文章编号: 1001-0920 (2011) 05-0797-04

一种基于 Mobicast 的最优 QoS 安全认证算法

靳 京, 秦志光, 王佳昊

(电子科技大学 计算机科学与工程学院，成都 611731)

摘 要: 为保证无线传感器追踪网络 (WSTNs) 移动组播服务质量 (QoS) 和安全性, 在 Mobicast 协议基础上提出一种最优 QoS 安全认证算法, 将被监测实体运动速度与组播应用服务需求相关参数向量化, 并在其基础上得出满足最优 QoS 的多级 μTESLA 认证协议级数 M 的函数表达式. 分析和仿真结果表明, 该算法能够对达到特定 QoS 需求所需的相应安全认证密钥级数进行有效分析和预测, 且对于网络能耗和通信实时性的影响是可以接受的.

关键词: 多级 μTESLA；安全认证；服务质量；移动组播；无线传感器追踪网

中图分类号: TP393 **文献标识码:** A

Mobicast-based optimal QoS secure authentication algorithm

JIN Jing, *QIN Zhi-guang*, *WANG Jia-hao*

(School of Computer Science and Engineering，University of Electronic Science and Technology of China，Chengdu 611731，China. Correspondent：JIN Jing，E-mail：jzd7508@163.com)

Abstract: To ensure the quality of service(QoS) and security of mobile multicast in the wireless sensor tracking networks(WSTNs), an optimal QoS secure anthentication algorithm is presented, which makes the speed of the monitoring entity and relevant parameters of multicast applications to vectorization. Furthermore, the level number M of the authentication protocol and the multi-level μTESLA meeting with the optimal QoS are derived. The analysis and simulation results show that this algorithm can analyze and predict effectively the corresponding key level of authentication under the certain QoS requirements, and the impact on network energy consumption and real-time communication is acceptable.

Key words: multi-level μTESLA；secure authentication；quality of service；mobile multicast；wireless sensor tracking networks

1 引 言

现有的无线传感器追踪网络 (WSTNs) 移动组播协议 (如 Mobicast[1])具有良好的能效、追踪预测精度, 以及时空约束保证性能. 然而在其通信过程中存在一定的安全问题, 例如: 在组播会话过程中没有任何身份认证机制, 无法提供安全通信保证, 极大地限制了其在入侵者追踪或战场信息侦察等安全领域的应用. 因而急需引入高效的安全认证机制, 优化和改善移动组播安全性能, 以适应那些对服务质量 (QoS) 要求较高的监控应用.

将多级 μTESLA[2]与改进后的 Mobicast 协议相结合, 是一种比较有效的解决办法. 动态分簇安全移动组播方案 (DCSMS)[3]的分簇移动组播监控形式巧妙地解决了多级 μTESLA 协议在密钥管理时对基站过于依赖的不足; 同时, 多级 μTESLA 协议的分级密钥生成机制也高效地保障了簇内节点组播通信的可靠性.

然而移动组播 QoS 中相关参数的取值与多级 μTESLA 的级数存在一定的制约关系. 当级数 M 增加时, 与认证相关的各种任务量也会随之增多, 并将对组播 QoS 产生影响. 因此对于追踪应用而言, 如何确定能够保证最优 QoS 的密钥级数 M 也是一个非常关键的问题.

本文提出一种最优 QoS 安全认证算法, 将移动组播 QoS 需求向量化, 进而给出多级 μTESLA 级数 M 与相关 QoS 参数的函数表达关系, 可以方便地得出使 QoS 达到最优时所需的 M 值. 通过理论分析和仿真模拟, 验证了算法的低耗性和有效性.

2 相关工作

现有 Mobicast 安全路由协议中大多着眼于组密

收稿日期: 2010-04-11；**修回日期:** 2010-07-20.

基金项目: 国家自然科学基金项目(60903157).

作者简介: 靳京(1975−), 男, 博士生, 从事网络信息安全、无线传感器网络等研究；秦志光(1956−), 男, 教授, 博士生导师, 从事计算机应用、信息安全等研究.

