第 39 卷 第 4 期 计 算 机 工 程 2013 年 4 月
Vol.39 No.4 Computer Engineering April 2013

·移动互联与通信技术· 文章编号：1000—3428(2013)04—0100—05 文献标识码：A 中图分类号：TP393.4

物联网中跨域移动节点的信任迁移

马满福，倪 伟

(西北师范大学计算机科学与工程学院，兰州 730070)

摘 要：针对物联网中移动节点跨域后信任缺失的问题，参考当前信任领域和传感器网络的研究成果，提出物联网中面向跨域移动节点信誉体系的网络模型、服务模型和信誉模型，并在此基础上研究异动节点跨域后信任的迁移和建立过程。结合高斯分布的传感器网络信誉模型(GRFSN)，讨论跨域移动节点的信誉初始化、信誉更新、信誉整合和信誉共享方法。仿真结果证明，在物联网节点跨域环境下，跨域移动节点的信誉收敛速度快于传统 GRFSN 模型，并能保持 GRFSN 模型可检测恶意节点的特点。

关键词：物联网；移动节点；信任迁移；高斯分布；信誉体系

Trust Transfer of Cross-domains Mobile Node in Internet of Things

MA Man-fu, NI Wei

(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

【Abstract】This paper targets on the problem which mobile nodes lose trusts after crossing domains in Internet of Things(IoT), and references current researches on networking trust and Wireless Sensor Network(WSN). It raises network model, service model and reputation model of reputation system for cross-domains nodes in IoT. It describes a series of processes which give trust transfer and initialization. It gives methods of reputation initialization, update, integration and sharing via Gaussian Reputation for Sensor Network(GRFSN) model. Simulation results show that in the context of IoT, it has higher convergence speed than the traditional GRFSN model in WSN and it also keeps the attribute of detecting malevolence nodes.

【Key words】 Internet of Things(IoT); mobile node; trust transfer; Gaussian distribution; reputation system

DOI: 10.3969/j.issn.1000-3428.2013.04.024

1 概述

随着物联网技术和应用受到学术界的普遍关注，物联网(Internet of Things, IoT)中的信任计算与评估也成为物联网安全问题研究的焦点[1-2]。国际电信联盟(ICU)的定义[3]指出，物联网需要在任何时间、任何地点，以任何方式提供信息访问和管理服务。根据 ICU 的定义，物联网中的节点可以在网内漫游。进而，物联网移动节点的信任问题也成为物联网安全问题研究的重要方向。

文献[4]指出，物联网中的移动节点漫游的组合安全认证协议虽然是针对物联网中移动节点的身份信任提出的协议，但是其中采用的信任域的概念和将中间件技术与服务计算技术融入的方法同样可以应用于物联网中移动节点漫游的行为信任模型当中。本文在这些概念和方法的基础上，参考文献[5]中移动业务中基于跨信任域节点的信任计算的 RBAC 模型以及文献[6]中移动代理的信任管理方法，探讨一种基于高斯分布[7]的物联网信誉体系，形式化地分析体系的网络模型、服务模型和信誉模型。

2 面向跨域移动节点的信任体系

物联网中存在多个传感器网络，每个传感器网络网关感知区域内的所有节点都属于这个网关所属的感知子网，这样就天然地划分了信任域[5]。如图 1 所示，存在这样的节点，它可以在信任域间漫游，那么这个节点就需要与多个信任域相互作用，在某个时间跨度上受多个信任域管理。为降低节点跨域时所带来的信誉计算、信誉分享和信誉评价的复杂度，本文在现有无线传感器网络信任模型、物联网中间件技术[8]和服务计算技术的基础上，结合物联网中跨域节点的特点，提出了面向跨域移动节点的信任体系。在此体系中，网络模型作为基础设施处于最下层，信誉模型作为核心处于最上层，而服务模型作为中间层，起到连接网络模型和信任模型的关键作用。

基金项目：教育部科学技术研究基金资助重点项目(208148)；甘肃省科技攻关计划基金资助项目(2GS064-A52-035-03)

