基于 Core-Selecting 机制的物联网安全路由协议①

夏有华, 林 晖, 许 力, 周赵斌

(福建师范大学 数学与计算机科学学院, 福州 350007)
(福建师范大学 福建省网络安全与密码技术重点实验室, 福州 350007)

摘 要: 设计安全的路由协议以确保网络与隐私信息安全是物联网面临的一个巨大挑战, 提出了一种 Core-Selecting 机制, 并将该机制应用于物联网路由协议设计, 在此基础上设计并实现了一种新的物联网安全路由协议 PALXC, 有助于抵御合谋攻击和选出可信路由. 理论分析和仿真实验结果表明了所设计的协议的有效性.

关键词: 物联网; 网络安全; 路由协议; Core-Selecting 机制

Core-Selecting Mechanism Based Secure Routing Protocol for Internet of Things

XIA You-Hua, LIN Hin, XU Li, ZHOU Zhao-Bin

(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China)
(Fujian Province Key Laboratory of Network Security and Cryptography, Fujian Normal University, Fuzhou 350007, China)

Abstract: Designing a secure routing protocol to ensure the privacy of information and network security is a huge challenge of Internet of Things. In this paper, a new Core-Selecting mechanism is proposed, and the mechanism is applied to the design of routing protocol for the Internet of Things. Based on this, we designed and implemented a new secure routing protocol named PALXC for Internet of Things, which can help to resist internal collusion attack and select trusted route. Theoretical analysis and simulation experiment results show the effectiveness of the designed protocol.

Key words: internet of things; network security; routing protocol; core-selecting mechanism

物联网是一种实现任何事物与互联网连接, 进行信息交换和通信, 以实现智能化监控和管理等的新型网络[1]. 物联网的安全架构如图 1 所示, 包括身份安全、数据安全、控制和行为安全、感知层安全、网络层安全、中间件层安全和应用层安全等.

物联网应用范围的不断扩大, 使得大量信息将出现在网络中[2], 这些信息的泄露将对国家、社会以及个人造成重大的影响. 因此, 保证物联网的网络信息安全是物联网需要重点关注的问题之一[3].

路由协议作为物联网的一个重要组成部分, 用于寻找从源节点到目的节点的最优路径. 路由过程的数据中包含了许多安全和隐私相关的信息, 因此, 针对路由协议的攻击一直是物联网面临的一个严重的安全威胁. 目前, 物联网中的安全路由协议主要直接从传感器网络, Ad Hoc 网络等传统网络中移植而来, 无法完全适用于物联网, 因此设计能够满足物联网特点, 又可以保障网络和信息安全的新型物联网安全路由协议显得尤为重要.

1 相关工作

物联网中的路由协议正在成为研究热点, 涌现出了一些研究成果. Sharief[5]等针对物联网的多样性提出了路由协议 PAIR, 并用一个代价模型来适应物联网的多样性需求. Kassio Machado[6]等提出了路由协议 REL 来适应物联网的应用. 它主要考虑链路的连接质量, 剩余能量和跳数来选出最佳路由路径. Sudip Misra[7]等提出了一个混合跨层和自适应学习的容错路由协议应用于物联网之中, 在有错误的情况下, 确保了数据包的成功传输, 具有高可扩展性, 可以动态的适应变化的环境. Ying Lu[8]等用蚁群算法在物联网中寻找路由

① 基金项目:国家自然科学基金(61202450,61363068,61472083);福建省教育厅 A 类科技项目(JA15121)
收稿时间:2015-08-17;收到修改稿时间:2015-11-02

路径, 具有随机多发和短生命周期特点的广播信号, 克服了更多的网络节点和多变量网络结构问题.