钥分配[4-5]和管理[6-7], 没有从组播机制和构架的层面实现突破, 而且基本是在静态分组的条件下实现, 因而不适用于对QoS要求较高的监控应用.

μTESLA[8]是专门为传感器网络中严格信息源约束环境提供认证广播的一种流认证协议. 由于在源认证中所需载荷过多, 且保证生存周期的密钥链效率不高, 不适用于大规模无线传感器网络.

LIU 等针对该问题提出了多级 μTESLA 协议. 它在源认证初始化过程中能够大大减少能耗和时间延迟的需求. 由于其减少了密钥链的长度, 安全系统的存活期也成倍提高; 同时, 对于DoS等多种攻击的抵御能力也大大加强, 因而非常适用于安全移动组播应用中[3].

DCSMS 对 Mobicast 协议作出了改进, 从结构和路由机制上对QoS加以保障; 同时, 与多级 μTESLA 协议完美结合, 在一定程度上提高了组播通信的安全性. 然而DCSMS并没有分析多级密钥管理与QoS的相互关系, 对QoS的最优化分析指导不够.

目前, 包括DCSMS在内的现有WSTNs应用QoS有关的研究中, 大多只着眼于某几个性能指标, 而且针对某种特定应用的特定分析, 在宏观上缺乏通用的抽象分析理论, 对QoS进行综合把握.

3 最优 QoS 安全认证算法

多级 μTESLA 成倍地提高了流认证的安全性和效率. 但当级数 M 增加时, 相应的伪随机操作、相邻密钥链生成以及消息认证码(MAC)和递交分布消息(CDM)等消息处理与传递的任务量也会随着增多, 进而对组播时间延迟、网络节点能耗等产生影响.

对于追踪应用QoS而言, 其级数并非越高越好. 本节提出一种最优QoS安全认证算法, 用来描述多级 μTESLA 中级数 M 与QoS各种参数之间的制约关系. 在应用中相关参数需求确定时, 即可求出使QoS达到最优的多级 μTESLA 的相应级数.

最优QoS安全认证算法包含两个部分: 自感知QoS需求算法和最优QoS多级 μTESLA 级数分析算法. 前一个算法智能地将实体运动速度与组播应用服务需求相关参数向量化; 后一个算法在其基础上得出了满足最优QoS的多级 μTESLA 级数 M.

3.1 自感知 QoS 需求算法

3.1.1 QoS 算法基本需求

QoS算法的基本需求是使一个组播会话包从forwarding簇内节点产生后, 在消耗最少能量的前提下, 以最短的时间、最可靠的方式传送到应用层.

网络QoS需求是随着时间的变化而不断变化的. 为保证信息传递的最佳效果, 需要将不同状态的各种性能参数选出的最能保证应用需求的若干方面加以综合利用, 比如组播树复杂度、节点传递跳数、通信带宽、监测信息采集量等. 因而, 计算在某一时刻为满足应用需求的即时QoS量是必需的.

3.1.2 应用需求向量表

不同的应用对于数据传递的需求(即QoS)重点是不同的. 比如有的是能量优先, 有的是实时性优先, 或是可靠性优先. 因而, 首先根据QoS应用的特点, 确定一组一维QoS需求向量表

$$\mathrm{QoS}(A)=(\mathrm{QoS}_1[w_1],\mathrm{QoS}_2[w_2],\cdots,\mathrm{QoS}_m[w_m]),\quad(1)$$

其中 $\sum_{i=1}^{m}W_i=1$.

实际上, 这组向量表明了满足应用需求时各参数不同的权重.

3.1.3 算法描述

每个节点将自身当前状态参数值发送给簇头节点, 以一组一维 m 元向量 $\langle E_n,M_n,B_c,T_p,\cdots\rangle$ 表示, 其中 $E_n,M_n,B_c,T_p,\cdots$ 分别表示节点能量、存贮空间、通讯带宽和拓扑信息等QoS相关参数. 簇头节点收到 n 个成员节点状态参数后, 将所有信息保存为一个 $n\times m$ 矩阵 $T(t)$.