作者简介：马满福(1968－)，男，副教授、博士后，主研方向：移动计算，计算机系统结构；倪 伟，硕士研究生

收稿日期：2012-05-18 **修回日期：**2012-08-20 **E-mail：**riverflood@163.com

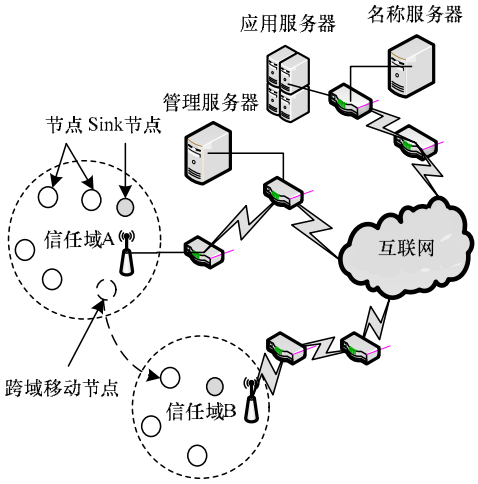

图 1　移动节点在信任域间的移动

2.1　网络与服务模型

物联网的网络通信技术包括各种有线和无线传输技术、交换技术、组网技术、网关技术[1,8]，本文所采用的网络模型布局如图 2 所示。

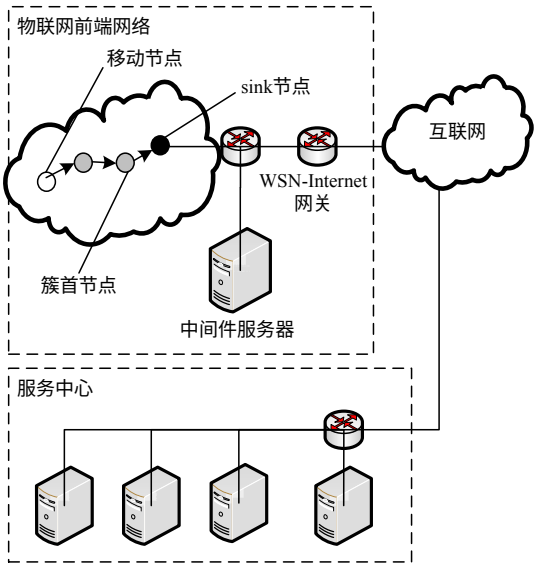

图 2　信任体系的网络模型

物联网前端网络通过 WSN-Internet 网关接入互联网，在物联网前端路由器部署中间件服务器，在互联网端部署服务中心，服务中心是一组服务器机群，其管理范围覆盖多个物联网前端。服务中心包括各种数据处理服务器、ONS 服务器、CA 服务器和管理服务器。这些网络和设备以一定的网络结构组织起来，形成了体系的网络模型，使其具备了分布式信誉计算、分布式信誉存储、信誉共享以及信誉评价的能力。

网络模型使物联网具备了信誉计算、存储、共享和评价的能力，为将这些能力有效地组织起来，本文引入服务模型概念并将其整合入信任体系中。服务模型可以将分布式的信誉计算、存储、共享和评价的能力有机结合起来，封装成服务，如图 3 所示。