目前物联网安全路由协议的研究还不多见. Liu[9]等考虑了一种基于团结构的设施策略异构可信路由, 应用于异构转发策略的网络中, 减少了路由发现开销, 并且避免了因不兼容策略造成的路由失效问题. Zhang[10]等提出了一种上下文感知优化链路状态路由协议 CAOLSR(Context-aware optimized Link State Routing Protocol), 该协议采用了一种上下文信息机制, 将节点间相对移动预测、前后访问时间以及节点连接度情况引入 MPR (Multi Point Relays)选择, 使其在节点快速移动与拓扑快速变化环境下比其他协议具有更为良好的性能和安全保障. Zhou[11]等以保障网络总体安全性能为首要目标, 提出了一种可抵抗干扰攻击的安全路由协议 SRRJ (Secure Routing Resilient to Jamming). SRRJ 协议通过引入切换通信模式, 实现了对干扰攻击的有效抵御.

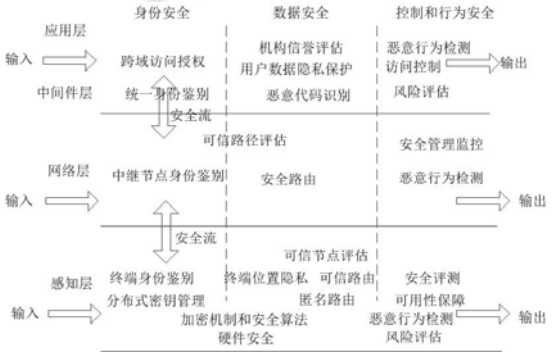

图 1 物联网安全架构[6]

现有的研究成果虽然能提供一定的性能优化和路由安全保障, 但是无法实现对合谋攻击的有效抵御.

针对上述问题, 本文将 Core-Selecting 机制[12]引入物联网安全路由协议的设计中, 并结合节点可信度的评估, 提出了一种新的物联网安全路由协议 PALXC, 在确保能够选取出一条可信路由的同时, 实现了对内部合谋攻击的有效防御.

2 系统和攻击模型

2.1 系统模型

本文研究采用的是传感器物联网系统结构, 如图 2 所示, 该系统结构主要由 9 个节点组成, 源节点是 N_0, 目的节点是 N_8, 节点 N_3 和 N_4 联盟发动合谋攻击, 将数据包转发的权利转移到自己手中, 并依据自己的需求将数据包转发给下一跳节点.

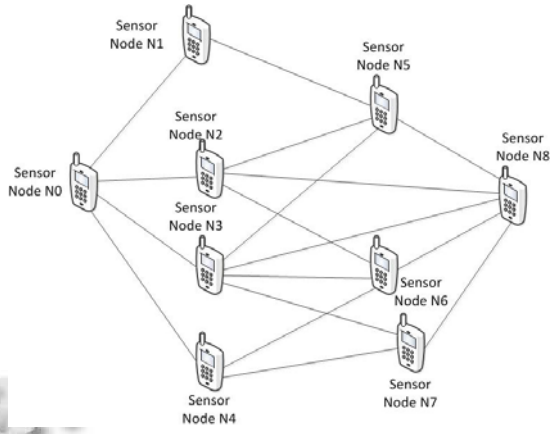

图 2 传感器物联网系统结构

2.2 攻击模型

本文主要考虑内部合谋攻击. 合谋攻击是指两个或两个以上的恶意节点通过联盟进行攻击[13]. 合谋攻击除具备一般攻击的基本特性外, 还具备以下 3 个特点: (1)互相担保, 使攻击节点看似合法节点; (2)互相伪装, 建立虚假链路; (3)作伪证陷害合法节点.

3 动态信誉机制

动态信誉机制是一种可以对节点的信誉度进行动态实时评估的信誉机制. 在动态信誉机制中, 节点的信誉度和节点间的信任关系不仅取决于当前的评估结果, 也与距离最近一次评估的时间间隔相关[15], 节点的动态信誉度可以通过以下四种方式进行评估:

1) 直接信誉度评估: 根据和邻居节点的交互情况, 给出邻居节点的信誉度值.

2) 间接信誉度评估: 根据对邻居节点的信任程度, 给出和该节点不相邻, 而和其邻居节点相邻的节点的信誉度值.

3) 动态信誉度评估: 节点信誉度评估和上一次评估的时间间隔有关, 时间间隔越长, 节点的信誉度评估值越小.

