EGAKA:一种面向LTE-A机器类型通信的高效组认证与密钥协商协议

宋亚鹏 陈 昕
(北京信息科技大学计算机学院 北京 100101)

摘 要 机器类型通信(Machine Type Communication,MTC)作为物联网的基础,有着广阔的市场和应用前景。LTE-A网络能够为MTC的发展提供有力的支持,第三代合作伙伴项目(3rd Generation Partnership Project,3GPP)已经在3GPP标准Release10中正式定义了MTC。与普通的移动用户设备相比,MTC设备具有数量多、功耗低的特点,这给LTE-A网络的身份认证问题提出了新的挑战。当大量MTC设备同时接入网络时,如果每个设备都进行独立的身份认证过程,则会导致LTE-A网络出现严重的信令拥塞问题。同时,MTC设备由于计算资源有限,不宜做大量的运算。针对MTC网络中设备认证过程的信令拥塞问题,提出了基于聚合代理签名和消息认证码的组认证与密钥协商协议EGAKA。该协议采用聚合代理签名使得LTE-A网络可以同时验证多个MTC设备,并最小化认证过程中的信令开销。采用消息认证码的方法进行密钥协商,有利于降低MTC设备的计算开销。通过着色Petri网(Colored Petri Nets,CPN)的建模和分析,证明该协议能够正确完成认证和密钥协商。另外,通过在性能方面与文中引用的协议比较,证明该协议在信令开销和计算开销方面具有一定优势。

关键词 LTE-A,MTC,组认证,密钥协商,CPN
中图法分类号 TP309.2 **文献标识码** A

EGAKA:An Efficient Group Authentication and Key Agreement Protocol for MTC in LTE-A Network

SONG Ya-peng CHEN Xin
(School of Computer Science,Beijing Information Science & Technology University,Beijing 100101,China)

Abstract Machine type communication (MTC),as the basis of the Internet of things,is a wide open area in market and a great application trend. The MTC networks can be strongly supported by the LTE-A networks,and the 3rd Generation Partnership Project (3GPP) has formally defined the MTC in the standard of Release 10. Compared to the normal mobile user equipment,the MTC devices have some special features,such as the huger quantity and lower power consumption. These features lead to more research challenges for the identity authentication in the LTE-A networks. When a mass of MTC devices are accessed to the LTE-A network simultaneously with a full authentication and key agreement process for each device,the communication signaling would congest the network. Meanwhile,the limited computation resources in MTC devices do not allow too many operations. Aimed at the congestion problems in the authentication processes,an authentication and key agreement protocol based on the aggregated proxy signature and message authentication code was proposed and named as EGAKA. The protocol adopts the aggregated proxy signature to make the LTE-A networks able to authenticate multiple MTC devices simultaneously and minimize the communication consumption. And the adoption of the message authentication code can decrease the computation consumption of the key agreement process. Then,the protocol was modeled and analyzed by the colored Petri nets (CPN),whose results demonstrate that the protocol is safe. Finally,via the performance analysis,the results demonstrate that the communication consumption is better than other protocols of the same kind,and the computation consumption is better than other protocols of the same kind which adopt the asymmetric encryption.

Keywords LTE-A,MTC,Group authentication,Key agreement,CPN

1 引言

机器类型通信,也称为机器到机器(Machine to Machine,M2M)的通信,被视为下一代无线网络技术之一,引起了国际标准化组织的极大兴趣。第三代合作伙伴项目在Release10中正式定义了MTC,将它应用于工业领域。传统移动通信技术是针对人与人(Human to Human,H2H)的通信业务设计的,在传输特性、QoS要求、移动性和终端分布密度方面都与

本文受国家自然科学基金面上项目(61370065),国家自然科学基金青年项目(61502040),国家科技支撑计划项目(2015BAK12B03-03)资助。
宋亚鹏(1990—),男,硕士生,主要研究方向为无线网络与安全,E-mail:songyapeng_bistu@sina.com;陈 昕(1965—),男,博士,教授,主要研究方向为计算机网络及性能评价、网络安全、航电网络。

MTC 有很大不同。MTC 设备(MTC Device,MTCD)的数量会增长得更快,文献[1]预计 MTCD 的数量在未来将超过传统用户设备(User Equipment,UE)的 1000 倍。如果 MTCD 的接入认证过程采用当前 3GPP 提出的标准认证和密钥协商(Evolved Packet System Authentication and Key Agreement,EPS-AKA)协议[2],当多个 MTCD 同时进行接入认证过程时,LTE-A 网络会发生严重的信令过载,导致 LTE-A 网络拒绝这些 MTCD 的访问。因此,LTE-A 网络需要新的接入认证协议来避免大量 MTCD 接入时导致的拥塞。