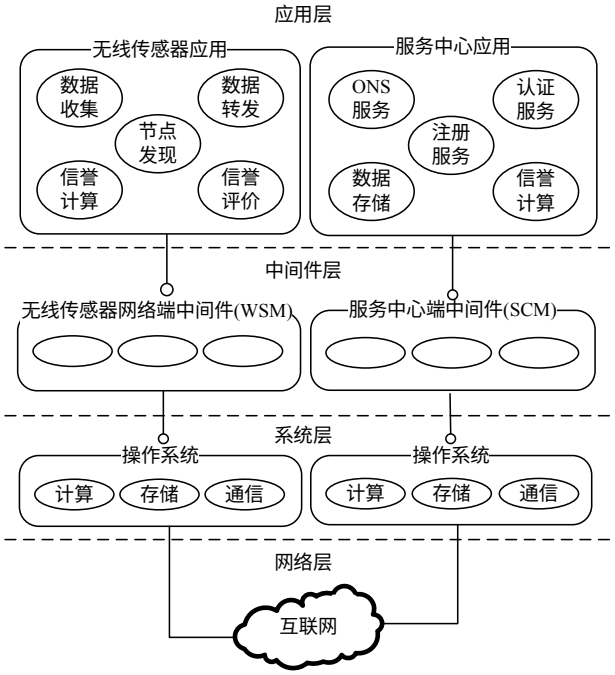

图 3　信任体系的服务模型

物联网在无线传感器网络、普适计算和云计算等技术之间普遍地使用了中间件技术[8]，利用中间件将各种技术有机结合起来为整个物联网系统提供服务。中间件是位于操作系统和应用之间的一个软件层，它有效地解决了分布式异构网络之间的通信和系统差异的复杂性[9-10]。中间件是本文服务模型的支撑点。

2.2　信誉模型

信誉模型作为信任体系的核心，是信任体系中信誉计算的基本模型，也为信誉评价提供了依据。

文献[7]讨论了基于高斯分布的传感器网络信任模型(Gaussian Reputation For Sensor Network, GRFSN)，本文在此模型的基础上参考文献[11]的对等网络信任和信誉机制并引入初始化参数来计算跨域节点迁移后的初始信誉。

2.2.1　带有参数的信誉分布初始化

文献[7]对新加入节点的初始信誉值赋为 0.5，但对于从其他信任域迁移而来的节点，如果不迁移它之前的信誉，对以前信誉良好的节点并不公平，而对以前信誉不良的节点在一段时间有所姑息。本文针对这种不公平性以及物联网中存在着大量移动节点的情况，提出将移动节点移动前所在域的信誉分布按式(1)进行计算后作为移动节点在移动后信任域的初始信誉分布，称为信任迁移。式(1)参考了文献[6]的信誉整合公式，并引入初始化参数 α_j 与 μ_j：

$$X_{ij}=N(0.5\alpha_i+\mu_i(1-\alpha_i),0.5^2\alpha_i^{\,2}+\sigma_i^2(1-\alpha_i)^2) \quad (1)$$

其中，$\alpha\in[0,1]$ 是移动后信任域对原信任域的权重。初始化参数 α_j 与 μ_j 分别为移动节点移动前的信誉分布 $X_s=N(u,v^2)$ 中的均值 u 和方差 v，X_s 通过物联网服务向服务中心请求移动节点的上下文时获得，移动节点的上下文包括

移动节点的身份标识、移动前的信誉分布等信息。

2.2.2 信誉更新、信誉整合与信誉共享

移动节点的信誉分布初始化后就可以此为依据进行信誉的更新。文献[7]已证明独立的贝努利事件可以用高斯分布建模。本文根据高斯分布模型采样与信誉的更新，设 $v=\mu=m/(m+n)$，$u^2=\sigma^2=mn/(m+n)^2$，其中，m 和 n 分别表示在 t 时段内节点 i 与节点 j 进行通信成功和失败的次数。假设节点 i 关于节点 j 的信誉分布 X_{ij} 服从 $N(\mu_j,\sigma_j^2)$，$(X_{ij})_1(X_{ij})_2\cdots(X_{ij})_t$ 是 X_{ij} 的样本，参数 μ_j 的先验分布为 $N(v,u^2)$，信誉 X_{ij} 的后验分布服从高斯分布，且满足式(2)：

$$\begin{cases}\mu_j'=\dfrac{\dfrac{t}{\sigma_j^2}\bar{X}+\dfrac{v}{u^2}}{\dfrac{t}{\sigma_j^2}+\dfrac{1}{u^2}}\\ \sigma_j'=\dfrac{1}{\dfrac{t}{\sigma_j'^2}+\dfrac{1}{u^2}}\end{cases}\tag{2}$$

算法 1 样本采样

输入 采样相关节点的下标 i,j 及采样时段 t

输出 X_{ij} 的一个样本 X_{ave}

```
sum:=0
listener_ij:=NULL;      // listenerij 是 ij 节点之间的监视器
INIT(listener_ij);      //初始化 listener_ij
for i:=1 to t do
        sum:=sum+listener_ij[success]/listener_ij[total]
X_ave:=(1/t) * sum
return X_ave
```