4) 综合信誉度评估: 由节点在 t_i 时刻和 t_n 时的信誉度评估值按一定的权重分配求和给出节点的综合信誉度评估值.

4 Core-Selecting机制

Core-Selecting 机制是一种可以解决 VCG 机制中

小团体联盟问题的机制, 可以有效防御节点的合谋攻击. Core-Selecting 机制中的 Core 是以集合的形式给出[12], 定义为:

$$Core(N)=\left\{u\geq 0 \mid \sum_{i\in N}u_i=WD(N),\sum_{i\in C}u_i\geq WD(C)\right\} \quad (1)$$

其中, u_i 表示用户 i 的收益(在路由协议中, 收益可以是使得节点的信誉值变高), WD 即是 WDP(Winner Determination Problem)问题中的 WD 函数.

WDP 是一个拍卖博弈的问题, 竞价者的集合为: $N=\{1,2,\cdots\cdots,n\}$; 物品的集合为: $M=\{1,2,\cdots\cdots,m\}$; S 为物品子集合, 即 $S\subseteq M$; $v_i(s)$ 表示竞价价格; 物品的分配用 $x_i(s)\in\{0,1\}$ 表示, $x_i(s)$ 为 0 时, 表示物品没有被分配, $x_i(s)$ 为 1 时, 表示物品已被分配. $x_i(s)$ 用于计算最大竞价估值, 满足以下 2 个约束条件, 分别表示被分配的物品和物品的集合不会多于一次.

$$\sum_{i\in N}\sum_{S\subseteq M}x_i(s)\leq 1 \quad (2)$$

$$\sum_{S\subseteq M}x_i(s)\leq 1 \quad (3)$$

依据以上两个条件 WDP 问题可以分成两类, 分别是 WDP_{OR} 和 WDP_{XOR}, 都用于计算最大竞价估值. 其中, WDP_{OR} 是在限制条件中满足公式(2)时的最大竞价估值, 表示为:

$$x\in\arg\max\left(\sum_{i\in N,S\subseteq M}v_i(s)x_i(s)\mid x\text{ 满足(2)}\right)$$

WDP_{XOR} 是在限制条件中同时满足公式(2)和公式(3)时的最大竞价估值, 表示为:

$$x\in\arg\max\left(\sum_{i\in N,S\subseteq M}v_i(s)x_i(s)\mid x\text{ 满足(2) 和 (3)}\right)$$

5 LX-Core机制

本节提出了一种基于 Core-Selecting 机制的 LX-Core 机制. 在 LX-Core 机制中, 定义 WDP 问题中的 WD 函数为:

$$WD(N)=\max\sum_{i\in N}\sum_{S\subseteq N}b_s(i)x_i(s) \quad (4)$$

其中, S 表示联盟节点的集合, N 表示所有节点的集合, i 表示某一个节点, $b_s(i)$ 表示联盟节点 S 对节点 i 给出的信誉推荐值, $x_i(S)$ 表示节点 i 和联盟节点 S 是否处于对数据包转发权的竞争过程中, 如果是, $x_i(S)$ 的值为 1, 如果不是, $x_i(S)$ 的值为 0.

该目标函数的约束条件为:

$$\begin{cases}\sum_{S\subseteq N}x_s(i)\leq 1 & \forall i\in N\\ x_i(k)+x_j(k)\geq 1 & \forall i,j,k\in N\\ x_i(S),x_i(k)\in\{0,1\} & \forall i\in N,\forall S\subseteq M\end{cases} \quad (5)$$

第一个约束条件表明联盟节点只能对其他节点中的一个节点给出推荐信誉值; 第二个约束条件表明多个节点可以对一个节点给出信誉推荐值; 第三个约束条件中, $x_i(S)$ 表明节点 i 和联盟节点 S 处于或不处于对数据包转发权的竞争过程中, $x_i(k)$ 表明节点 i 可以或不可以对节点 k 给出信誉推荐值.