基于群组的通信机制,能将多个地理位置相似或属于同一用户的 MTC 设备组成一个群组。根据群组中各成员设备的通信能力、通信链路质量、电池容量等因素,选择一个群组长,群组成员可以通过组长设备与 MTC 服务器进行数据传输。组长对组中所有成员的数据进行整合后统一发送,能在很大程度上节约信令开销。文献[3]提出了一种 MTCD 分组算法来避免拥塞,在该算法中,多个 MTCD 被构建成一个组,并选出组长,组中其他成员通过组长与 MTC 服务器交换数据。但是该文献没有考虑 MTCD 与 MTC 服务器之间的安全因素,没有接入认证的功能。文献[4]提出了基于组的认证和密钥协商方法,来保证一组用户设备(User Equipment,UE)与服务网络(Serving Network,SN)之间的安全通信。在该协议中,属于同一家庭网络(Home Network,HN)的多个 UE 被命为一个组,由组中第一个接入 SN 的 UE 与 SN 进行认证,并将该 UE 和组中其他成员的认证信息保存在 HN 中,当其他成员接入 SN 时,可以由 HN 直接认证,从而减少 HN 与 SN 之间的通信次数。但是当有大量设备同时接入 SN 时,这种方法依然不能避免拥塞。文献[5]提出了针对车辆自组织网络(Vehicular Ad Hoc Networks,VANETs)的匿名批认证与密钥协商协议。车辆到车辆(Vehicle to Vehicle,V2V)通信是一类特殊的 M2M 通信,服务供应商能够同时认证多个车辆,并为不同车辆生成不同的会话密钥,从而减少通信次数。文献[6]采用证书和非对称加密的方式,事先向 HN 和一组 MTCD 发放证书,当该组 MTCD 接入 SN 时,由组长聚合所有成员的证书,与 HN 进行认证。由于不需要再次经过 SN 来认证,因此减少了 HN 与 SN 之间的通信次数。但是该方法在进行认证和密钥协商时都采用了非对称加密的方法,会大大增加计算量,这不适用于资源非常有限的 MTC 设备。文献[7]同样采用消息认证码验证 MTCD 的身份,该协议要求一组 MTCD 中,第一个接入 SN 的 MTCD 在完成认证过程后,将该组其他成员的认证信息下载到 HN 中。后续成员的身份认证只需要通过 HN 认证而不用经过 SN,由此减少了 SN 与 HN 的通信次数,而且计算量方面也少于采用非对称密码体系的方法。但是该协议要求第一个接入 SN 的 MTCD 与后续成员使用不同的认证过程,这增加了认证系统的复杂性;另外,将认证信息下载到 HN 中增加了泄露用户身份信息的风险。文献[8]采用消息认证码的方法,由组长聚集所有成员的消息认证码,然后经过 HN 发送给 SN 进行验证。与公钥方法相比,该方法能显著降低 MTC 设备的计算开销。但是该方法每次认证都必须经过 SN 的验证,会增加 HN 与 SN 之间的信令开销。文献[9]提出了一种用二叉树结构管理各组及组成员密钥的方法,但是该组认证协议在安全性和信令开销方面都没有改进。

针对上述问题,本文利用文献[10]中的聚合代理签名的方法,先为 MTCD 组中每一个 MTCD 和移动管理实体(Mobile Management Entity,MME)分配由归属签约用户服务器(Home Subscriber Server,HSS)授权的代理签名;然后由组长对每个组成员的代理签名聚合之后发送给 MME 验证,同时组长也能接收 MME 的代理签名来验证 MME 身份的合法性。因此,MTCD 组能直接与 MME 相互验证身份,而不需要 HSS 的参与,降低了 HN 到 SN 的信令开销。在密钥产生阶段,放弃常用的 Diffie-Hellman 密钥协商方法,而采用消息验证码生成 MTCD 与 MME 的会话密钥,这样能大大减少公钥计算的次数,降低认证过程的计算机量。

本文第 2 节介绍所提出的认证协议的前提和背景;第 3 节详细描述该协议的运行流程;第 4 节和第 5 节分别分析了该协议的安全性和性能;最后作出总结。

2 背景

2.1 网络架构

如图 1 所示,MTC 网络架构基于 3GPP 标准[11,12],分为 3 个部分:1)无线接入网(Evolved Universal Terrestrial Radio Access Network,E-UTRAN),由 MTC 设备和演进型基站(evolved Node B,eNB)组成;2)分组核心网(Evolved Packet Core,EPC),包括用来执行接入认证功能的 MME,以及 HSS、服务网关(Serving Gateway,S-GW)、分组数据网络网关(Packet Data Network Gateway,P-GW);3)非 3GPP 部分,例如互联网。MTC 设备通过应用程序接口与 MTC 服务器连接,MTC 服务器可以通过两种方式与 LTE-A 网络连接:1)由移动服务提供商部署 MTC 服务器,并由 LTE-A 网络控制 MTC 服务器;2)由 MTC 用户布置 MTC 服务器,将它置于 LTE-A 网络外。

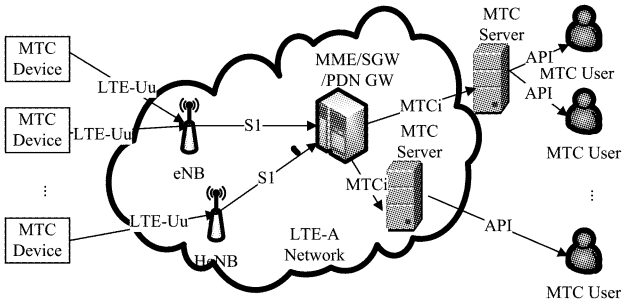

图 1 MTC 网络架构

当大量 MTCD 同时接入或者离开网络时,会发生信令的拥塞[13]。3GPP 系统支持多种 MTC 应用,例如测量或者监控。当能源中断或者经过一段同步时间间隔后,相关 MTCD 可能同时激活,向 MME 和 HSS 等网络结点同时发送大量信令,从而导致拥塞。拥塞可能发生在两个地方:1)当大量 MTC 设备同时接入 eNB 时,多个设备争抢同一个信道,会导致无线接入网内的拥塞[14];2)EPC 中各结点的拥塞,主要包括负责设备接入管理的 MME、负责运载流量的 S-GW 和负责在 MTC 设备与 MTC 服务器之间转发数据的 P-GW。文中主要关注传输认证消息的实体,例如 eNB 和 MME 中的拥塞问题。