QoS需求算法最终要得出某时刻保证及时准确地传送到应用层的最关健的一个或多个参数项, 因此该算法可抽象为一个矩阵转化的数学模型. 即: 将一个 $n\times m$ 矩阵与实体的即时速度 V 相匹配, 并与应用需求向量相匹配, 最终得到一个最优序列值.

3.1.4 算法分析

在QoS算法中加入参数 V (实体运行速度), 当速度较低时Mobicast稳定期较长, 节点运算时间充足, 精度将提高; 当速度较高时, 应降低数据运算量, 在牺牲一定计算精度的前提下保证追踪的实时性.

簇内节点当前状态矩阵为

$$T(t)=\begin{bmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\ \vdots&\vdots&\ddots&\vdots\\ a_{m1}&a_{m2}&\cdots&a_{mn}\end{bmatrix},\quad(2)$$

单位速度QoS需求矩阵为

$$E_{\mathrm{QoS}}=\begin{bmatrix}\mathrm{QoS}_1&&0\\ &\ddots&\\ 0&&\mathrm{QoS}_m\end{bmatrix}.\quad(3)$$

当前速度所需QoS指标阵与应用需求向量阵QoS(A)匹配, 从而得出最佳QoS需求序列阵

$$\mathrm{QoS}(t)=T(t)\cdot\mathrm{QoS}(A).\quad(4)$$

各项指标中与各节点当前状态的最小差值即为当前最佳入簇阈值, 即

$$\min\{T(t)-V(t)E_{\mathrm{QoS}}\}. \tag{5}$$

3.2 最优 QoS 多级 μTESLA 级数分析算法

由文献[2]可知, 针对不同的基站特点, 多级 μTESLA 有 3 种相应的变体. 在 Mobicast 会话过程中, 临时基站的角色都是由普通节点来充当, 数量可以很多, 但其资源却严重受限. 因而, 可选择杂交多级 μTESLA 作为本算法的理论基础.

3.2.1 算法描述

根据杂交多级 μTESLA, 可得出当级数为 M 时各种 QoS 相关参数的表达式 $f_k(M)$, 由此可得出 M 与不同参数相关的取值范围 $M \leqslant g^{-1}k$ (k 表示不同的参数类别). 由这些取值可构成一个一维的 M 级 QoS 损耗阵 QoS(M). 将 QoS(M) 与即时最佳 QoS 需求序列阵 QoS(t) 相匹配后, 即可得到最佳 QoS 相关参数表 L(QoS), 表中只包括使 QoS 达到最佳时所需的相关参数. 这些不同参数将决定 M 的最终取值范围, 取最大整数值, 即可得到最优 QoS 安全认证级数 M 的值.

3.2.2 算法分析

设杂交多级 μTESLA 级数为 M, 根据文献[2]中的式(4)可知, 其认证过程带宽消耗表达式为

$$Rc \geqslant \frac{(M_B-1)(1-R_d)(1-\sqrt[ml]{1-P})}{(M_B-1)(1-\sqrt[ml]{1-P})+\sqrt[ml]{1-P}}. \tag{6}$$

其中: R_d, R_c, R_a 分别为所有密钥链级中可信 CDM 信息、数据包以及伪造的 CDM 信息所需带宽的比重; m 为每一级密钥链中 CDM 缓冲区个数; l 为时间片长度; P 为一个传感器节点在下一个时间片中故障恢复的期望概率.

可推导出与带宽相关的级数 M_B 取值范围为

$$M_B \leqslant \frac{R_c\sqrt[ml]{1-P}}{(1-\sqrt[ml]{1-P})(1-R_d-R_c)}+1. \tag{7}$$

因为 $R_c+R_d+R_a=1$, 所以式(7)可表示为

$$M_B \leqslant \frac{(R_c-R_a)\sqrt[ml]{1-P}+R_a}{R_a(1-\sqrt[ml]{1-P})}. \tag{8}$$

由于基站存贮量主要由各级密钥构成, 根据文献[2]可知, 认证过程中基站所需存贮空间 M_j 为

$$M_j \geqslant M_M\cdot L\cdot \mathrm{LEN}_k+\frac{L^{M_M}-L}{L-1}\cdot \mathrm{LEN}_{\mathrm{CDM}}. \tag{9}$$

其中: M_M 为与存贮量相关的级数, L 为密钥链中密钥个数, LEN_k 和 $\mathrm{LEN}_{\mathrm{CDM}}$ 分别为密钥长度和 CDM 数据包长度.