接下来, 我们证明 LX-Core 机制为 Core-Selecting 机制. 一个机制属于 Core-Selecting 机制, 需要满足以下性质:

① 存在联盟团体时的 WD 值小于等于不存在联盟团体时的 WD 值.

② 存在联盟团体时, 成员使用 Core-Selecting 机制获得的收益比使用 VCG 机制获得的收益要小.

定理 1. 在路由选择的过程中, 当有少部分节点发生合谋情况的时候, 就会有关系式 $WD(N)\geq WD'(N)$ 成立, 其中 $WD'(N)$ 是当有合谋情况发生时的 $WD(N)$ 值

证明: 如系统模型图 2 所示, 节点 $N_1,N_2,\cdots\cdots$ 给出的推荐信誉值矩阵为:

$$\begin{bmatrix} - & m_2 & \cdots & m_i & \cdots\\ n_1 & - & \cdots & n_i & \cdots\\ q_1 & q_2 & \cdots & q_i & \cdots\\ p_1 & p_2 & \cdots & - & \cdots\\ \cdots & \cdots & \cdots & \cdots & \cdots\end{bmatrix}$$

各个节点依据其行为重要性的程度划分其权重值分别为: $\alpha_1,\alpha_2,\cdots,\alpha_i,\cdots$ 且 $\alpha_1+\alpha_2+\cdots+\alpha_i+\cdots=1$. 其中每个权重与行为的重要程度成比例, 特定行为的权重越大, 该行为对信任值越重要, 反之亦然.

假设有两个节点 N_i 和 N_k 合谋, 则其他节点对 N_j 和 N_k 给出的信誉推荐值都为: $\alpha_2n_1+\alpha_3p_1+\alpha_4q_1+\cdots-(\alpha_jr_j+\alpha_ks_k)$ (即第一列数值和权重相乘之后再求和减去权重为 α_j 和 α_k 的那两项), 如果节点 N_j 和 N_k 不合谋, 则其他节点分别对 N_j 和 N_k 给出的信誉推荐值为: $\alpha_2n_1+\alpha_3p_1+\alpha_4q_1+\cdots-\alpha_jr_j$ (即第一列数值和权重相乘之后再求和减去权重为 α_j 的那一项), $\alpha_2n_1+\alpha_3p_1+\alpha_4q_1+\cdots-\alpha_ks_k$ (即第一列数值和权重相

乘之后再求和减去权重为 α_k 的那一项). 由于合谋时信誉推荐值多减去了一项, 所以当有合谋情况发生时的推荐信誉值小于不合谋时的推荐信誉值.

上述证明表明: 当有节点合谋时, 就会有关系式 $WD(N)\geq WD'(N)$ 成立, 其中 $WD'(N)$ 是有合谋情况发生时的 $WD(N)$ 值.

定理 2. 当发生合谋情况的时候, 使用 Core-Selecting 机制时被选节点获得的收益不大于使用 VCG 机制时被选节点获得的收益.

证明: 我们用 $\sum u_i$ 表示节点使用 VCG 机制(关于 VCG 机制的详细介绍请参考文献 5)时获得的收益, 用 WD 函数表示节点使用 Core-Selecting 机制时获得的收益. 因为

$$WD'(N\setminus C)=WD(N\setminus C)$$

所以

$$WD(N)-WD'(N\setminus C)=WD(N)-WD(N\setminus C)$$

又由于我们有限制条件

$$\sum_{i\in C}u_i\leq WD'(N)-WD(N\setminus C)$$

根据定理 1 中的

$$WD'(N)\leq WD(N)$$

所以

$$\sum_{i\in C}u_i\leq WD(N)-WD(N\setminus C)$$

又因为

$$\sum_{i\in N\setminus C}u_i=WD(N)-\sum_{i\in C}u_i$$

所以

$$\sum_{i\in N\setminus C}u_i\geq WD(N\setminus C)$$

上述证明表明: 当发生合谋攻击时, 使用 Core-Selecting 机制时被选节点获得的收益小于等于使用 VCG 机制时被选节点获得的收益. 即被选节点采用 VCG 机制时获得的收益会大于等于被选节点采用 Core-Selecting 机制时获得的收益.