若只是依靠节点 i 对节点 j 的直接信誉更新信誉，算法收敛速度很慢，采样的周期会很长，计算的开销也会很大。根据实体之间信誉具有弱传递性的特点，采用间接信誉更新移动节点的信誉是合理的，式(3)描述了直接信誉和间接信誉共同更新移动节点信誉。

$$X_{ij}=X_{ij}^{D}\otimes X_{ij}^{ID}\tag{3}$$

其中，X_{ij} 表示更新后节点 i 对节点 j 的信誉；X_{ij}^{D} 表示它们之间的直接信誉；X_{ij}^{ID} 表示它们之间的间接信誉；$\otimes$ 运算表示一种抽象运算，它的具体内容根据具体的信誉模型来决定。根据以上关系，文献[12]提出了式(4)并给予了证明。

$$X_{ij}=N(\alpha\mu_j+(1-\alpha)\mu_{kj},\alpha^2\sigma_j^2+(1-\alpha)^2\sigma_{kj}^2)\tag{4}$$

其中，$\alpha\in[0,1]$ 是直接信誉的权重。根据以上公式，通过直接信誉和间接信誉就可以计算出更新后节点 i 对节点 j 的信誉。

当移动节点离开原信任域时，物联网前端请求信誉收集服务来收集原信任域中各节点对移动节点的信誉评价，然后请求信誉计算服务计算原信任域对移动节点的整体信誉分布 X_s，计算服务根据式(5)计算 X_s。

$$X_s=N(\sum_{i=1}^{k}\varpi_i\mu_i,\sum_{i=1}^{k}\varpi_i^2\mu_i^2)\tag{5}$$

其中，$\omega_i\in[0,1]$ 表示原信任域中第 i 个节点对整体信誉计算的权重，且有 $\sum\omega_i=1$。计算完成后，原信任域的 sink 节点调用物联网信誉共享服务，将计算结果 $N(u,v^2)$ 更新到服务中心。其中，算法 2 为中间件计算 X_s 的伪代码：

算法 2 计算原域对移动节点的信誉分布

输入 原域中对移动节点有信誉评价的节点集合 *Nodes*；原域中移动节点的信誉矩阵 ***X***，行数:=|*Nodes*|，行的向量为(*p*, *q*)，其中 *p* 为 μ，*q* 为 δ^2；节点的权重向量 ***W***

输出 原域对移动节点的整体信誉分布 X_S

```
u:=0
v:=0
k:=|Nodes|
for   i:=1 to k   do
        u:=u+W[i] * X[i].p
        v:=v+(W[i]^2) * X[i].q
XS:=(u,v)
return XS
```

更新到服务中心的信誉分布可以被其他的信任域共享，在服务中心管理域中的物联网前端在检测到移动节点移入后请求服务中心共享移动节点的历史信誉分布。

2.3 算法流程

假设物联网前端具有检测移动节点移入、移出其所属信任域的能力[13]，系统的算法流程如下伪代码：

(1)算法 3 为物联网前端主节点服务流程伪代码。

算法 3 前端主节点服务流程

```
//建立看门狗检测移动节点行为
wtd:=Create_Watchdog()
//监听物联网前端服务器发来的消息
eventlistener:=Create_Event_Listener()
//看门狗服务
Begin Serv_CheckNode(wtd, eventlistener)
If wtd.action is move_out;        //节点移出
 Request_caculate_trust(m);     //请求计算节点 m 的信任
Else If wtd.action is move_in;   //节点移入
 id:=Request_nodeId();          //向节点 m 请求节点的身份标识
//发送节点 m 的身份标识到前端服务器中间件请求节点 m 的
//上下文
 Request_context(id)
End If
End Serv_CheckNode
//消息处理服务
Begin Serv_HandlerMsg(wtd,eventlistener)
v:=eventlistener.msg
If v.validate_tag is false;      //检测身份验证
```

```
  Refuse_serv(m);                 //失败则拒绝服务
Else
  Init_Trust(v.XS_m);             //成功则初始化信誉分布
End If
End Serv_HandlerMsg
```