2.2 聚合代理签名

文献[10]提出了基于椭圆曲线的聚合代理签名方法,它

允许源签名人将签名权力授予 n 个代理签名人，由 n 个代理签名人对 n 个不同的消息签名之后，再将这 n 个独立的签名聚合成一个签名。接收到该签名的用户可通过双线性对运算验证该聚合签名是否合法，从而通过一次运算验证 n 个代理签名人的身份。该方法能显著减少发送签名和验证签名所需的带宽和计算开销，因此被越来越多地运用在资源有限、能耗低的移动设备中。

3 组认证与密钥协商协议

该协议是基于聚合代理签名和消息认证码的组认证与密钥协商协议，分为初始和组认证与密钥协商两个阶段。在初始阶段，由 HSS 向 MME 和 MTCD 分配代理签名；在组认证与密钥协商阶段，MME 与 MTCD 通过验证代理签名互相确认身份，再通过消息认证码方式生成共享密钥。

3.1 初始阶段

HSS 选择大素数 p，并以 p 为模数生成两个椭圆曲线组 G_1 和 G_2。在 G_1 中选择基本点 P，然后由 HSS 产生随机数 $x\in Z_P$ 作为私钥，并计算系统公钥 $Q=xP$。选择合适的双线性对映射 $e:G_1\times G_1\rightarrow G_2$，哈希函数 H_1、H_2，其中 H_1 是二进制串到椭圆曲线组的映射 $H_1:\{0,1\}^*\rightarrow G_1$，$H_2$ 是二进制串到整数的映射 $H_2:\{0,1\}^*\rightarrow Z_p$。选择加密函数 f_K^e 和能生成消息认证码的函数 f_K^m，并由 HSS 向外公布系统参数 $\{p,G_1,G_2,e,P,Q,H_1,H_2,f_K^e,f_K^m\}$。

每个 MTC 设备都拥有一个身份标识 ID_{MTCD}，它由供应商直接安装在 MTC 设备中，用来作为注册 3GPP 网络的唯一标识。当 MTCD 和 MME 第一次接入网络或者密钥过期时，HSS 向每个 MTC 设备发送私有密钥 K_{Gi-j}，其中 i 和 j 表示第 i 个组中的第 j 个 MTC 成员。对于由 n 个 MTCD 组成的 MTC 组，令该组名称为 $G1$，其中每个 MTC 组成员共享组私有密钥 K_{G1}，且每个成员与 HHS 共享私有密钥 K_{G1-i}。当 HSS 接收到 MME 的身份标识 ID_{MME} 时，HSS 计算 $S_{MME}=xH_1(EID_{MME})$，并将 S_{MME} 由安全通道发送给 MME 保存起来作为长期的私钥。与 MME 相似，当 $G1$ 组的每个成员 $MTCD_{G1-i}(i=1,2,\cdots,n)$ 第一次接入网络时，由 HSS 生成 $S_{MTCD_{G1-i}}=xH_1(EID_{MTCD_{G1-i}})$，并保存在 $MTCD_{G1-i}$ 中作为长期私钥。协议在初始阶段的详细过程描述如下。

1) $MTCD_{G1-i}\rightarrow leader:(EID_{MTCD_{G1-i}},MAC_{EID_{G1-i}})$

选出一个设备代表所有组内成员与 MME 通信，将这个设备命名为 *leader*。$MTCD_{G1-i}$ 使用与 HSS 共享的密钥加密 $ID_{MTCD_{G1-i}}$，由式(1)和式(2)计算出 $EID_{MTCD_{G1-i}}$ 和消息验证码 $MAC_{EID_{G1-i}}$，并将它们发送给 *leader*。

$$EID_{MTCD_{G1-i}}=f^e_{K_{G1-i}}(ID_{MTCD_{G1-i}}) \tag{1}$$

$$MAC_{EID_{G1-i}}=f^e_{K_{G1}}(EID_{MTCD_{G1-i}}\|ID_{MTCD_{G1-i}}) \tag{2}$$

2) $learder\rightarrow MME:(REQ_{G1})$

leader 接收到来自每个成员的 $EID_{MTCD_{G1-i}}$ 和 $MAC_{EID_{G1-i}}$ 之后，对 $MAC_{EID_{G1-i}}$ 进行验证。验证通过后，由式(3)计算 MAC_{G1}，并将 REQ_{G1} 发送给 MME，其中 $REQ_{G1}=(EID_{MTCD_{G1-1}}\|\cdots\|EID_{MTCD_{G1-n}}\|MAC_{G1})$。

$$MAC_{G1}=MAC_{EID_{G1-i}}\oplus MAC_{EID_{G1-2}}\oplus\cdots\oplus MAC_{EID_{G1-n}} \tag{3}$$

