|  |
| --- |
| 1. **课题来源**   自拟   1. **课题研究的目的、意义**   物联网伴随着人们的日常生活，自他诞生起就改变着人类的生活与生产方式，例如，物联网可以让我们随时随地的支付购物，可以随时查看所在地的很多消息，也可以让我们尽情享受智能家居带来的方便与智能。物联网通过无线网技术使得物体通过网络相互连接，让多个孤立的个体能够变得相互关联，并且不需要关心连接的物体具体形态，每个连接的物体都可以看成是一个抽象的实体存在，而连接之后他们变为一个相互关联的整体。在2005年《ITU互联网报告：物联网》中曾指出物联网就是通过各种诸如像无线网络和射频自动识别技术以及智能计算、云存储以及大数据等技术将世界上各种物体和设备连接起来并实现相互通信和协同工作所实现的网络。  物联网技术本身是一个很大范畴，其中主要包括RFID(Radio Frequency Identification,射频识别)、无线传感网络、自组织网络、红外感应、激光扫等许多技术，实现物体的相互连接、交换信息、追踪、定位以及识别等功能。目前物联网处于发展阶段，很多地方存在不足和问题，比如在利用物联网实现通信过程中可能导致信息被窃取，用户身份信息被盗用，诸如此类的很多问题都可以归结于安全性问题，而安全问题是关注用户切身利益的问题，所以在研究物联网技术的时候不得不考虑安全性，针对这些潜在的安全威胁和安全漏洞，基于物联网的安全性分析显得尤为重要。  物联网许多应用都是基于客户端-服务器模型和使用单播数据传输，也有很多应用如电话会议、在线游戏等，它们都是基于群组通信，并且要求群成员通信的私密性，在这种场景中广播通信比单播通信效率更高，它要求由一个信任的发送者发送数据给群组里的所有成员，并且只有群成员能够获取信息，并不希望群外部人员获取信息，并且在群成员加入后并不能获取之前的信息，群成员离开之后也不能获取以后的群信息。  保证群组成员之间的通信私密性是群组通信的基本保障，通过使用群组密钥，使其只能被群组成员获取，使得成员之间的通信可以通过群组密钥加密和解密。除此之外还需要考虑物联网本身资源是受限，如存储和计算能力较低、电量有限等，在保证群组成员之间通信的私密性和安全性问题的基础上，如何降低计算复杂度、空间复杂度、通信消耗、节省电量等也是需要考虑的问题。因为有成员的动态加入或者离开，为了保证前向和后向安全性，需要对群组密钥进行更新。其中所谓前向安全是指新成员加入群组的之后不能解密加入前的信息，保证之前通信的安全性。后向安全是指旧成员离开之后无法解密群组成员的之间的通信，即保证了有成员离开之后群通信的安全性。  综上所述，基于目前互联网不可阻挡的发展趋势，越来越多的基于物联网技术的应用出现，同时又由于物联网技术的不成熟，以及物联网本身的特性所带来的的安全性问题亟待解决，尤其是在群体通信的应用领域中，亟需要高效安全的实现群通信的协议。所以本课题旨在以基于物联网环境，从通信安全性出发，研究设计出能够适用与物联网环境能够满足安全性的高效群密钥管理方案。   1. **课题的国内外研究现状和发展动态**   根据不同的划分标准，群密钥管理方案被细分为不同的类型。根据管理方式，分为集中式、分布式和分层式群密钥管理方案。  （1）集中式群密钥管理方案  1997年，Harney首先提出了组密钥管理协议（FKMP），此协议中，依赖于组控制者完成密钥的生成、分发和更新等一系列操作。当有成员加入或退出后，利用当前组内所有成员的私钥对组密钥加密，此方案容易实现，但是通信开销与实际的组内成员数目呈线性关系，当成员数目较多时，会带来较高的通信成本，这使得其应用范围仅限于小型群组。为了降低通信开销，2000年Wong提出了基于逻辑密钥层次树的组密钥管理方案，通过引入密钥图的概念保证组密钥的安全性，此方案中包括三种不同类型的节点：根节点、叶子节点和虚拟节点。成员加入或退出后，只需要更新叶子节点上的密钥，虚拟节点上的密钥则保持不变，这使得密钥更新过程中的通信复杂度降低至，其中n代表实际参与的组成员数目，但是该方案增加了组成员的存储成本。