(2)算法 4 为物联网前端服务器中间件服务流程伪代码。

算法 4 前端服务器中间件服务流程

```
//监听消息，消息来源为物联网前端主节点或服务中心
eventlistener:=Create_Event_Listener()
//消息处理服务
Begin Serv_HandlerMsg(eventlistener)
  If eventlistener.action is request_caculate
//消息是请求计算信任，来源为前端网络主节点
        XS_m:=Calculate_Trust(m);   //计算移动节点 m 的信任
        Request_Update(m, XS_m);    //请求更新信任
  Else If eventlistener.action is request_context
  //消息是请求节点上下文，来源为前端网络主节点
        msg:=eventlistener.msg;     //获取消息内容
        id:=msg.id
        //向服务中心请求节点标识为 id 的节点的上下文
        Request_context(id)
  Else If eventlistener.action is   response_context
  //消息 msg 是应答节点上下文的请求消息，来源为服务中心
        Response_context(msg.v); //向主节点发送 m 的上下文
  End if
End Serv_HandlerMsg
```

(3)算法 5 为服务中心服务流程伪代码。

算法 5 服务中心服务流程

```
//监听物联网前端网络服务器发来的消息
eventlistener:=Create_Event_Listener()
//消息处理服务，消息来源为物联网前端网络服务器
Begin Serv_HandlerMsg(eventlistener)
  If eventlistener.action is request_update
        Update_trust(msg.id, msg.XS);    //更新节点的信任
  Else If eventlistenr.action is request_context
        v:=Search_context(msg.id);      //查找节点的上下文
        //向前端网络服务器发送节点的上下文
        Response_context(v)
  End If
End Serv_HandlerMsg
```

(4)算法 6 为 Init_Trust(XS_m)的伪代码。

算法 6 节点 m 信誉分布初始化

输入 XS_m：信任域 A 对 m 节点的推荐信誉分布

输出 XS_m'：信任域 B 对 m 节点的初始化信誉分布

```
  u:=0
  v:=0
  if XS_m is NULL then
        XS_m':=(0.5, 0.5*0.5)
  else
        u:=0.5 + XS_m[0]
        v:=0.5*0.5 + beta*XS_m[1]*XS_m[1]
        XS_m':=(u,v)
  end if
  return XS_m'
```

(5)在节点 m 与信任域 B 的交互过程中，B 通过算法更新节点 m 的信誉分布。系统算法流程如图 4 所示。

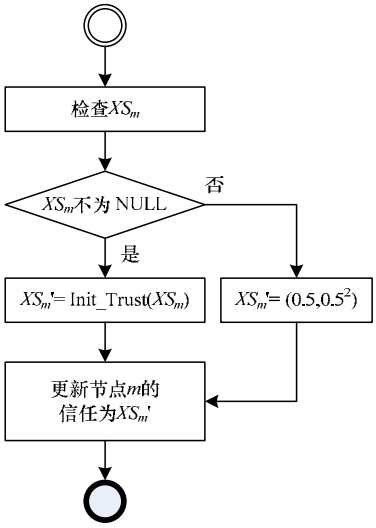

图 4　移动节点 m 初始化流程

3　仿真分析

为验证本文提出观点的有效性，在 TOSSIM 仿真环境下[14]，部署 2 个信任域 A、B，共 101 个节点，每个信任域有 50 个节点，节点 m 为移动节点，数据包以多层树状结构形式沿着传感器节点向基站传递，每个节点使用一个看门狗来监视其邻居节点的行为。实验分为 2 个阶段：第 1 阶段假定初始时各节点信誉服从 $N(0.5,0.5^2)$，每个时段节点 m 的邻节点 i 向 m 发送 100 个数据包，假设发送数据包的事件相互独立，节点 i 测试节点 m 转发数据包的情况并计算节点 m 的信誉分布 $N(\mu_1,\sigma_1^2)$；第 2 阶段节点 m 向信任域 B 进行迁移，初始化时信任迁移的高斯模型(T-GRFSN)的信誉服从 $N(0.5\times0.5+0.5\mu_1,0.5^2\times0.5^2+0.5^2\cdot\sigma_1^2)$ 而高斯分布模型(GRFSN)服从 $N(0.5,0.5^2)$，节点 m 的邻节点 j 以第 1 阶段节点 i 相同的行为模式分别计算在 2 种信任模型下节点 m 的信誉分布。第 1 阶段与第 2 阶段中间的 1 个时段，节点 m 完成从 A 到 B 的移动及身份的验证，由于 T-GRFSN 与 GRFSN 都需要与服务中心进行通信，因此 2 种模型中移动节点与服务中心之间的通信开销间的差别可以忽略。