3) $MME\rightarrow HSS:(REQ_{G1}\|ID_{MME})$

4) $HSS\rightarrow MME(RESP_{MME})$

HSS 在接收到来自 MME 的 REQ_{G1} 和 ID_{MME} 之后，先验证 MAC_{G1} 是否正确。验证通过之后，使用与 MTCD 的共享密钥 K_{G1-i} 对每一个 $EID_{MTCD_{G1-i}}$ 解密，得到 $ID_{MTCD_{G1-i}}$，由 HSS 检查该 $ID_{MTCD_{G1-i}}$ 是否属于合法用户。如果用户的身份合法，则 HSS 选择随机数 r_{HSS}，使用组密钥 K_{G1} 生成一个临时密钥 $GTK=f^m_{K_{G1}}(r_{HSS})$。然后，计算 $MTCD_{G1-i}$ 和 MME 的长期私有密钥 $S_{MTCD_{G1-i}}=xH_1(EID_{MTCD_{G1-i}})$，以及 $S_{MME}=xH_1(f^e_{GTK}(ID_{MME}))$。由以上信息组成回复信息 $RESP_{MME}=(S_{MTCD_{G1-1}}\|\cdots\|S_{MTCD_{G1-n}}\|S_{MME}\|T_{terminal}\|GTK\|r_{HSS})$ 发送给 MME，其中 $T_{terminal}$ 表示长期私钥过期的时间。

5) $MME\rightarrow leader:(RESP_{leader})$

MME 保存 S_{MME} 和 GTK，将 $RESP_{leader}=(S_{MTCD_{G1-1}}\|\cdots\|S_{MTCD_{G1-n}}\|T_{terminal}\|r_{HSS})$ 发送给 *leader*。

6) $leader\rightarrow MTCD_{G1-1}:(S_{MTCD_{G1-i}}\|T_{terminal}\|r_{HSS})$

将 HSS 生成的代理签名 $S_{MTCD_{G1-i}}$ 发送给相应的 $MTCD_{G1-i}$ 作为 $MTCD_{G1-i}$ 长期持有的私有密钥。然后 $MTCD_{G1-i}$ 使用共享的组密钥 K_{G1} 生成临时密钥 $GTK=f^m_{K_{G1}}(r_{HSS})$ 并保存起来，用来与 MME 进行密钥的协商。

3.2 组认证和密钥协商阶段

一组 MTCD 尝试同时接入网络时，先根据组中各成员的通信能力、存储能力和电池状态等信息选出一个组长 *leader* 代表组内其他所有成员与 MME 进行相互认证。在双方互相确认身份后，由组中每个 MTCD 生成一个会话密钥，来保证 MTCD 与 MME 的通信安全。另外，本文假设所有的 MTCD 都支持 LTE-A 和 WiFi。该认证阶段的详细过程描述如下。

1) $MTCD_{G1-i}\rightarrow leader:(V_{G1-i},EID_{MTCD_{G1-i}},GID,T_{G1-i})$

令 $w=(EID_{MTCD_{G1-i}}\|GID\|T_{G1-i})$，根据式(4)和式(5)计算 h_i 和 V_{G1-i}，然后将向量 $(V_{G1-i},EID_{MTCD_{G1-i}},GID,T_{G1-i})$ 发送给 *leader*。

$$h_i=H_2(w) \tag{4}$$

$$V_{G1-i}=h_iS_{MTCD_{G1-i}} \tag{5}$$

2) $leader\rightarrow MME:(AUTH_{leader})$

组长 *leader* 通过 WiFi 接收到所有组内成员发送来的签名 V_{G1-i} 后，将这 n 个签名聚合成一个签名 $V_{G1}=\sum_{i=1}^{n}V_{G1-i}$，将向量 $AUTH_{leader}=(EID_{MTCD_{G1-1}}\|\cdots\|EID_{MTCD_{G1-n}}\|GID\|T_{G1-1}\|\cdots\|T_{G1-n}\|V_{G1})$ 发送给 MME。

3) *MEE* 验证 MTC 组

MME 接收到来自 *leader* 的认证消息 $AUTH_{leader}$ 后，执行以下步骤：

①检查每一个 T_{G1-i} 是否超时，如果超时，则向 *leader* 发送一条认证失败的消息；否则进入步骤②的验证过程。

②计算 $h_i=H_2(EID_{MTCD_{G1-i}}\|GID\|T_{G1-i})$，验证公(6)是否成立。

$$e(V_{G1},P)=e(\sum_{i=1}^{n}h_iH_1(EID_{MTCD_{G1-i}}),Q) \tag{6}$$

③当式(6)验证成功后，由 MME 选择当前时间 T_{MME}，并根据式(7)，由消息认证码函数 f_K^m 通过 MME 保存的密钥 GTK 生成会话密钥 K^S_{G1-i}。

$$K^S_{G1-i}=f^m_{GTK}(EID_{MTCD_{G1-i}}\|f^e_{GTK}(ID_{MME})\|T_{G1-i}) \tag{7}$$

