

军事车联网密钥管理方案研究

刘俊杰^{1,2}, 赵佳^{1,2}, 张强³, 刘吉强^{1,2}, 韩磊⁴

- (1. 北京交通大学智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044;
2. 北京交通大学计算机与信息技术学院, 北京 100044;
3. 北京市公安局网络安全保卫总队, 北京 100029;
4. 信息保障技术重点实验室, 北京 100071)

摘要: 研究了几种典型的军事车联网密钥管理方案, 对其存在的安全问题及多种攻击方式进行了总结, 在此基础上提出了一种等级树状结构的军事车联网密钥管理方案, 从而提高了通信效率和安全性。本方案对解决军事车联网通信中的密钥管理提供了很好的解决思路。

关键词: 密钥管理; 军事车联网; 安全通信; 树状结构

中图分类号: TN918.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018068

Research on key management scheme for military vehicle network

LIU Junjie^{1,2}, ZHAO Jia^{1,2}, ZHANG Qiang³, LIU Jiqiang^{1,2}, HAN Lei⁴

1. Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China
2. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China
3. Beijing Municipal Public Security Bureau Network Security and Security Corps, Beijing 100029, China
4. Science and Technology on Information Assurance Laboratory, Beijing 100071, China

Abstract: A scheme of military vehicle network security based on the hierarchical tree structure was proposed, which could improve communication efficiency and security of military vehicle network key management. The proposed scheme provides a good solution to solve the key management in military vehicle network communication.

Key words: key management, military vehicle network, secure communication, tree structure

1 引言

车载网络是新兴产品物联网和智能汽车两大领域的重要交叉点。车载网络是指通过网络设备使车与车之间、车与人、车与路边单元设备、车与建筑物等进行相互联通, 共同通信, 从而实现信息的交流、发布、共享等各种方便人们生活的

服务, 使人们的出行、交通等更加智能化^[1]。目前, 人们的生活质量稳步提高, 汽车已经成为人们生活必需品。在道路上行驶的汽车数量随着汽车人均拥有量的快速增加而不断增加, 车载网已经进入迅速发展阶段, 相应的车载技术也逐渐走向成熟, 并且以非常迅猛的速度应用于各个行业。在军事领域, 当今时代的战争实则是一场高级技

收稿日期: 2018-06-07; 修回日期: 2018-07-20

通信作者: 刘俊杰, 17125212@bjtu.edu.cn

基金项目: 中央高校基本科研业务费基金资助项目 (No.2018JBM016); 国家自然科学基金青年科学基金资助项目 (No.61502030); 信息保障技术重点实验室开放基金资助项目 (No.KJ-17-107)

Foundation Items: Fundamental Research Funds for the Central Universities (No.2018JBM016), National Natural Science Foundation of China (No.61502030), Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-17-107)

术的比拼,不需要任何的兵器和武器,作战空间也非常广阔,样式多变,战机稍纵即逝^[2]。车载网络通信中的安全问题显得更为重要,不仅直接影响驾驶员或乘客的生命和财产安全,甚至关乎一场战争的成败与否。

巨大的军事信息量和以上多种原因导致了军事通信任务的艰巨性,确保数据通信的安全性、完整性是军队通信指挥的重中之重,通信系统的完整和安全是军队战斗力的要素之一。而密码技术是在信息通信过程中,保障信息的完整性、机密性和安全性最常用到的技术之一^[3]。车载自主网络在军事领域应用中,使用车载网收集一些比较敏感的信息时,如果不法分子在外部窃听,一旦攻击成功,重要的内部通信数据被截取,导致车载网络中信息被泄露,后果将不堪设想。为了防御不良攻击行为,能够有效保证通信系统中数据的完整、保密、安全和不可否认等性质,基于群组的加密技术是很好的选择^[4]。车载网中的密钥使用量不断增加,为了减少开销,增加通信效率,密钥的管理和保护是提高作战效率,增强信息通信过程中安全性、完整性最重要的一环,因此密钥的管理成为需慎重考虑的问题。

根据车载自主网络具有高速动态性和无结构中心的特点,分布式密钥管理方案在网络中的应用最为常见^[5]。但该管理方案的管理复杂度比较大,使整个网络系统的连通率低,通信量和计算量偏大等。本文旨在解决这些问题,为了满足其在军事方面的应用需求,结合国内外密钥管理方案的研究现状,提出了一种基于树状结构模型的群组密钥管理方案。该方案以广播的形式进行组间和组内通信,从而在一定程度上提高了军事通信效率,减小了存储开销,提高了安全性^[6]。