基于对LKH协议方案的改进，2003年Sherman提出了基于单向函数树的组密钥管理方案，通过引入盲节点，该方案将密钥更新过程的通信复杂度从降为，且该方案具有较好的可扩展性，能适用于大型动态环境下的组播通信场景，然而对比LKH协议，OFT协议方案需要耗费更高的存储成本  （2）分布式群密钥管理方案  由于集中式组密钥管理方案过于依赖可信任的控制中心，会造成单点失效的现象发生。基于此，通过构建密钥协商算法，一系列分布式组密钥管理方案纷纷提出。此类方案中，不存在控制中心，且所有的节点地位是对等的。1998年Steiner等人提出了基于D-H（Diffie-Hellman）算法的组密钥管理方案，由两个组成员扩展到n个组成员共同参与组密钥的构建，此方案中不会出现单点失效的情况，但是每个成员需要依次共享出自己的私钥，并按照一定的次序组成一个逻辑环，这使得该方案的计算成本较高，并且在缺乏管理中心的条件下难以检验成员的身份。随后Lee等人提出基于二叉逻辑树的组密钥管理方案，通过加入公开的盲密钥，每个节点能计算出所在路径的密钥，该方案有效降低了计算复杂度，但是会存在中间人攻击的情况，无法保证方案的安全性。  （3）分层式群密钥管理方案  结合以集中式和分布式群密钥管理方案的优势，分层式群组组密钥管理方案被纷纷提出。1997年Mittra提出了可扩展的群密钥管理方案将整个群组细分为更小的子组，此方案拥有较高的安全性能，当有成员变动时，密钥更新所带来的开销较小，但延迟时间较长，会出现网络拥堵的现象。Srivatsa所构造的方案不需要依赖可信第三方，此方案中，密钥进行双重加密后被发送给组内成员，且任意组成员拥有两个私钥，当接收到消息后，进行两次解密后即可恢复出群密钥，但是当子组成员数目发生变化时，后向安全得不到保证。  基于不同的管理方式，上文对已有的群密钥管理方案进行了归纳总结。此外，群组密钥管理方案的构建基于不同的密码学理论。2003年，Saze提出基于秘密共享的密钥预分发协议，在初始化阶段，可信赖的第三方将秘密片预先发送给组内成员；在密钥分发阶段，只有持有秘密片的成员才能获得秘密份额。2008年，Zheng等人提出了基于中国剩余定理的组密钥管理协议，在组密钥更新阶段，任意组内成员仅仅进行一次模运算和异或运算就能计算出组密钥，降低了密钥更新过程的计算复杂度。然而，该方案将更多的计算开销转移到密钥服务器上，这可能会导致密钥服务器崩溃。为了降低计算开销，Zou提出了轻量级的分布式组密钥管理方案，通过构造访问控制多项式提高了方案的安全性，基于哈希函数的单向性，恶意攻击者无法逆向计算出组密钥，但是有成员加入或退出时，需要重新构造访问控制多项式，这提高了组密钥更新过程的计算成本。2010年，Han提出了基于秘密共享的组密钥管理协议，该方案降低了组成员的存储成本，任意成员始终存储一对私钥，但是每更新一次组密钥，组成员需要发送不同的随机质询给密钥生成中心，作为秘密多项式函数的输入，这会增加组密钥更新阶段的通信开销。2013年，Vijiyakumar提出了基于最大公约数的二维密钥管理协议第一个维度用于降低组密钥更新阶段的计算开销，第二个维度用来降低控制者和组成员保存密钥而耗费的存储成本。2014年，Vijiyakumar等人提出了基于中国剩余定理的集中式组密钥管理方案，此方案中，组密钥更新过程的计算复杂度是，由于具有较低的计算开销，该协议迅速被应用于车联网和云计算领域。然而，Vijiyakumar的方案是不安全的，无法保证动态环境下的前向安全要求。2016年，Qin提出了面向车联网通信的分层式组密钥管理方案，在不需要与其他子组交流的前提下，任意成员可以恢复出所在子组的会话密钥，但是该方案的扩展性能较差，无法应用于大型动态群组环境。当组内成员较多时，该方案具有较高的计算成本和通信开销。2020年Kumar提出了基于RSA公钥密码体制的动态组密钥管理方案，基于大数分解问题的困难性，该方案是安全的，但组密钥加密过程具有较高的计算复杂度。   1. **课题的研究内容、拟采取的技术方案或研究方法**   1.研究内容：  本课题主要研究在物联网环境下的群密钥管理协议，实现在物联网环境下实体之间安全、可靠和高效的群通信，并且适应于群成员动态改变的群。