④令 $w=(EID_{MME}\|GID\|T_{MME})$，其中 $EID_{MME}=f^e_{GTK}(ID_{MME})$。由式(4)和式(5)分别计算 h_{MME} 和签名 V_{MME}，由 MME 生成认证消息 $AUTH_{MME}=(EID_{MME}\|GID\|T_{MME}\|V_{MME})$，然后将 $AUTH_{MME}$ 发送给 *leader*。

4) $MME \rightarrow leader:(AUTH_{MME})$

5) $leader \rightarrow MTCD_{G1-i}:(AUTH_{MME})$

leader 将认证消息 $AUTH_{MME}$ 通过 WiFi 广播给组内所有的 $MTCD_{G1-i}$。$MTCD_{G1-i}$ 执行以下步骤：

①$MTCD_{G1-i}$ 首先计算 $h_{MME}=H_2(EID_{MTCD_{G1-i}} \| T_{MME})$，然后通过公式 $e(V_{MME},P)=e(h_{MME}H_1(EID_{MTCD_{G1-i}}),Q)$ 验证 MME 的身份是否合法。

②如果 MME 的身份是合法的，则由式(7)生成会话密钥 K_{G1-i}^{S}。

③由 $MTCD_{G1-i}$ 向 MME 发送确认消息，告知 MME 会话密钥成功生成，可以进行通信。

在第一次验证完成之后，将 MME 的签名 V_{MME} 和加密后的身份标识 EID_{MME} 存储在 $MTCD_{G1-i}$ 中。$MTCD_{G1-i}$ 再次接入网络时，可以直接产生会话密钥，而不需要再次向 MME 请求签名和身份标识。

4 着色 Petri 网验证协议的安全性

4.1 着色 Petri 网的定义

着色 Petri 网是用于系统描述、设计、模拟和验证的图形化工具。它能对 Petri 网中的标志着以不同的颜色，将标志分类，使它的托肯(token)可以描述任意复杂的数据。另外，着色 Petri 网的建模可以分层，有利于用自上而下或者自下而上的思想设计系统，使系统层次更加清晰。

定义 1 着色 Petri 网是七元组 $\Sigma=(S,T;F,C,W,I,M)$，其中：

1) S 是库所的有限集合，$S=\{s_1,s_2,\cdots,s_m\}$，T 是变迁的有限集合，$T=\{t_1,t_2,\cdots,t_n\}$，$S \cup T \neq \varnothing$，$S \cap T=\varnothing$。

2) F 是有限弧集，$F \subseteq S \times T \cup T \times S$，它是变迁颜色与库所颜色之间的对应关系，$\times$ 是笛卡尔积。

3) C 是颜色的有限集 $C=\{c_1,c_2,\cdots,c_k\}$，$W:F \rightarrow L(C)_+$，$I:T \rightarrow L(C)_+$，$M:S \rightarrow L(C)$。$L(C)$ 表示定义在颜色集 C 上的一个非负整数系数线性函数，$L(C)_+$ 表示系数不全为 0 的 $L(C)$，即 $L(C)=a_1c_1+a_2c_2+\cdots+a_kc_k$，$L(C)_+=b_1c_1+b_2c_2+\cdots+b_kc_k$，$a_i$、$b_i$ $(i=1,2,\cdots,k)$ 均为非负整数，且 $b_1+b_2+\cdots+b_k \neq 0$。

4.2 CPN 的建模与分析

用 CPN 对切换认证协议的流程建模，分析它的所有终止状态是否与预期相同。如果存在可疑的终止状态，则说明协议的设计存在漏洞，其是不安全的。仿真工具 CPN Tools 4.0.1能方便地构建出切换认证协议的着色 Petri 网模型，并自动生成状态空间。

4.2.1 组认证与密钥协商协议 CPN 模型的声明与建模

该认证协议涉及 MTCD、MTCD 群组组长(leader)、MME 和 HSS 4 个实体之间的信令交互，本模型用 5 个库所表示它们，如图 2 中粗边框圆形所示。在 CPN ML 语言中，分别用 INFO_MTCD_I、INFO_MME 和 INFO_HSS 3 种类型的颜色集表示，这 3 个颜色集分别包含了每个实体在协议运行过程中需要传输的参数。图 2 中粗边椭圆表示认证结果，当“Success”、“Session Key in MME”和“Session Key in MTCD”这 3 个库所同时产生 token 时，表示 MME 和 MTCD 中都产生了会话密钥，认证成功；当库所“Failure”中产生 token 时，说明 MTCD 与网络之间的认证失败，token 的值表示失败发生的位置，例如产生的 token 值为“MME Verify Failure”时，表示是在 MME 验证 MTCD 的身份时失败。