2 国内外的研究现状

在国外,根据车载网络的动态结构特点研究人员提出了多种密钥管理方案,最为常见的是采用分布式思想,在传统认证中心的密钥管理的基础上提出或改进优化的方案^[7]。文献[2]介绍了在军事车载网环境中最传统的几种基于认证中心的密钥管理方案,以及在其基础上提出的分布式密钥管理方案。局部分布式管理方案的算法是生成

K 个私钥分量,并在其中选取 K 个车辆节点充当服务节点,每一个有效证书的颁发都是需要由多个服务节点同时提供部分正确的证书才可以完成的。例如,有车辆申请签发证书时,原本被选取的 K 个服务节点中必须至少有 n 个以上同意并利用自己持有的密钥分量签发部分正确证书,最后才能组合成一个正确的完整密钥颁发^[8]。另一种是在局部分布式密钥管理方案的基础上进行改进的完全分布式密钥管理方案,该方案中每一个车辆节点都可以充当服务节点,所有服务节点共同组成中心。通过这种方式,局部分布式方案中服务节点离开网络导致中心不可用的问题便被解决了。

在国内,学者们也结合车载网络的结构特点针对密钥管理中存在的问题提出了各种不同的解决方案。文献[6]中提出的是一种 K 级门限密钥的自治群组密钥管理方案,该方案通过多级共享的方式使高层密钥被多个解密密钥共享,当成员发生动态变化时,密钥更新具有独立性且密钥更新效率与网络结构无关。还有根据2种不同的攻击模型,文献[8]提出了一种基于身份的密码加密区域网格结构的安全管理方案,还有一种是在局部分布式密钥管理方案的基础上,增加证书撤销和密钥更新机制,不需要依赖任何可信权威机构。而且,能够有效限制群密钥有效期的密钥管理方案^[9]。另外一种是实现没有特定辅助认证中心的认证方法并且被广泛应用的基于浮动车的群组密钥管理^[10]。

通过以上对国内外几种典型的密钥管理方案的研究分析,结合军事车载网的结构特点,本文提出了一种基于树状结构模型的群组密钥管理方案。

3 树状群组密钥管理方案

在军事通信过程中,军队的编制体制具有特殊性,军队兵员数量巨大,信息传送时的节点很多。尤其是在户外野战的环境下,由于各种客观条件的限制,可以按照军队的编制分为各个层级和各级单位。每个层级和单位之间都具有隶属关系,军队通信中还存在访问权限问题。即高层的成员可以获得低层之间的群会话密钥,从而知道

低层成员之间的相互通信信息，反之则不能^[11]。各层级和各级单位之间相互通信时的信道带宽往往较狭窄，基于树状结构模型的密钥管理方案就是根据军队管理的特殊性而提出的一种适用于军事环境下动态车载网中的密钥管理方案^[12]。本节详细介绍了树状群组密钥管理方案中等级树结构模型的建立过程和群密钥管理过程。

3.1 符号定义

表 1 是对本节用到的变量进行了统一定义，具体定义如表 1 所示。

表 1 符号定义	
符号	定义
G	层间密钥管理器
G_i	底层小组内密钥管理器
K	生成的密钥
S_i^j	第 j 层第 i 个小组长
P_i	底层第 i 小组的成员
Q	用户群
GC	可信管理
q	一个大素数
$H: \{0,1\} \rightarrow F_q$	0,1 串经过散列函数 H 映射到 q 阶的有限域
$f(x)$	访问控制多项式
Z	随机数

3.2 等级树结构模型

等级树结构模型是根据军队特殊的隶属关系建立的，树的建立过程如下。

- 1) 根据军队特殊的编制情况把所有的用户划分为 M 个底层小组 $P_i(i=1,2,3,4,\cdots,M)$ ，且规定小组成员不超过 35 人。
- 2) 在划分的每个小组中确定一个组长，记为 $S_i(i=1,2,3,\cdots,M)$ ，组长 S_i 同时充当该小组密钥管理器 G_i ；对底层小组的管理按照 ACP 轻量级密钥管理方案。具体见 3.3.2 节。
- 3) 规定每 n 个组长 S_i^j 中确定上一层的组长 S_i^{j-1} ，若剩余底层小组长个数不到 n 个，则仍需要确定产生一个上一级组长。
- 4) 等级树结构模型的构建是重复上述第 3 步由下往上确定各层小组长直到产生一个最高组长 S_1^1 为止。在考虑降低存储开销和提高计算效率的前提下，第 i 层的 ID 可用 ID_i 表示，且令 $ID_i=I$ ，当 $n=2$ 时，如图 1 所示的树状等级结构模型，是根据军队成员特殊的隶属关系构建的图 1 中由上到下等级依次降低，即 S_1^1 是第一层组长，依次到 S_n^m 是第 m 层的第 n 个小组长。

