨迹



(c)G3 受到的攻击轨迹

图 6 检测 G1,G2 和 G3 时的受到的攻击轨迹

图 6(a)表明,入侵者 Intruder 冒充了 A 并与 B 进行通信,并将入侵者的消息发送给 B;图 6(b)中表明,入侵者 Intruder 冒充了 B 与 S 进行通信,而 S 认为是 B 与其通信,得到了消息后又转发给了入侵者 Intruder;图 6(c)表明,入侵者冒充了 S,而 B 确认为其通信方是 S,直接与 Intruder 通信,并且接收 Intruder 的响应。

上述 3 种情况表明,入侵者冒充了 A,B 和 S,从表面看来是不满足认证性的,因为入侵者 I 可以冒充 A 或 B 或 S。但是进一步分析 SIPNS 发现攻击对于整个协议的安全并没有实质性的影响。因为在 SNEP 协议中,协议实现点到点的认证是通过 MAC 实现的,要想解密获取的密文,必须获取共享计数值(CTR)和密钥。从上述情况可以看出,入侵者主要是截取消息并转发,而不能获得加密用的共享计数值。根据 SNEP,为了解密发送内容,必须获得双方共享的密钥和计数值,而这个计数值是根据时间而产生的,入侵者根本无法获得。所以,入侵者即使能截取消息,冒充 A,B 和 S 的身份进行通信,也不能在 A,B 和 S 中获得任何利益。

(2)机密性 $G4$

1)$A->I(B)$:Na,A

2)$I(B)->S$;$\{Ni,I,Na,A\}_{kbs}$

3)$S->I(B)$;$\{Ni,A,Skab\}_{kbs}$

消息 1 表示 A 发送给 B 后,消息被 I 截获,同时冒充 B 发送自己产生的消息 2 给 S。S 还不知道接收到的消息是入侵者的,于是根据消息 2,产生消息 3 发送给 B,此时消息 3 再次被入侵者截获。这时,因为之前的消息 2 也是入侵者冒充了,入侵者可以根据 CTR 对消息 3 进行解密,从而获得分配给 A 和 B 的共享密钥 SK_{AB},破坏了机密性。

结束语 本文分析过程充分考虑了 WSN 的环境和自身特点,提出了一种适用于 WSN 的安全协议建模分析方法,并用此方法验证了 SPINS 协议的机密性和认证性。实验结果表明,模型检验方法同样可以有效地应用到 WSN 的安全协议分析上,从而拓展了模型检验的应用范围。同时,展示了如何使用模型检验方法(尤其是 SPIN 工具)对 WSN 的安全协

议进行建模分析。

参 考 文 献

[1] Mayank S. Security in Wireless Sensor Networks[OL]. http://www.cs.utk.edu/~saraogi/594paper.pdf,2005

[2] Perrig A,et al. SPINS:Security Protocols for Sensor Networks [J]. Wireless Networks,2002,8(5):521-534

[3] Tobarra L,et al. Model Checking Wireless Sensor Network Security Protocols:TinySec + LEAP[C]// WSAN'07. Albacete (Spain),IFIP Main Series,Springer,September 2007:95-106

[4] 张玉清,王磊,肖国镇,等. Needham-Schroeder 公钥协议的模型检测分析[J]. 软件学报,2000,11(10):1348-1352

[5] luk M,et al. MiniSec:A Secure Sensor Network Communication Architecture[C] // IPSN' 2007. Cambridge, Massachusetts, USA. ACM,April 2007:479-488

[6] Marrero W,et al. A Model Checker for Authentication Protocols [C]//DIMACS Workshop on Design and Formal Verification of Security Protocols. Sep 1997:147-166

[7] Dolev D,Yao A C. On the Security of Public Key Protocols [C] //FOCS,IEEE. 1981:350-357

[8] Li Y J,Xue R. Using SPIN to Model Cryptographic Protocols [C]//Proceeding of the International Conference on Information Technology:Coding and Computing,ITCC'04. Volume 2,2004:741-746

[9] 常亮,古天龙,郭云川. 互联网密钥交换协议的 SMV 分析[J]. 计算机工程与应用,2005,41(19):154-158

[10] 常亮,古天龙,郭云川. 电子合同签订协议的符号模型检验分析[J]. 计算机工程与应用,2005,41(01):161-164

[11] 董荣胜,陈大伟,郭云川,等. 公平非否认协议的有限状态分析[J]. 计算机科学,2005,38(8):83-86

[12] Clarke E M. The Birth of Model Checking[M]. 25 Years of Model Checking,2008:1-26