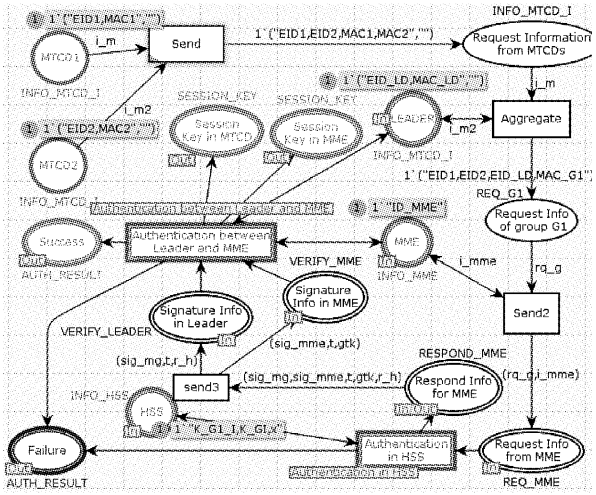

图 2 EGAKA 的着色 Petri 网模型

该模型把认证的具体步骤划分到子页面中，如图 2 中粗边矩形所示。替代变迁“Authentication in HSS”仿真的是协议在初始阶段 HSS 对 MTCD 身份的验证和代理签名的产生过程。替代变迁“Authentication between Leader and MME”仿真的是在认证与密钥协商阶段 MTCD 组组长(leader)与 MME 之间互相验证身份，以及产生会话密钥的过程。

4.2.2 组认证与密钥协商协议 CPN 模型的分析

向“MTCD1”和“MTCD2”两个库所分别写入一个 token 进行仿真，则仿真结果代表协议运行一次可能产生的结果。通过 State Space 工具能得到该模型状态空间的详细报告，通过整合得到报告的部分内容，如表 1 和表 2 所列。

表 1 CPN 模型状态空间的统计信息

Statistics	State Space	Nodes	18
		Arcs	41
		Secs	0
		Status	Full
	Scc Graph	Nodes	18
		Arcs	41
		Secs	0

表 2 CPN 模型状态空间的活性信息

Liveness Properties	Dead Markings	4[8,13,17,18]
	Dead Transition Instances	None
	Home Markings	None

表 1 中统计信息显示，CPN 模型的状态空间(State Space)包括 18 个节点(Node)和 4 条弧(Arcs)。状态空间图中强连通组件(Scc Graph)的数目与状态空间的节点数目相等，说明认证协议的流程没有出现死锁的情况，即协议中没有任何一个流程会产生循环。表 2 中活性信息中显示模型有 4 个死标识 8、13、17 和 18，表示 CPN 模型在到达这 5 个标识后，没有变迁可以触发。

用 State Space 工具能得到这 5 个死标识的详细情况。对于死节点 8，库所“Failure”中产生了托肯(token)“HSS Verify Failure”，说明模型中 HSS 在对 MTCD 身份验证时失败，即 MTCD 组中至少有一个成员的身份不合法；这是协议预期达到的状态，说明协议运行正确。对于死节点 13，库所“Failure”中产生了托肯“MME Verify Failure”，说明模型中 MME 在对 MTCD 身份验证时失败，即 MTCD 组中至少有一

个成员的代理签名不合法；这是协议预期达到的状态，说明协议运行正确。对于死节点 17，库所“Failure”中产生托肯“MTCD Verify Failure”，说明模型中 MTCD 在对 MME 身份验证时失败，即 MTCD 接收到的代理签名不合法，符合协议的预期。对于死节点 18，库所“Success”、“Session Key in MME”以及“Session Key in MTCD”都接收到正确的托肯，说明模型中所有的认证环节都验证成功。由上述内容可知模型状态空间中的死节点都是预期可达到的，说明协议的运行是正确的。

由表 2 可知模型中没有死变迁（Dead Transition Instances），即每个变迁都至少在一种标识下是可触发的，说明协议的设计中没有冗余步骤。模型中没有家态标识（Home Marking），说明协议流程中没有循环，协议的运行总是能够到达终点。

5 EGAKA 协议的性能分析和比较

该节计算本文提出的协议在通信和计算方面的开销，并将其与文献[6,7]中提出的协议作比较。假设有 n 个 MTCD 组成一个组，接入网络 t 次，其通信开销和计算开销的分析如下。

5.1 通信开销

假设在一个 MTCD 组中，各成员与组长（leader）之间的通信、组长与 MME 之间通信以及 MME 与 HSS 之间的通信均需要 1 个时间单位。当 MTCD 组第一次申请接入网络时，在初始阶段，MTCD 向网络请求验证身份，并由 HSS 向 MTCD 和 MME 分配长期持有的私钥，需要 $(2n+4)$ 个时间单位；在认证与密钥协商阶段，MTCD 与 MME 之间通过签名相互认证身份，并由消息认证码方式生成会话密钥，需要 $(2n+3)$ 个时间单位。在后续的验证过程中，由于 MTCD 保存了 MME 的签名等信息，需要 $(n+3)$ 个时间单位完成认证过程。将提出的组认识协议与 LTE-A 标准认证协议以及文献[6,7]的组认识协议比较，得到如表 3 所列的结果。由表 3 中 MTCD 组 t 次接入网络的总通信次数可知，当 t 的值较大时，本文的协议明显好于 EPS-AKA 和文献[7]的协议，略好于文献[6]的协议。

表 3 通信开销的比较

	第一次接入	后续的(t−1)接入	t 次接入总通信次数
EPS-AKA[15]	6n	4n(t−1)	6n+4n(t−1)
文献[6]	8n	(n+3)(t−1)	8n+(n+3)(t−1)
文献[7]	3n+6	(2n+4)(t−1)	3n+(2n+4)(t−1)+6
本文的协议	5n+7	(n+3)(t−1)	5n+(n+3)(t−1)+7