3.3 树状群组密钥管理

树状群组密钥是指在本群组内的所有成员之间相互通信的数据都通过本密钥进行加密和解密，称之为群组共享密钥，该密钥的产生是通过

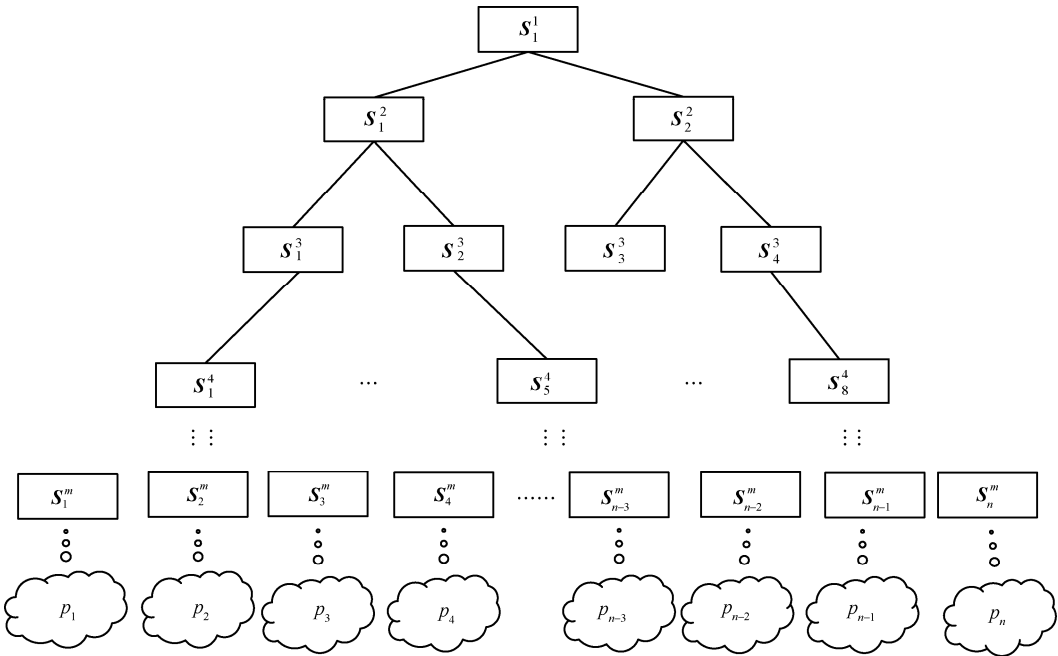


图 1 树状结构

群组内的成员共同协商产生的^[13]。因为军事车载自主网络环境下的群组具有动态结构, 群组成员具有动态性, 为了保证群组成员添加后群内的之前数据通信的安全保密性和群组成员退出之后的群内数据通信的安全保密, 群密钥需要不断及时更新, 在更新的过程中会产生各种消耗和问题, 由此群组密钥管理便是必不可少的。本节中 3.3.1 节具体介绍了密钥的分发与生成过程, 3.3.2 节介绍了对底层小组密钥的管理过程, 3.3.3 节介绍了密钥更新算法和需要密钥更新的几种情况。通过以上小节的具体实现过程, 即为本文提出的基于树状结构模型的群组密钥管理方案。

3.3.1 密钥生成与分发

基于等级树的结构模型, 密钥的种类主要分为 2 种: 一种是层间密钥; 另一种是底层小组组内密钥。2 种密钥的生成方式及步骤如下。

第 1 步: 由每一组的密钥管理器 G 根据密钥生成算法 $g: L \rightarrow K \times K$ 产生一个临时密钥 K_0 。

第 2 步: 根据密钥计算式 $K_i = H(K_{i-1} || ID_i)$, ($i=1, 2, 3, \dots, m$), 计算每一层的密钥 K_i ($i=1, 2, \dots, m$)。该过程用到的算法是单向散列散列函数。