可推导出级数 M_M 的取值范围为

$$M_M \leqslant \frac{\ln\left[L+\dfrac{(M_j-L\cdot \mathrm{LEN}_k)(L-1)}{\mathrm{LEN}_{\mathrm{CDM}}}\right]}{\ln L}. \tag{10}$$

由文献[2]可知, 认证过程中基站所需的预计算量 C_j 为

$$C_j \geqslant \frac{L^{M_c+1}-L}{L-1}\mathrm{LEN}_k+\frac{L^{M_c}-L}{L-1}\mathrm{LEN}_{\mathrm{CDM}}, \tag{11}$$

其中 M_c 为与计算量(即能耗和时延)相关的级数. 因而, 可以推导出 M_c 取值范围为

$$M_c \leqslant \frac{\ln\left[\dfrac{C_j(L-1)+L(\mathrm{LEN}_k+\mathrm{LEN}_{\mathrm{CDM}})}{L\cdot \mathrm{LEN}_k+\mathrm{LEN}_{\mathrm{CDM}}}\right]}{\ln L}. \tag{12}$$

这样, 可得到 M 级 QoS 相关参数阵为

$$\mathrm{QoS}(M)=(M_B,M_M,M_C,\cdots). \tag{13}$$

假设在与 QoS(t) 相匹配后, 某应用最佳 QoS 相关参数表 $L(\mathrm{QoS})=\langle M_B,M_M,M_C\rangle$, 这样将不等式(8), (10), (12)交集后取最大整数值即为该应用多级 μTESLA 最佳级数.

4 评估与仿真

设在 1 000×1 000 m^2 的区域中, 均匀分布 100 个节点, 设节点通讯半径为 50 m, 误码率为 0, 每簇节点数为 Nc, 移动实体速度为 v, 随机地沿直线通过监测区域. 本文分析了所有的网络生存周期、成功唤醒率以及精度延迟率的仿真数据.

为了检测 QoS 安全认证算法的效率, 将其应用于 DCSMS(QoS-DCSMS), 并与Mobicast 和 DCSMS 进行比较.

其中有关性能规则定义如下:

1) 网络生存周期 (NSC): 网络中不同时间的有效节点数.

2) 成功唤醒率 (SW): 应唤醒节点数与唤醒节点数的比率.

3) 精度延迟率 (ADR): 在一次组播会话中, 组播传送数据量与完成时间的比率.

图 1 和图 2 分别为 NSC 和 SW 的仿真效果图. 可

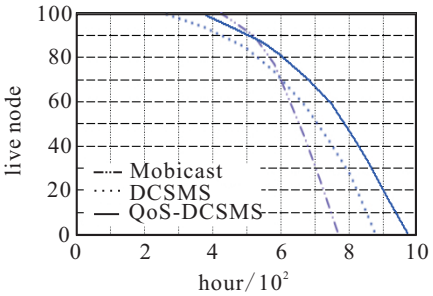

图 1　网络生存周期仿真效果

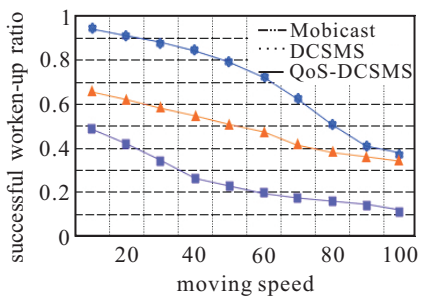

图 2　成功唤醒率仿真效果

见QoS-DCSMS在性能方面比DCSMS有了较大的改善.

为了对最优QoS安全认证算法的效果进行验证, 本文在特定应用需求条件下, 对使用不同级数的多级μTESLA进行安全认证时组播过程ADR进行仿真.