3.1　信誉收敛速度

在持续合作的情况下，选定阈值为 0.95。如图 5 所示，第 1 阶段信任迁移的 T-GRFSN 与 GRFSN 具有相同的初始信誉分布，因此 T-GRFSN 与 GRFSN 有相同的信誉计算收

敛速度。第 2 阶段 GRFSN 经过 5 个时段信誉达到 0.95 左右水平，而 T-GRFSN 经过 4 个时段信誉值就达到 0.95 左右的水平。由于 T-GRFSN 的初始信誉比 GRFSN 更接近真实情况，因此 T-GRFSN 在连续合作的情况下信誉计算收敛速度大于 GRFSN。

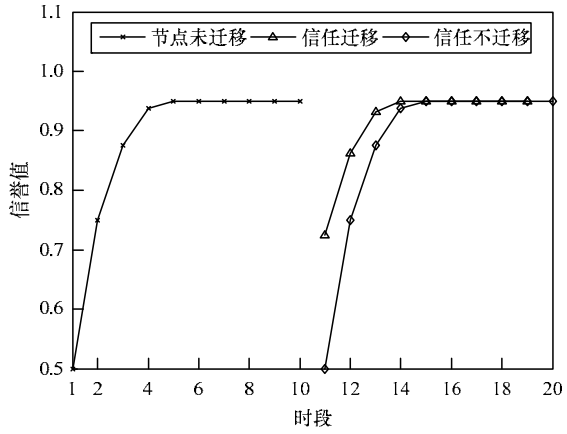

图 5 节点迁移前后合作信任值变化

在持续不合作的情况下，选定阈值为 0.08。如图 6 所示，第 1 阶段 T-GRFSN 与 GRFSN 具有相同的信誉计算收敛速度。第 2 阶段 GRFSN 经过 3 个时段信誉达到 0.08 左右水平，而 T-GRFSN 只经过 2 个时段信誉值就达到该水平。因此，T-GRFSN 在连续不合作的情况下信誉计算收敛速度大于 GRFSN。

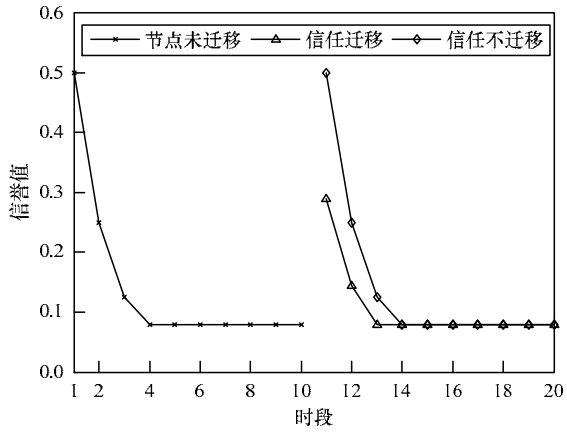

图 6 节点迁移前后不合作信任值变化

3.2 恶意节点能力检测

若移动节点 m 为在历史上伪装成一个信誉优良的节点，假设在信任域 A 中，节点 m 的信誉水平达到 0.95，在新的信任域 B 中，经过信誉初始化计算，其信誉水平达到 0.72。假设阈值为 0.08，节点 m 的相邻节点 j 测试 m 转发数据包的情况，如图 7 所示，m 多次转发失败，节点 m 对节点 j 的信誉呈下降趋势(时段 12~17)，当信誉下降到阈值以下时，节点 j 将节点 m 归类为恶意节点，节点 j 隔离节点 m(时段 18、19)。根据文献[15]的 CORE 协议，在每个时段开始时节点 j 会以一定的概率让节点 m 重新加入。因此，T-GRFSN 具有检测恶意节点的能力。