第 3 步: 用层间共享密钥 K_i^j 对通过第 2 步计算得到的新的密钥 K_i 信息进行加密, 用每一层的密钥管理器 G 将更新后的新密钥通过 $G \rightarrow S_i^j: \{K_i\}_{k(i)}$ ($j=1, 2, 3, \dots, m$) 分发到本层成员的手中。通过这种方式每一层的成员 S_i^j 就得到了所在层的新密钥。

第 4 步: 在底层小组中, 小组的密钥管理器 G_i 和 P_i 内成员通过注册的方式来建立一条安全通道, 以此获得组内密钥 K_j ($j=1, 2, 3, \dots, M$) 和自己的私钥。

通过以上 4 个步骤, 最底层小组 P_i 内的成员能够获得所在小组的组内密钥 k_j ($j=1, 2, 3, \dots, N$) 和自己的私钥。层间密钥是由各层密钥管理员 S_i^j 按照从上到下的顺序依次获得的^[14]。算法实现过程如图 2 所示。

3.3.2 底层小组密钥管理

在等级树结构模型中, G_i 密钥管理器可以使用轻量级密钥管理方案 (ACP, access control polynomial) 访问控制多项式, 对最底层 P_i 小组进行轻量级密钥管理。ACP 的概念最早是由 Zou-Dai-Bertino 等提出的一种用于群通信

的轻量级密钥管理方案, 主要用在动态场景下为自组织网络分配群密钥^[15]。该方案简要介绍如下。

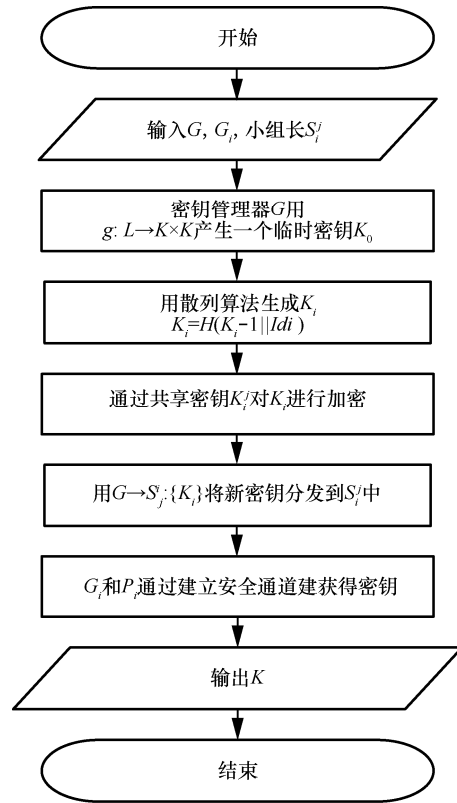


图 2 密钥生成与分发

假设通信系统中的群成员的密钥由一个可信的 GC 负责管理。若用户群 $Q = \{Q_1, Q_2, \dots, Q_n\}$, GC 提前为每个群成员 $Q_i \in Q$ 颁发私钥 K_i 。设定一个大素数 q , $H: \{0, 1\}^* \rightarrow F_q$ 是抗碰撞散列函数, GC 随机选择 $s \in F_q$ 作为群会话密钥, 构建 $f(x)$ 访问控制多项式^[16]。 $f(x)$ 形式如下:

$$f(x) = (x - H(s_1, z))(x - H(s_2, z)) \cdots (x - H(s_n, z)) + k$$

其中, $Z \in {}_R F_q$ 是随机选择的整数。 $f(x)$ 进一步变形:

$$f(x) = a_n x^n + \cdots a_1 x + a_0$$

GC 广播向量 $(a_0, a_1, \dots, a_n)$ 和随机整数 Z 任意的 $Q_i \in Q$ 可以利用自身私钥 K_i , 随机整数 Z 和公开的散列函数 H 计算群会话密钥 $k = f(H(s_i, z))$, 不用与系统中其他实体交互。