设实体运动速度为20; R_a, R_c, R_d分别为1%, 80%, 19%; L为600, m为4, l为0.5, P为99%, 密钥长度为8, CDM包长度为29; 簇头为认证所分配的可用存贮空间M_j和预计算量C_j分别为32×10^4和9×10^6.

根据式(8), (10), (12), 分别得到M_B, M_M, M_C, 因而得到最优级数M为3. 图3的仿真结果验证了算法结论的正确性.

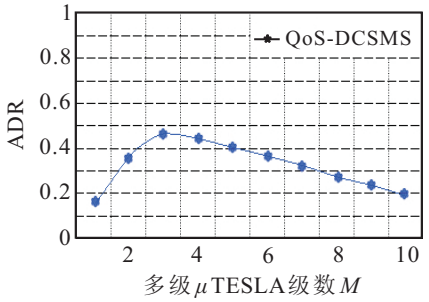

图 3 QoS-DCSMS不同级数认证ADR仿真效果

5 结 论

如何将安全认证与QoS相匹配是WSTNs中一个重要问题. 本文在Mobicast基础上提出了一种最优QoS安全认证算法, 首先利用自感知QoS需求算法实时地生成与实体运动速度相适应的组播应用服务需求相关参数, 并将其向量化; 然后在此基础上, 通过最优QoS多级μTESLA级数分析算法得到使QoS达到最优的多级μTESLA的相应级数. 仿真结果表明, 该算法能够有效地分析QoS相关参数与多级μTESLA密钥生成级数之间的相互关系, 且在一定程度上改善了网络组播性能.

参考文献(References)

[1] Huang Q F, Lu C Y, Roman G C. Spatiotemporal multicast in sensor networks[C]. Proc of SenSys'03. New York, 2003: 5-7.

[2] Liu D G, Ning P. Multi-level μTESLA: Broadcast authentication for distributed sensor network[C]. Proc of 10th Annual Network and Distributed Systems Security Symposium. San Diego, 2003: 263-276.

[3] Jin J, Qin Z G, Xiong H, et al. DCSMS: A mobicast-based dynamic clustering secure mobile multicast scheme for large-scale sensornets[C]. Proc of WCN2009 Workshop of 4th Int Conf on Frontier of Computer Science and Technology. Shanghai, 2009: 722-727.

[4] Subhas K G, Ranjeet K P, Manik R, et al. Secure group communication in wireless sensor networks[C]. Proc of ICACT 2008. Phoenix Park, 2008: 17-20.

[5] Roberto D P, Luigi V M, Yee W L, et al. LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks[C]. Proc of Int Conf on Parallel Processing Workshops. Kaohsiung, 2003: 6-9.

[6] Hui L, Taieb Z. GKM: A group dynamics aware key management scheme for Mmulticast communications in Ad-hoc sensor networks[C]. Proc of IPCCC 2007. New Orleans, 2007: 11-13.

[7] 靳京, 秦志光, 王佳昊, 等. 无线传感器网络中的追踪组播密钥管理机制研究[C]. 第六届中国信息和通信安全学术会议. 南京, 2009: 250-254.
(Jin J, Qin Z G, Wang J H, et al. Search on key management mechanism of tracking multicast in wireless sensor networks[C]. Proc of CCICS'2009. Nanjing, 2009: 250-254.)

[8] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

(上接第796页)

[8] 陈丹, 方康玲, 陈乔礼. 遗传算法在PID参数优化中的应用[J]. 微计算机信息, 2007, 23(7): 19-20.
(Chen D, Fang K L, Chen Q L. The application of float-point genetic algorithm in the PID parameter optimization[J]. Microcomputer Information, 2007, 23(7): 19-20.)

[9] Kroese D P, Rubinstein R Y, Porotsky S. The cross-entropy method for continuous multiextremal optimization methodology and computing[J]. Applied Probability, 2006, 8(6): 383-407.

[10] Rubinstein R Y, Kroese D P. The cross-entropy method: An unified approach to Monte Carlo simulation randomized optimization and machine learning[M]. New York: Springer-Verlag, 2004.