5.2 计算开销

EPS-AKA 使用对称密钥，它的计算开销可视作零。令椭圆曲线加密算法中的点乘运算时间为 T_{mul}，双线性对操作的运算时间为 T_{pair}，由加密的身份标识到椭圆曲线点的哈希函数执行时间为 T_{etp}。由文献[5]可知，$T_{mul}=T_{etp}=0.6$ms，$T_{pair}=4.5$ms，本文协议、文献[6,7]的计算开销如表 4 所列。本文协议中，每个 MTCD 的计算开销只有一个 T_{mul}，好于文献[6,7]中的协议，更适用于计算资源非常有限的 MTC 设备。对于 LTE-A 网络，本协议的计算开销较文献[7]略差，这是因为文献[7]主要使用了对称加密算法，仅在密钥生成阶段使用基于椭圆曲线的 Diffie-Hellman 算法，只需要少量的点乘运算。

表 4 计算开销的比较

	文献[6]	文献[7]	本文
MTCD	$4T_{mul}$	$2T_{mul}$	T_{mul}
LTE-A 网络	$nT_{etp}+(2n+1)T_{mul}+2T_{pair}$	$(n+1)T_{mul}$	$nT_{etp}+nT_{mul}+2T_{pair}$

结束语 本文提出了基于聚合代理签名和消息认证码的组认证与密钥协商协议，该协议采用群组验证的方法，利用聚合代理签名使多个 MTC 设备的身份信息聚合成一个组身份信息。MME 只需要对该组身份信息进行一次验证即可验证所有 MTC 设备的身份，从而减少了 MTC 设备与 MME 之间的通信次数，解决了 MTC 网络中因多个用户同时接入引起的信令拥塞问题。另外，该协议在初始阶段由 HSS 向每个 MTC 设备及 MME 发送源签名，然后由 MTC 设备和 MME 产生代理签名。MTC 设备与 MME 之间通过相互验证对方的代理签名来验证双方身份的合法性，而不需要向 HSS 发出身份验证请求，这减少了 MME 与 HSS 的通信次数，进一步解决了 MTC 网络的信令拥塞问题。

由于 MTC 设备大都具有计算资源和电池容量有限的问题，本文采用消息认证码生成 MTC 设备与 MME 的会话密钥，在保证信令开销较优的情况下，同时降低了 MTC 设备的计算开销。与其它信令开销相近的协议[5-7]相比，本文协议中 MTC 设备的计算开销最小。

参 考 文 献

[1] Fadlullah Z M, Fouda M M, Kato N, et al. Toward intelligent machine-to-machine communications in smart grid[J]. Communications Magazine, IEEE, 2011, 49(4): 60-65

[2] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Rei 11), 3GPP TS 33 401 Vl1. 3. 0[Z]. Mar. 2012

[3] Jung K R, Park A, Lee S. Machine-Type-Communication(MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network[M]// Security-Enriched Urban Computing and Smart Grid. Springer Berlin Heidelberg, 2010: 167-178

[4] Chen Y W, Wang J T, Chi K H, et al. Group-based authentication and key agreement[J]. Wireless Personal Communications, 2012, 62(4): 965-979

[5] Huang J L, Yeh L Y, Chien H Y. ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1): 248-262

[6] Cao J, Ma M, Li H. A group-based authentication and key agreement for MTC in LTE networks[C]// Global Communications Conference (GLOBECOM). IEEE 2012: 1017-1022

[7] Lai C, Li H, Lu R, et al. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks [J]. Computer Networks, 2013, 57(17): 3492-3510

[8] Lai C, Li H, Lu R, et al. LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks [C] // Global Communications Conference (GLOBECOM). IEEE 2013: 832-837

[9] Choi D, Hong S, Choi H K. A group-based security protocol for Machine Type Communications in LTE-Advanced[C]// Computer Communications Workshops (INFOCOM WKSHPS). IEEE 2014: 161-162

[10] Lin Y C, Wu T C, Tsai J L. ID-based aggregate proxy signature scheme realizing warrant-based delegation[J]. Journal of Information Science and Engineering, 2013, 29(3): 441-457

[11] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC) (Rei 11), 3GPP TS 22.368 VI 1.4.0[Z]. Mar. 2012

[12] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type Communications (Rei 11), 3GPP TR 33.868 VO.7.0[Z]. Feb. 2012

[13] Chen Xin, Si Yuan, Xiang Xu-dong. Delay-Bounded Resource Allocation for Femtocells Exploiting the Statistical Multiplexing Gain [J]. The Journal of Supercomputing, 2015, 71(9): 3217-3236

[14] Chen Xin, Wang Hong-lu, Xiang Xu-dong, et al. Joint Handover Decision and Channel Allocation for LTE-A Femtocell Networks [C]// Proc. of Game Theory for Networks (GAMENETS'14). Beijing, China, 2014: 70-74

[15] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Rei 11) 3GPP TS 33.401 Vl1.3.0[Z]. Mar. 2012

(上接第 321 页)