$f(x)$ 的表达式中不含群外成员的私钥, 所以群外成员不能计算出群会话密钥 k 。如果有成员变动时, GC 会重新选择一个随机数 $Z' \in$

${}_R F_q$, 新的 $k' \in F_q$, 重新构造访问控制多项式 ACP^[17]。

3.3.3 密钥更新

群组密钥更新算法一般有以下2个步骤。

首先, 由系统检测到节点的加入或者离开, 如果检测到有节点变动将发送节点变动请求触发密钥更新算法时, 树结构模型发生变化包括节点的命名等^[18]。

然后, 根据新的树结构模型用密钥生成算法生成和发布新的密钥。

基于树状结构模型的密钥管理方案中所有成员构成了等级树结构模型, 一旦有相关成员变动时树的结构也会发生变化, 为了保证数据通信的安全, 必须及时进行密钥更新。针对本文方案的密钥更新有以下几种情况。

1) 有新的成员加入小组。因为上层对下层有访问权限, 所以底层小组成员发生动态变化时并不需要更新层间密钥, 只需要更新组内密钥 k 即可。组内密钥 k 的更新采用轻量级密钥管理即只需要更新 ACP 具体公式如下

$$\begin{aligned} f(x) &= (x - H(s_1, z'))(x - H(s_2, z')) \cdots (x - H(s_n, z')) + k' \\ &= a'_{n+1}x^{n+1} + a_1x + a'_0 \end{aligned}$$

更新完成后由小组密钥管理器 G_j 通过层间共享密钥把新的组密钥 k'_i 发送给所属上级 S'_i 。

2) 有成员离开小组。成员的离开同增加一样通常发生在最底层小组内, 同上述情况一样, 只需要更新组内密钥 k_j , 层间密钥不需要更新, 该密钥的更新依旧采取轻量级密钥管理只需更新 ACP 具体公式如下:

$$\begin{aligned} f(x) &= (x - H(s_1, z'))(x - H(s_2, z')) \cdots (x - H(s_n, z')) + k' \\ &= a'_{n-1}x^{n-1} + a_1x + a'_0 \end{aligned}$$

更新完成后由小组密钥管理器 G_j 通过层间共享密钥把新的组密钥 k'_i 发送给所属上级 S'_i 。

3) 成员升级。成员升级是指原本在低层小组的成员 S' 晋升成了高层成员 S'' , 晋升后 S'' 的访问权限变大了, 信任值提高了, 此时只需要为该晋升成员 S'' 增加 a 层层间密钥和所管辖的各组的组密钥即可, 不需要更新各层的层间密钥。

4) 成员降级。指上层成员降成了下层或降成了最底层小组成员, 此时密钥更新方法如下。

① 当上层成员 S'' 的级别降低为下层成员 S' 时, 只需更新层间密钥, 底层组内密钥不需要更新。而层间密钥按照同 3.3.1 节中的前两步进行更新, 然后通过层间共享密钥将更新后的新层间密钥分发至各层。

② 若 S' 直接降为最底层小组 P_i 内的成员, 那么原本 S' 在高层时所管辖的所有群组密钥和所知道的层间密钥都需要及时更新, 且组内密钥的更新方法同第一种情况新成员加入。层间密钥更新根据 3.3.1 节第 1 和第 2 步, 然后将新的密钥分发给各层和组内成员。密钥更新算法过程如图 3 所示。

4 方案性能分析

基于树状结构模型的密钥管理方案适用于动态自组织军事车载网中, 该密钥管理方案是先以构建等级树为结构模型, 然后运用 Zou 等提出的轻量级密钥管理方案讨论分析该树状群组密钥管理方案的优劣, 本节从通信系统的安全性、存储开销和通信开销 3 个方面对该方案进行了具体分析^[19]。

4.1 安全性分析

基于树状结构模型的密钥管理方案中, 用单向散列函数计算出层间密钥 K_i , 具体的计算公式如下。

$$K_i = H(K_{i-1} \| ID_i), (i=1, 2, 3, \cdots, m)$$

由单向散列函数的性质可知, 给定任意的散列值 h , 满足 $H(x=h)$ 的 x 值是无法计算出来的。即下级由上级层密钥 K_i 不能得到 K_{i+1} , 由函数的单向性可知上层对下层的访问权限。

对底层小组 P_i 的密钥管理采用文献[2]提出的 Zou-Dai-Bertino 协议轻量级密钥管理方案, 该管理方案的算法是利用自身密钥 s 、随机数 n 和公开的散列函数计算出的群会话密钥, 大大提高了安全性, 因为即使攻击了 $H(s, n)$ 也是不能获取 P_i 的。基于树状结构模型的密钥管理方案中, 密钥更新过程中, 当群组成员发生动态变化时, 各层之间的密钥和各小组内的组内密钥的及时更新保证了通信中数据的向前安全和向后安全^[20]。