6 动态信誉度计算

在LX-Core机制中, 对于节点信誉度的计算采用动态信誉机制中信誉度计算的方法分别计算出节点的直接信誉度、间接信誉度、动态信誉度以及综合信誉度.

6.1 直接信誉度与动态信誉度评估

设 $R_{t_i,u}^{final}$ 为时刻 t_i 关于u的综合信誉度, 该结果保存在v的本地信誉度数据库中. $R_{t_n,u}^{direct}$ 为时刻 t_n 关于 u 的动态直接信誉度. 考虑时间变化对信誉度的影响, $R_{t_n,u}^{direct}$ 将参考 $R_{t_i,u}^{final}$ 的值计算获得.

$$R_{t_n,u}^{direct}=\frac{f_{t_n}^{r}+f_{t_n}^{\xi}}{f_{t_i}^{r}+f_{t_i}^{\xi}}R_{t_i,u}^{final} \tag{6}$$

其中, $f_{t_i}^{r}/f_{t_n}^{r}$ 和 $f_{t_i}^{\xi}/f_{t_n}^{\xi}$ 是时刻 t_i, t_n 节点的信誉度值和可靠性衰变因子.

$$\begin{cases} f_{t_n}^{r}=e^{-\left(\left(R_{t_i}^{final}\right)^{-1}\times\Delta t\right)^{2k}} \\ f_{t_n}^{\xi}=f_{t_i}^{\xi}+\dfrac{\overline{\xi_{(i,x)}^{t_n}}-\overline{\xi_{(i,x)}^{t_i}}}{\xi_{(i,x)}^{t_n}} \\ f_{t_0}^{r}=f_{t_0}^{\xi}=0.5 \end{cases} \tag{7}$$

$$\begin{cases} \overline{\xi_{(i,x)}^{t_i}}=\dfrac{1}{m^{t_i}}\sum_{i=1}^{m^{t_i}}\xi_{(i,x)}^{t_i} \\ \overline{\xi_{(i,x)}^{t_n}}=\dfrac{1}{m^{t_n}}\sum_{i=1}^{m^{t_n}}\xi_{(i,x)}^{t_n} \end{cases} \tag{8}$$

其中, m^{t_i} 和 m^{t_n} 是时刻 t_i, t_n 推荐节点集合 R_{t_i}' 和 R_{t_n}' 中的节点数[13].

6.2 间接信誉度评估

若无 $R_{t_i,u}^{final}$, 或 $R_{t_n,u}^{final}<TH_{\min}^{v}$, 设推荐节点集合为 $R(|R|=\tau)$, 第 i 个推荐意见的权重因子为 f_i, 则 v 将计算 u 的间接信誉度 R_u^{rec}:

$$R_u^{rec}=\sum_{k=1,k\in R}^{\tau}f_k\times R_{t_n,u}^{direct}/\tau \tag{9}$$

6.3 综合信誉度评估

v 按照公式(10)计算 u 的综合信誉度 R_u^{final}:

$$\begin{cases} R_u^{final}=\eta_1\times R_{t_n,u}^{direct}+\eta_2\times R_u^{rec} \\ \eta_1+\eta_2=1,(\eta_1,\eta_2\in[0,1]) \end{cases} \tag{10}$$

其中, η_1 和 η_2 代表节点关于时间对信誉度评估影响的重视程度, η_2 的值越大, 节点越重视时间的影响.

7 PALXC路由协议

本节设计并实现了新的安全路由协议 PALXC. PALXC 主要包括 2 个步骤: 1)路由的建立; 2)路由的维护[13].

1) 路由的建立: PALXC通过源节点构建路由设置消息 SETM 并广播该消息给邻居节点来启动路由建立过程, 路由建立过程包括路由发现和路由响应两个步骤, 具体描述如下:

①首先, 源节点 u 查询本地存放的相关邻居节点的信誉度, 如果存在节点集合 Φ, 集合中的任意一个节点 k 的信誉度值 $R(k)$ 都大于门限值 $THmin$ $(\forall k\in\Phi,R(k)>TH_{\min})$, 则 u 向 Φ 中的节点广播 SETM 消息, 启动路由发现过程.