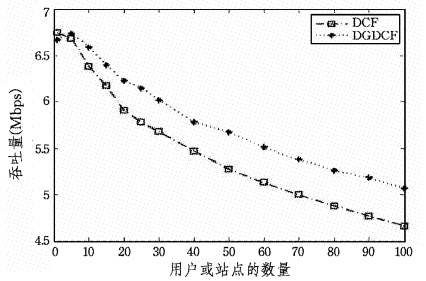

图 3 DCF 机制在吞吐量方面的性能比 NGDCF 低

综上所述，在 OFDMA-WLAN 系统中 AP 按照非合作竞争的博弈方法，同时给多 STAs 发送数据，分配不同质量的信道资源。由于 WiFi 网络基础架构简单，缺乏协议支持多 STAs 同时接入的机制，对 WiFi 网络协议做出修改以支持下行 OFDMA 具有重要的现实意义。现有 IEEE 802.11 DCF 机制存在不足之处：接收方成功收到 CTS 帧后，就开始传输数据帧；接收方如果不能成功收到 CTS 帧，采用指数退避算法计算一个新的退避时间来降低重传 RTS 帧，从而存在产生冲突的可能。对于 RTS 帧来说，退避时间是从 $(0, cw-1)$ 这个范围里面选择的（cw 是指竞争窗口的大小），随着用户数目的增加，竞争窗口 cw 增大，信道接入概率就会减小。已经存在一些通信系统采用 OFDMA 的接入技术，如 LTE 的下行采用 OFDMA，WiMAX 上下行都采用 OFDMA。为了利用 OFDMA 技术提供的多 STAs 分集增益，LTE/WiMAX 等系统通常需要确保多个 STA 发送的时间差在可容忍的范围内，并划分专用信道收集 STA 信道状态信息 CSI，调用调度算法确定 STA 相应的资源块与调度次序。但这些方案需要复杂的基础架构（如蜂窝网）作为支持，均不适合简单的 WiFi 网络架构。根据现有的 IEEE 802.11ac 标准，AP 一次只能和一个客户端通讯，当接入设备少时数据传输率不存在问题，若接入的设备增加到数十、上百个，其 80MHz 的频宽和传输量被海量设备分割，大部分设备都在等待与 AP 通讯。本文提出的采用 AP 集中调度的 NGDCF 算法较好地解决了上述问题。

结束语 在同一个 WLAN 中，接入的设备越多，数据传输率越低，在不牺牲数据传输率的前提下，信道资源分配的优化目标是使 WLAN 的吞吐量最大化。由于 IEEE 802.11 DCF 中没有中心协调的用户，因此每个用户竞争信道时都会影响到它的邻居用户。本文基于 OFDMA 技术并利用非合作博弈理论，采用 AP 集中调度机制（文中称之为非合作博弈分布式协调功能 NGDCF）裁决用户对不同质量信道的竞争，不会影响其它多个用户的数据传输，提高了数据传输率。另外，本文提出的 NGDCF 算法在信道分配时，对链路间的信道质量加以考虑，由于无线链路的质量受到多方面的影响，无线网络中不同用户间链路所需带宽也各不相同，需要对 STA 最终获得的速率以非合作博弈的竞争方式加以限制，引入效用函数来增强竞争力较弱的 STA 的实力，使 WLAN 系统在资源分配的公平性与数据传输率之间达到了更好的折中。

参 考 文 献

[1] Liu Xiu-long, Li Ke-qiu, Min Ge-yong, et al. Efficient Unknown Tag Identification Protocols in Large-Scale RFID Systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12): 3145-3155

[2] Xiao Yong-kang, Shan Xiu-ming, Ren Yong. Game Theory Models for IEEE 802.11 DCF in Wireless Ad Hoc Networks [J]. IEEE Radio Communication, 2005, 43(3): 22-26

[3] Bianchi G. Performance Aalysis of the IEEE 802.11 distributed coodination function [J]. IEEE Journal on Selected Areas in Communication, 2000, 18(3): 536-547

[4] Perahia E, Gong M X. Gigabit wireless LANs: an overview of IEEE 802.11ac and 802.11ad [J]. Mobile Computing and Communications Review, 2011, 15(3): 23-33

[5] Valentin S, Freitag T, Karl H. Integrating multiuser dynamic OFDMA into IEEE 802.11 WLANs-LLC/MAC extensions and system performance [C] // IEEE International Conference on Communications. Beijing, China, 2008: 3328-3334

[6] Chen Li-jun, Low S H, Doyle J C. Random access game and medium access control design [J]. IEEE/ACM Trans. on Networking, 2010, 18(4): 1303-1316

[7] Bao Nan, Xia Wei-wei, Shen Lian-feng. Resource allocation based on fairrness and QoS provisioning for OFDMA-WLAN system [J]. Journal of Southeast University English Edition, 2014, 30(1): 1-6

[8] Scutari G, Palomar D P, Facchinei F, et al. Game Theory and Variational Inequality Theory [M] // IEEE Signal Processing Magazine. 2010: 35-49

[9] Kwon H, Hanbyulseo, Kim S, et al. Generalized CSMA/CA for OFDMA Systems: Protocol Design, Throughput Analysis, and Implementation Issues [J]. IEEE Trans. on Wireless Communications, 2009, 8(8): 4176-4187

[10] Johari R, Tsitsiklis J N. Efficiency loss in a network resource allocation game [J]. Mathematics of Operations Research, 2004, 29(3): 407-435