4.2 存储开销分析

密钥的存储量或者说密钥的存储个数称之为存储开销。从图 1 等级树结构模型可以知道需要

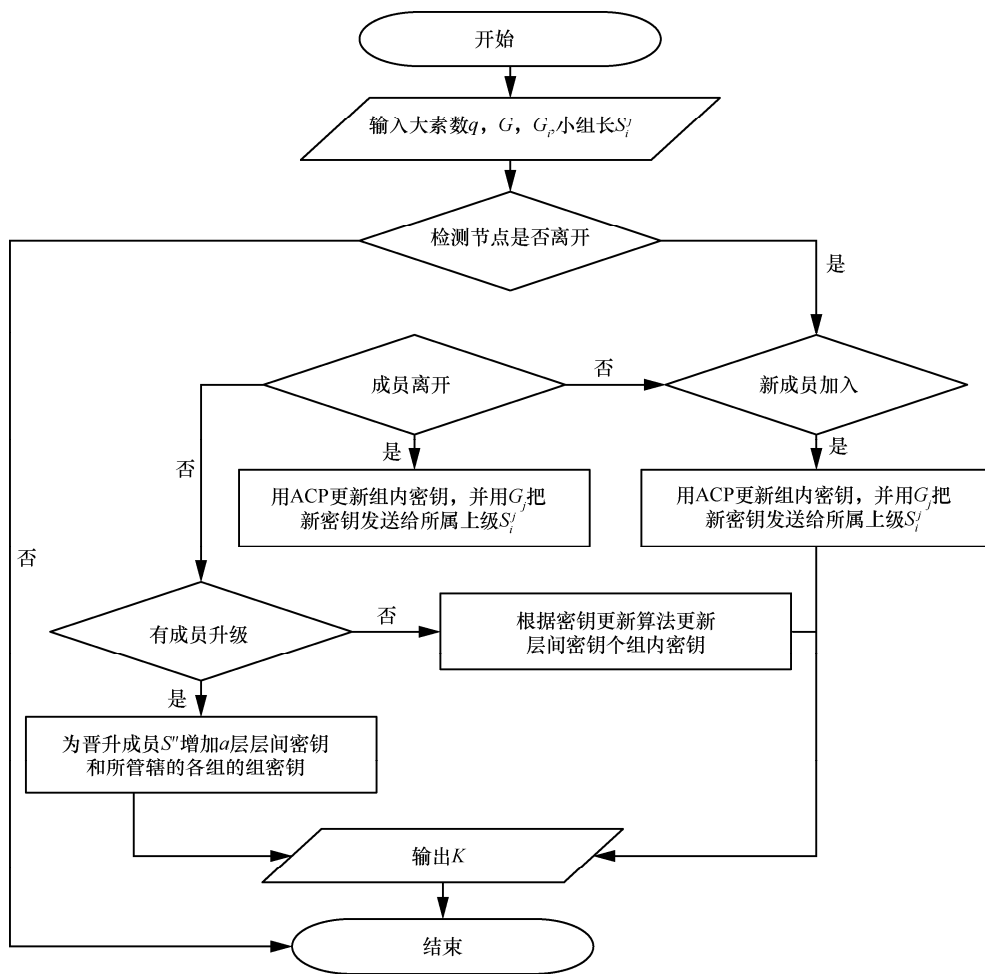


图3 密钥更新算法过程

存储密钥的有群组管理器 G 、小组管理器 G_i 、中间各层节点 S_i 和小组内部成员 P_i 。即以上各节点的具体密钥存储量情况如表 2 所示, 表中的符号和等级树结构模型中的符号一致。

表2 各节点的密钥存储量

节点	密钥存储量
G	$\left(\frac{a}{a-1}\right)N + N + 1$
G_i	$ P_i + 2$
S_i^j	$a^{m-j} + 1$
小组 P_i 成员	2

4.3 通信开销分析

更新密钥时需要发送信息的条数通常被称作是通信开销。在基于树状结构模型的密钥管理方案中, 更新层间密钥是通过单向散列函数计算得到的, 在计算之前必须先根据密钥生成算法由密