②任意 Φ 中的节点v收到SETM消息后, v将首先

计算关于u的在当前的t_n时刻的直接信誉度$R^{direct}_{t_n,u}$:

(2a)v广播查询消息给邻居节点, 要求提供u的直接信誉度评估结果, 并等待对方的回应, 等待的时间长为T.

(2b)任意邻居节点k收到查询消息后, 首先在本地信誉度数据库上查询关于u的直接信誉度, 然后启动基于Core-Selecting的LX-Core机制反馈真实的信息给v.

(2c)经过T时刻后, v将收到的所有推荐信息汇总, 计算出关于u的推荐信誉度, 并结合本地所拥有的关于u的直接信誉度计算出最终的u的综合信誉度R^{final}_u.

(2d)如果$R^{final}_u < TH^{final}_{\min}$则$v$认定$u$为不可信节点, v将忽略u的SETM消息, 并将这次计算的R^{final}_u保存在本地信誉度数据库中. 如果u不是恶意节点, 则v将通过计算Winner Determination Problem (WDP) 问题中的WD函数, 启动LX-Core机制来反馈真实的信息.

③若无节点集合Φ或Φ中的节点都没有提供反馈信息, 则u向Φ外的其它邻居节点广播SETM消息.

④任意的其它邻居节点k'收到SETM消息后, 将执行(2)中的内容对u的信誉度进行评估判断u是否为可信节点, 并最终决定是否为u提供中继服务.

⑤ u收到邻居节点的反馈信息后, 将综合考虑跳数信息d_i和节点的信誉度值信息b_i, 利用以下公式计算并选取出合适的下一跳节点.

$$\begin{cases} L = Max\left(m * d_i + n * b_i\right) \\ m + n = 1 \\ m > n \\ Th_1 < b_i < Th_2 \end{cases} \tag{11}$$

⑥每个节点反复执行步骤2、3、4和5, 直到找到一条最优的路径.

⑦目的节点收到路由发现的消息以后, 它将沿路由发现消息所经过的路径, 返回一个PREP消息给源节点来启动路由响应过程, 直到源节点收到这个PREP消息.

2)路由的维护: PALXC采用信道感知策略实现路由路径的维护, 详细过程见文献[14].

8 仿真实验与性能分析

本文使用MATLAB 对PALXC协议的可信度和抗合谋攻击能力进行仿真实验和性能分析.

8.1 仿真环境

仿真中选择了以下 4 种指标来比较和分析 PAIR 协议和 PALX[15]协议的性能.

(1)恶意节点识别率 (MIR): 路由维护和数据转发过程中被准确地识别出的恶意节点的数量与恶意节点总数的比值;

(2)分组传输率 (PTR): 目的节点接收到的数据包的数量与源节点发送的数据包的数量的比值, 体现了网络从源节点到目的节点的数据包传输的有效性, 值越大越好;

(3)传输时延 (TD): 从开始发送数据包到数据包发送完毕所需要的时间减去接收数据包的时间的差, 同发送数据包的时间的比值;

(4)恶意节点参与率 (MPR): 路由过程中未被识别和检测出, 成功的成为路由路径上的转发节点的恶意节点的数量与恶意节点的总数的比值;

8.2 信誉机制性能分析

首先, 我们比较 LX-VCG 机制和 LX-Core 机制的恶意节点识别率 MIR, 从图 3 中可以看出随着时间的增加, MIR 随之增加, 其中 LX-Core 机制要比 LX-VCG 机制要增加的大. 在起初, 由源节点发出消息, 此时恶意节点很少或者是还未参与进来, 所以识别率较低, 但是随着路由发现的过程, 一些恶意节点出现了, 所以采用了可以防御合谋攻击的 Core-Selecting 机制的 LX-Core 机制要比 LX-VCG 机制的恶意节点识别率要高.