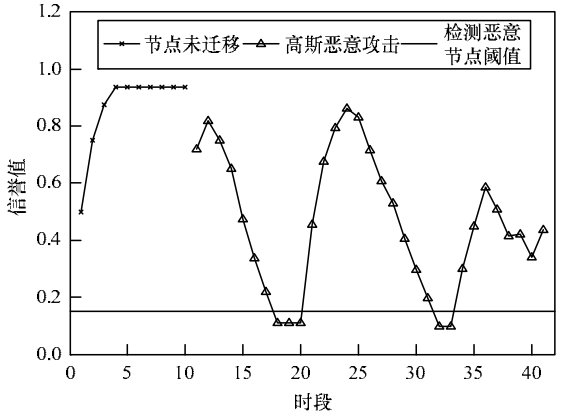

图 7 恶意节点攻击时的信任变化

4 结束语

本文根据物联网的特点，结合无线传感器网络的 GRFSN 模型，探讨了一种基于高斯分布的物联网信任体系，在这种体系中引入移动节点历史所在信任域对现在所在信任域的推荐信誉，并给出移动节点历史信任的更新和请求的流程以及物联网前端网络信任初始化、信任更新和信誉采样的算法。仿真结果表明，这种推荐能加快移动节点的信誉计算的收敛速度，并具有传统 GRFSN 模型能够检测恶意节点的能力。当然，本文所讨论的体系也有不足之处，首先没有考虑恶意推荐的情况，其次没有考虑信任域之间使用异构信誉模型的情况，这是下一步的研究方向。

参考文献

[1] Atzori L, Iera A, Morabito G. The Internet of Things: A Survey[J]. Computer Networks, 2010, 54(15): 2787-2805.

[2] Weber R H. Internet of Things——New Security and Privacy Challenges[J]. Computer Law & Security Review, 2010, 26(1): 23-30.

[3] International Telecommunication Union. ITU Internet Reports 2005: The Internet of Things[R]. Tunis: ITU, 2005.

[4] 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议[J]. 中国科学: 信息科学, 2012, 42(7): 815-830.

[5] 张 坤. 移动业务中基于信任计算的RBAC模型应用研究[D]. 北京: 北京交通大学, 2011.

[6] Lopez J, Roman R, Agudo I, et al. Trust Management Systems for Wireless Sensor Networks: Best Practices[J]. Computer Communications, 2010, 33(9): 1086-1093.

[7] 肖德琴, 冯健昭, 周 权, 等. 基于高斯分布的传感器网络信誉模型[J]. 通信学报, 2008, 29(3): 47-62.

[8] 沈苏彬, 范曲立, 宗 平, 等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报: 自然科学版, 2009, 29(6): 1-11.

(下转第 108 页)

约为 –7 dB□ –2.5 dB时有更好的性能。误比特率达到 10^{-4} 时，RLS 算法相对于 LMS 算法有 0.3 dB 的改善，同时随着信噪比增大，LMS 算法和 RLS 算法均有改善，当信噪比在 −2.5 dB 左右，两者对水声系统的影响没有差异。表明优化的 RLS 算法适用于低信噪比的时变水声信道的通信系统。

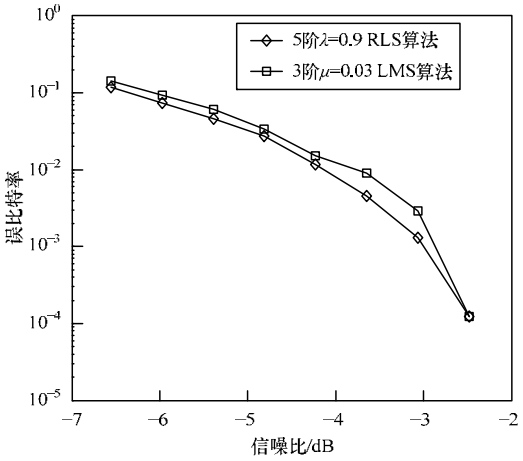

图 6 优化水声系统中的算法性能比较

4 结束语

本文基于 DQPSK 软解调的时变水声系统提出了优化均衡技术系统参数。针对水声通信系统的特点，首先研究了 DQPSK_SISO 软解调软译码算法、衰减损失和海洋噪声；然后通过仿真分析了 LMS 和 RLS 算法在时变水声系统中不同步长、阶数的收敛速度；最后在最佳自适应均衡器参数的条件下研究 2 种算法对此系统性能的影响。实验结果表明，本文提出的优化自适应均衡方案能在低信噪比条件下使得系统误码率性能大幅度提升，即使不同参数和算法系统的性能略有不同，也能满足时变水声系统传输要求。