[13] Ferreira A C,et al. On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks[C]// LNCS. Vol. 3420,Springer,2005:449-458

[14] Cortadella J,Michael. Deriving from Finite Transition System [J]. IEEE Transaction on Computers,1998,47(2):859-882

(上接第 93 页)

并不能满足全局优化。因此,算法的执行效果比 MNL_QoS 和 LEACH_QoS 要差。

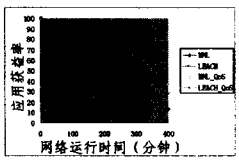


图 5 应用获益率

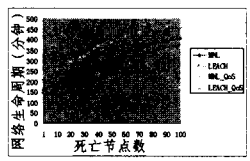


图 6 网络生命周期

结束语 本文首先提出一种基于服务中间件的无线传感器网络 QoS 保障框架,主要对其中的 QoS 评价问题进行了研究。利用云模型在定性和定量转换时的桥梁作用,提出一个基于云模型和获益驱动的多维 QoS 目标评价机制。此机制对应用任务进行定量评价,能比较准确地反映多维的 QoS 需求,使任务得到满意的执行。模拟实验表明,加入了评价机制的数据收集算法,比单纯的数据收集算法能更有效地延长网络生命周期。

今后的研究工作主要是对多维 QoS 评价进行进一步的验证,探讨多样化的 QoS 获益函数,并继续探讨云模型在 QoS 保障方面的应用,实现更完整的基于服务中间件的 QoS 保障框架原型。

参 考 文 献

[1] Pottie G J,Kaiser W J. Wireless integrated network sensors[J]. Communications of the ACM,2000,43(5):51-58

[2] Iyer R , Kleinrock L . QoS Control for Sensor Networks [C] // Proceedings of 2003 IEEE International Communications Conference on Communication. Anchorage Alaska: IEEE Computer Society,2003:11-15

[3] Saxena N,Roy A,Shin J,et al. Dynamic duty cycle and adaptive contention window based QoS-MAC protocol for wireless multimedia sensor networks [J]. Computer Networks,2008,52(13):2532-2542

[4] Yu Ming,Malvankar A,Su Wei,et al. A link availability-based QoS-aware routing protocol for mobile ad hoc sensor networks [J]. Computer Communications,2007,30(18):3823-3831

[5] Tai S,Benkoczi R R,Hassanein H,et al. QoS and data relaying for wireless sensor networks [J]. Journal of Parallel and Distributed Computing,2007,67(6):715-726

[6] Alex H , Kumar M , Shirazi B. MidFusion : An adaptive middleware for information fusion in sensor network applications [J]. Information Fusion,2008,9(3):332-343

[7] Yuan Yong,Yang Zongkai,He Zhihai,et. al. An integrated energy aware wireless transmission system for QoS provisioning in wireless sensor network [J]. Computer Communications,2006,29(2):162-172

[8] Mahapatra A,Anand K,Agrawal D P. QoS and energy aware routing for real-time traffic in wireless sensor networks [J]. Computer Communications,2006,29(4):437-445

[9] He Zhen,Lee Byung Suk,Wang X S. Aggregation in sensor networks with a user-provided quality of service goal [J]. Information Sciences,2008,178(1):2128-2149

[10] 岳昆,王晓玲,周傲英. Web 服务核心支撑技术:研究综述[J]. 软件学报,2004,15(3):428-442

[11] 李德毅,刘常昱. 论正态云模型的普适性[J]. 中国工程科学,2004,6(8):28-34

[12] 吕辉军,王晔,李德毅,等. 逆向云在定性评价中的应用[J]. 计算机学报,2003,26(8):1009-1014

[13] 熊和金,陈德军. 智能信息处理[M]. 北京:国防工业出版社,2006:56-65

[14] 张文博,陈宁江,魏峻,等. QoS 获益驱动的中间件调度框架研究[J]. 软件学报,2006,17(6):1381-1390

[15] Liang Weifa,Liu Yuzhen. Online Data Gathering for Maximizing Network Lifetime in Sensor Networks [J]. IEEE Transaction on Mobile Computing,2007,6(1):2-11

[16] Heinzelman W R,Chandrakasan A,Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks [C]// Proceedings of the Hawaii Int'l Conf. on System Sciences. San Francisco: IEEE Computer Society, 2000: 3005-3014