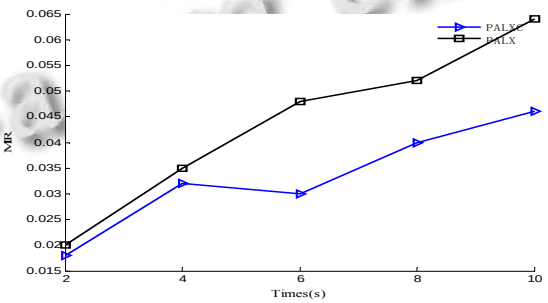

图 3　恶意节点识别率

8.3 路由协议性能分析

接下来, 比较三种协议的分组传输率和传输时延.

分组传输率的仿真结果如图 4 所示, 从图 4 中可以看出随着时间的增加, PALXC 路由协议的分组传输率变化不大, 而 PAIR 路由协议和 PALX 路由协议的分组传输率则随着时间的增加而减少, 由于 PALXC 路由协议使用了动态信誉度计算的方法和 Core-Selecting

机制, 可以防御合谋攻击, 所以目的节点接受数据包的数量变化不大, 故而分组传输率比较高; PALX 路由协议由于防御不了合谋攻击, 只能防御欺骗攻击和诽谤攻击, 所以其目的节点接收数据包的数量会有所下降; PAIR 路由协议有代价函数可以抑制代价的损耗, 但是缺乏安全机制来防御合谋攻击, 所以其分组传输率最低.

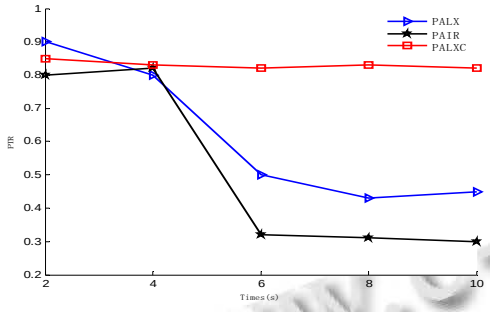

图 4 分组传输率

传输时延的数值仿真结果如图 5 所示, 从图 5 中可以看出随着时间的增加, PALXC 路由协议和 PALX 路由协议以及 PAIR 路由协议在起初变化不大, 随着路由过程的进行, PALX 路由协议和 PAIR 路由协议的传输时延开始增加, 但是 PALXC 路由协议由于采用了 Core-Selecting 机制可以抵御合谋攻击以及可以进行可信路由的选取, 传输时延发生了轻微的变化; PALX 路由协议不能抵御合谋攻击但是可以抵御网络节点中的欺骗攻击, 所以其传输时延有所增加; PAIR 路由协议虽然可以使满足不同需求和条件的节点在不使用骨干互联网的情况下就可以转发数据包, 但是缺乏一定的安全机制, 所以其传输时延增加的最大.

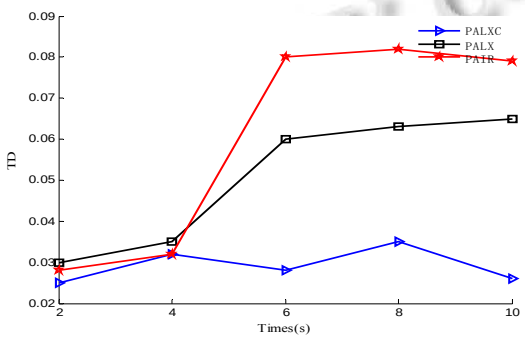

图 5 传输时延

8.4 安全性能分析

PALXC 路由协议除了在路由协议性能方面有一定程度的提升, 在路由安全方面也有所提高[17], 以下是我们对路由选择过程中, 恶意节点参与率的比较结果.