由于物联网环境存在自身的特点，如物联网中的实体计算、存储护能力低，电量有限，实体之间具有复杂的拓扑结构，每一个实体既有可能作为接受信息的对象，也可能作为发送信息的对象。本课题主要针对以上问题，通过学习密码学领域的理论知识和几种经典的群密钥管理方案，验证并实现一种群密钥管理方案，对该方案进行正确性、安全性和性能分析，并在此基础上分析其在物联网环境中实现的可行性，加以改进使其能够满足物联网环境的实际需求，达到物联网环境下的安全通信。  主要研究内容如下：  （1）研究物联网环境下群通信的方法和原理；  传统的通讯模式有单播和广播通信。单播通信是源主机和目标主机进行一对一的交流，满足了通信交流的个性化需求，但是若要发送相同信息给多个接收者，需要重复多次该过程，会提高传输成本，导致网络堵塞和延迟。广播通信是源主机向一定范围内的主机发送数据信息，该区域的主机能够获得相同的消息。然而，广播应用的区域范围有一定限制，且将消息发送给不需要的主机会造成资源浪费。在此背景下，组播随机产生，它结合单播和广播的优势，源主机将消息发送给特定的多个目标主机，且只需要发送一次即可，降低了单播通信模式中多次发送相同的消息导致的高成本，解决了广播中资源不必要浪费问题。  除了单播、广播和组播，多对多通信模式也是一种常见的群组通信模式。多对多的群组通信中每个成员的身份都是平等的，在群组内每个成员既可以发送消息也可以接受消息，不存在任何中央控制节点，群组会话密钥的生成是由群组中所有成员共同完成的。  学习物联网环境的群通信方法，就要掌握以上四种通信模式的方法和原理，并把握其优缺点，分析其适用的场景，并选定一种群通信的方法对其进行深入研究和实现。  （2）研究群密钥管理协议的基础理论和几种经典方案；  根据不同的划分标准，群密钥管理方案被细分为不同的类型。根据管理方式，分为集中式、分布式和分层式群密钥管理方案。学习基于不同管理方式的群密钥管理方案，分析其优缺点和适用场景。  此外，群组密钥管理方案的构建基于不同的密码学理论。查阅数论、密码学数学基础等课程资料，深入学习密码学中的基本理论，主要包括中国剩余定理、拉格朗日插值多项式、秘密共享、大数分解难题等基本理论，这些理论基础在密钥协议研究中经常用到，并作为密钥设计的一部分。  研究群密钥管理协议的基础理论，群密钥管理协议为多个实体建立共享的群密钥，负责对密钥进行生成、分发、更新等操作，保证群组内所有成员共享一个组密钥，接收到消息后，合法授权成员能计算出组密钥；当有成员加入或退出时，组密钥随即被更新，从而保证动态环境下的前向/后向安全。  （3）分析对比不同群密钥管理协议的优缺点；  对于总结的基于不同密码学理论的群密钥管理方案进行细化地学习，类比总结出不同方案的优缺点。为进一步选择要研究的一种方案深入学习做准备。  （4）研究并实现一种群密钥管理方案。  在完成群密钥管理方案的的相关理论学习后，选择一种具体的方案进行代码实现，并将其放在物联网环境下进行验证分析，并对此方案进行正确性、安全性和性能分析并进一步改进，使其能够满足物联网环境的实际需求，达到物联网环境下的安全通信。  2.研究方法：  （1）学习基础理论知识。学习数论、密码学数学基础等基础知识。掌握中国剩余定理、拉格朗日插值多项式、大数分解难题、数据加密算法秘密共享等基本理论。作为密钥管理方案设计的基础。  （2）阅读期刊、论文等，翻译相关的英文文献。学习基于管理方式不同分类的密钥管理方案，如集中式、分布式和分层式管理方案并总结其优缺点、分析其适用场景；学习基于不同密码学基本理论的密钥管理方案，掌握密钥生成、分发和更新的全过程，对其进行安全性、正确性和性能分析。  （3）深入研究群密钥管理方案并创新实践。本课题选择研究的方向是基于中国剩余定理的动态群密钥管理，在已有的方案的基础上进行创新，并对比之前的方案，对其进行安全性、正确性和性能分析  （4）代码实现群密钥管理方案，并在某个场景下进行验证。采用JAVA或者C语言编程实现算法，在代码实现的过程中，需要注意代码的可读性、可维护性，并且在完成代码之后，还需要对于代码进行测试，保障正确性、可行性及安全性。  **五、课题研究的重点、难点及创新点**  重点：研究群密钥管理方案，实现验证一种群密钥管理方案并加以改进，使其满足物联网环境的实际需求，实现在物联网环境下的安全通信。对比已有方案，在较低的计算复杂度的前提下，提升方案安全性能，并对方案进行正确性、安全性和性能分析，分析方案的优势所在。  难点：群密钥管理方案的掌握，需要较强的数学和密码学理论基础，因此在方案学习方面是一个难点。其次，通过代码实现方案过程，需要较强的编程能力。  创新点：将群密钥管理方案置于一种物联网特定环境中实现，基于中国剩余定理的密码学知识研究一种动态群密钥管理方案。  **六、课题研究的进度安排**  第一周（2.20-2.26）：搜集相关资料，准备开题报告。  第二周（2.27-3.5）：学习物联网环境下群通信方法和原理  第三周（3.6-3.12）：学习相关的密码学基本理论和数学难题  第四周（3.13-3.19）：阅读文献，研究已有的几种经典组密钥管理方案  第五周（3.20-3.26）：阅读文献，研究学习改进的组密钥管理方案  第六周（3.27-4.2）：研究车联网环境下群密钥管理机制  第七周（4.3-4.9）：分析对比不同群密钥管理协议的优缺点  第八周（4.10-4.16）：编程实现一到两种群密钥管理协议。  第九周（4.17-4.23）：整理资料，准备中期答辩。  第十周（4.24-4.30）：根据中期答辩结果，进行改进  第十一周（5.1-5.7）：完善实践成果  第十二周（5.8-5.14）：完善相关资料  第十三周（5.15-5.21）：撰写论文。  第十四周（5.22-5.28）：完善论文。  第十五周（5.29-6.4）：准备答辩。  第十六周（6.5-6.11）：答辩，提交材料。  第十七周（6.12-6.18）：整理归档。。  **七、课题研究目标或预期成果**  充分掌握不同的群密钥管理方案，研究分析不同群密钥管理方案的优缺点和适用场景，实现一种群密钥管理方案，并能够在一种特定的物联网环境中实现。预期成果完成一篇英文文献翻译，完成毕业设计论文和代码设计。  **八、主要参考文献**  [1]陈启雅. 面向安全组播通信场景的组密钥管理方案的研究[D].中国科学技术大学,2022.DOI:10.27517/d.cnki.gzkju.2022.001619.  [2]熊丽晖. 5G蜂窝车联网中基于群组的认证及密钥管理机制研究[D].西安电子科技大学,2021.DOI:10.27389/d.cnki.gxadu.2021.003672.  [3]王光杰. 在物联网环境下的群密钥管理协议研究[D].哈尔滨工业大学,2019.DOI:10.27061/d.cnki.ghgdu.2019.004105.  [4]Kumar, Vinod,Pal, Om,Thakur, Vinay,Kumar, Kamendra. SCGKM: a secure and cost-effective group key management scheme for multicast communication in large dynamic groups[J]. International Journal of Information Technology,2022(prepublish).  [5]Pandi Vijayakumar,Sudan Bose,Arputharaj Kannan. Chinese remainder Theorem based centralised group key management for secure multicast communication[J]. IET Information Security,2014,8(3). |
| **指导老师意见：**  **指导教师签字：**  **年 月 日** |
| **毕业设计（论文）检查组意见：**  **组长签字：**  **年 月 日** |
| **毕业设计（论文）指导小组意见：**  **签字（盖章）：**  **年 月 日** |