参考文献

[1] Hewavithana T C, Mike B. Soft Decisions for DQPSK Demodulation for the Viterbi Decoding of the Convolutional Codes[C]//Proc. of IEEE International Conference on Acoustics, Speech, and Signal Process. [S. 1.]: IEEE Press, 2003.

[2] Zhang Shuai, Li Jianping. A Variable Iterative Decoding Scheme for BICM_ID Based on Cross-entropy[C]//Proc. of WCSP'09. [S. 1.]: IEEE Press, 2009.

[3] Lu B, Yue Guosen, Wang Xiaodong. Performance Analysis and Design Optimization of LDPC-coded MIMO OFDM Systems[J]. Signal Processing, 2004, 52(2): 348-361.

[4] Tian Xinjin, Li Lin. An Optimized Symbol Mapping of 8PSK Modulation for BICM_ID in Low SNR[J]//Proc. of IEEE, Artificial Intelligence, Management Science and Electronic Commerce. [S. 1.]: IEEE Press, 2011.

[5] Chen Jinghu, Dholakia A. Reduced-complexity Decoding of LDPC Codes[J]. IEEE Transactions on Communications, 2005, 53(7): 12-32.

[6] 袁东风, 张海刚. LDPC 码理论与应用[M]. 北京: 人民邮电大学出版社, 2008.

[7] Zhang Huaqiong, Zhang Lulu. A New Interleaver Design for BICM-ID[C]//Proceedings of IEEE CCCM'10. [S. 1.]: IEEE Press, 2010: 461-464.

[8] Song Aijun, Badiey M. Generalized Equalization for Underwater Acoustic Generalized Equalization for Under-water Acoustic[C]//Proc. of IEEE OCEANS'05. [S. 1.]: IEEE Press, 2005.

[9] Stojanovic M, Freitag L, Johnson M. Channel Estimation-based Adaptive Equalization of Underwater Acoustic Signals[C]//Proc. of OCEANS'99. [S. 1.]: IEEE Press, 1999.

[10] 程小亮. 衰落信道上信道估计、均衡与相干检测技术研究[D]. 南京: 南京航空航天大学, 2006.

编辑 索书志

(上接第 104 页)

[9] Al-Jaroodi J, Jawhar I, Al-Dhaheri A. Security Middleware Approaches and Issues for Ubiquitous Applications[J]. Computers and Mathematics with Applications, 2010, 60(2): 187-197.

[10] Gadallah Y, Serhani M A, Mohamed N. Middleware Support for Service Discovery in Special Operations Mobile Ad Hoc Networks[J]. Journal of Network and Computer Applications, 2010, 33(5): 611-619.

[11] 马新新, 耿 技. 对等网络信任和信誉机制研究综述[J]. 计算机应用, 2007, 27(8): 1935-1941.

[12] Yu Yanli, Li Keqiu, Zhou Wanlei, et al. Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures[J]. Journal of Network and Computer Applications, 2012, 35(3): 867-880.

[13] 俞 靓, 王志波, 骆吉安, 等. 面向移动目标追踪的无线传感器网络 QoS 指标体系设计[J]. 计算机学报, 2009, [32(3): 442-462.

[14] 孙发军, 吴 昊. 一个基于 TOSSIM 的异构传感器网络仿真方案[J]. 计算机仿真, 2007, 24(10): 126-130.

15] Michiardi P, Molva R. Core: A Colaborative Reputation Mechanism Toenforce Node Cooperation in Mobile Ad Hoc Networks[C]//Proc. of Communication and Mutimedia Security Conference. Portoroz, Slovenia: [s. n.], 2002.

编辑 金胡考