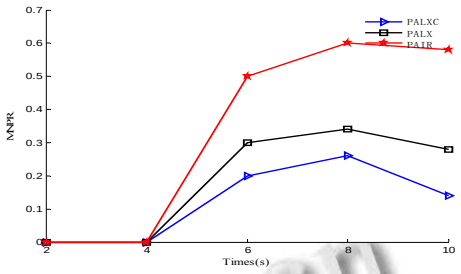

图 6 恶意节点参与率

从图 6 中我们可以看出, 随着时间的增加, 三种路由协议的恶意节点参与率在起初都没有恶意节点加进来, 所以其恶意节点参与率为零. 但是随着路由过程的进行, 会有恶意节点参与到路由选择的过程中来, 由于 PALXC 路由协议可以抵御合谋攻击, 并进行可信路由的选取, 所以恶意节点参与到其路由过程中的概率很小, 而 PALX 路由协议可以抵御欺骗攻击和诽谤攻击, 所以恶意节点参与到其路由过程中的概率次之, 但是 PAIR 路由协议缺乏一定的安全机制防御节点的攻击行为, 所以恶意节点参与到其路由过程中的概率最高.

9 总结

如何在路由过程中抵御节点的合谋攻击是物联网中的一个关键问题. 本文首先基于 Core-Selecting 机制设计出新的机制 LX-Core 机制, 并分析了该机制的有效性, 然后结合动态信誉机制选出一条可信的路由. 数值仿真分析表明该协议在有攻击的情况下, 本文提出的 PALXC 路由协议在分组传输率和传输时延以及恶意节点参与率、平均跳数等方面都要优于现有的 PAIR 路由协议和 PALX 路由协议, 有效的提高路由过程中的安全性能和隐私保障性能.

参考文献

1 Bandyopadhyay D, Sen J. Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 2011, 58(1): 49–69(21).

2 Babar S, Stango A, Prasad N, Japdip S, Prasad R. Proposed embedded security framework for internet of things (iot). 2011 2nd International Conference on Wireless

Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). IEEE. 2011. 1–5.

3 Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. Internet of Things Journal IEEE, 2014, 1(1): 22–32.

4 Liu Y, Zhou G. Key technologies and applications of internet of things. 2012 Fifth International Conference on Intelligent Computation Technology and Automation (ICICTA). IEEE. 2012. 197–200.

5 Sharief MA, Oteafy FM, Al-Turjman, Hassanein HS. Pruned adaptive routing in the heterogeneous internet of things. Global Communications Conference (GLOBECOM), 2012. IEEE. 2012. 214–219.

6 Machado K, Rosario D, Cerqueira E, Loureiro AAF, Neto A, de Souza JN. A routing protocol based on energy and link quality for internet of things applications. Sensors, 2013, 13(2): 1942–1964.

7 Misra S, Krishna PV, Harshit A, Gupta A, Obaidat MS. An adaptive learning approach for fault-tolerant routing in internet of things. Wireless Communications and Networking Conference (WCNC), 2012. IEEE. 2012

8 Lu Y, Hu W. Study on the application of ant colony algorithm in the route of internet of things. International Journal of Smart Home, 2013, 7(3): 365–374.

9 刘文懋.物联网感知环境安全机制的关键技术研究[博士学位论文].哈尔滨:哈尔滨工业大学,2013.

10 张可,张伟,李炜,曾家智.快速移动环境中上下文感知优化链路状态路由协议.计算机科学, 2011,38(6):110–113.

11 周晓芳.无线传感器网络中路由协议的跨层设计研究[博士学位论文].合肥.中国科学技术大学,2010.

12 Zhu Y, Li B, Fu H, Li Z. Core-selecting secondary spectrum auctions. IEEE Journal on Selected Areas in Communications, 2014, 32(11): 2268–2279.

13 Nasser N, Chen Y. SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. Computer Communications, 2007, 30(11): 2401–2412.

14 林晖.无线 Mesh 网络中基于信誉机制的安全路由协议研究[博士学位论文].西安:西安电子科技大学,2013.

15 Joshi P. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 2011, 3: 954–960.

16 Deswarte Y, Powell D. Internet security: An intrusion-tolerance approach. Proc. of the IEEE, 2006, 94(2): 432–441.

17 Lundberg J, Lundberg J. Routing Security in Ad Hoc Networks[Thesis]. Helsinki University of Technology, 2001: 329–354.