钥管理器 G 产生一个新的密钥 K' , 最后用共享密钥把新的密钥更新消息加密后发送出去, 其他层通过共享密钥解密后得到新的层间密钥。小组成员增加和减少的动态变化主要是发生在底层, 而组内密钥更新是通过轻量级密钥管理进行更新的, 并且文献[8]又对该算法进行了改进优化, 由文献[8]的改进算法可以知道: 当只有单个小组成员发生变化时, 成员个数的变动直接决定着系统的通信开销; 当更新开销为 $C=3m+n$ 时, 即此刻有 m 个成员加入和 n 个成员离开。

将基于树状结构模型的密钥管理方案和文献中常用于动态军事车载自主网络中的密钥管理方案进行比较, 具体情况如表 3 所示。为了使比较更有意义, 选择同类的密钥管理方案在假定 3 种密钥管理的方案中所选小组成员个数都是 $|P_i|$ 的情况下进行比较。与该方案进行比较的对象是一种大型动态密钥管理方案和一种基于成员隶属关系的密钥

表3 各节点的密钥存储量

存储量及开销	节点	文献[5]	文献[9]	本文方案
密钥存储量 s	G_i	$O(P_i)$	$O(P_i)$	$O(P_i)$
	中间各层 S_i^j	—	$O(a^{m-j})$	$O(a^{m-j})$
	G	$O(N)$	$O(N)$	$O(N)$
	小组 P_i 成员	$O(\log_d P_i)$	$O(\log_d P_i)$	2
小组 P_i 通信开销	成员退出	$O(\log_d P_i)$	$O(\log_d P_i)$	$O(1)$
	成员加入	$O(\log_d P_i)$	$O(1)$	$O(1)$

管理方案分别在文献[5]和文献[9]中有详细介绍。

通过表3比较可以看出在相同的条件下基于树状结构模型的密钥管理方案,密钥更新管理时,密钥的存储开销和底层小组内的通信开销等都优于其他2种密钥管理方案。在通信的过程中,因为层间密钥是共享的,基于树状结构模型的密钥管理方案特别明显地减少了信息的转发次数。而文献[5]中介绍的大型动态密钥管理方案中由于每个小组各自独立,彼此之间不共享密钥,从而使在密钥更新时增加了信息转发次数,增大了通信开销,并且消息不能及时同步存在时延问题^[21]。因此本文提出的基于树状结构模型的密钥管理方案在一定程度上改善了系统的通信效率,很好地减小了通信开销和存储开销。

5 结束语

在国防建设的军事通信过程中,赢得现代战争胜利的首要条件就必须保障通信信息的安全保密。本文结合车载自主网络的动态性及军事中的特殊结构和属性提出了一种基于树状结构模型的群组密钥管理方案。在保证系统基本安全的基础上,还满足了群组之间既能相互独立又能安全通信,组内安全通信等。而且,该方案也能够保证当组内成员变动时,密钥能及时更新从而满足数据的向上安全和向下安全^[22]。相对适用于车载自主网络中的几种传统的密钥管理方案,基于树状结构模型的密钥管理方案提高了安全性,增加了通信效率,并且在数据存储空间的开销和通信开销上都有非常明显的优势,相对其他同类密钥管理方案更加适合在人员数量大、层级隶属关系明显,数量多的群体以及战场环境下的部署。未来进一步的研究工作,将考虑增加进群的身份

识别和口令设置与基于树状结构模型的密钥管理方案相结合,在密钥更新或获取时直接通过简短口令或身份验证信息就能完成^[23]。进而更进一步提高整个通信系统的运行效率,更适合战时军事通信需要。

参考文献:

- [1] WEINFURTHER J M, PATON E R, CAUAUSHI A, et al. Vehicle network communication protection [J]. Ford Global Technologies, LLC, 2018, 2(16):1-10.
- [2] 吴海云. 面向车联网的群密钥管理方案的研究[D]. 合肥: 安徽大学, 2017.
WU H Y Research on group key management scheme for vehicle networking [D]. Anhui University, 2017.
- [3] MAHMOOD Z, NING H. A Polynomial Subset-Based Efficient Multi-Party Key Management System for Lightweight Device Net-works[J]. Sensors, 2017, 17(4): 670-696.
- [4] LAI C LU R ZHENG D *et al.* GLARM: group-based light weight authentication scheme for resource-constrained machine to machine communications[C]. Computer Networks, 2018(99): 66-816.
- [5] 魏楚元, 李陶深, 王高才, 等. 基于代理的分布式大型动态组播密钥管理协议[J]. 计算机工程与应用, 2007, 43(7): 155-59.
WEI C Y, LI T S WANG G C, *et al.* Distributed large dynamic multicast key management protocol based on agent[J]. Computer Engineering and Applications, 2007, 43(7): 155-159.
- [6] 周健, 孙丽艳, 陈红琳, 等. 星内集群自组织网络自治群组密钥管理研究[J]. 小型微型计算机系统, 2018, 39(05):904-909.
ZHOU J, SYN L Y, CHEN H L, *et al.* Key management of autonomous group in intra-satellite cluster self-organizing network[J]. Mini-micro Systems, 2018, 39(5):904-909.
- [7] HAITAO WANG, LIHUA SONG, GUOMING ZHANG, *et al.* Timetable-aware opportunistic DTN routing for vehicular communications in battlefield environments[J]. Future Generation Computer Systems, 2018(83)95-103.
- [8] 赵齐. 车载自组织网络群组密钥管理机制研究[D]. 吉林: 吉林大学, 2015.
ZHAO Q. Research on key management mechanism of vehicle self-organizing network group[D]. Jilin: Jilin University, 2015.
- [9] 高天寒, 李艳强. 车载自组织网匿名接入认证机制研究综述[J]. 网络与信息安全学报, 2016, 2(08):10-16.

- GAO T H, LI Y Q. A Review of research on anonymous access authentication mechanism of vehicle self-organizing network[J]. Chinese Journal of Network and Information Security, 2016, 2(8):10-16.
- [10] 李凤华. 信息技术与网络空间安全发展趋势[J]. 网络与信息安全学报, 2015, 1(1): 8-17.
- LI F H. Trends in Information technology and cyberspace security[J]. Chinese Journal of Network and Information Security, 2015, 1(1): 8-17.
- [11] 杜晓强, 鲍皖苏. 基于成员隶属关系的组播密钥管理方案[J]. 计算机工程与应用, 2013, 49(1): 101-106.
- DU X Q, BAO Y S. Multicast key management scheme based on member membership[J]. Computer Engineering and Applications, 2013, 49(1): 101-106.
- [12] SUTRALA, DAS, N KUMAR. On the design of secure user authenticated key management scheme for multi gate way-based wireless sensor networks using ECC[J]. International Journal of Communication Systems, 2018.
- [13] 马铭鑫, 史国振, 王亚琼, 等. 适用于分布式系统的多级安全访问控制策略[J]. 网络与信息安全学报, 2017, 3(8): 32-38.
- MA M X, SHI G Z, WANG Y Q, et al. Multi-level secure access control strategy for distributed systems[J]. Chinese Journal of Network and Information Security, 2017, 3(8): 28-34.
- [14] 高宝阳, 潘进, 康连瑞, 等. 一种基于等级树模型的群组密钥管理方案[J]. 计算机与现代化, 2014(8): 34-37.
- GAO B Y, PAN J, KANG L R, et al. A group key management scheme based on hierarchical tree model[J]. Computer and Modernization, 2014 2(8): 34-37.
- [15] 李德全, 张习勇, 张婷婷, 等. 具有私钥自愈能力的 DTN 密钥管理方案[J]. 网络与信息安全学报, 2017, 3(4): 26-31.
- LI D Q, ZHANG X T, ZHANG T T. DTN key management scheme with private key self-healing capability[J]. Chinese Journal of Network and Information Security, 2017, 3(4): 26-31.
- [16] 尹建东. 移动自组网中无证书可认证群组密钥管理方案研究[D]. 北京: 北京理工大学, 2016.
- YIN J D. Research on certificate-free certifiable group key management scheme in mobile ad hoc networks[D]. Beijing Institute of Technology, 2016.
- [17] ERMIS O, BAHTIYAR S, ANARIM E, et al. A secure and efficient group key agreement approach for Mobile ad hoc networks[J]. Ad Hoc Networks, Volume, 2017(67): 24-39.
- [18] 陈志广, 范晓琴. 一种基 LKH 的高效的组播密钥管理方案[J]. 电脑知识与技术, 2011, 7(25):6088-6090+6107.
- CHEN Z G, FAN X Q, et al. An efficient multicast key management scheme based on LKH[J]. Computer Knowledge and Technology, 2011, 7(25): 6088-6090.
- [19] 柯钢. 一种高效的无线网络组播密钥管理方案[J]. 西南师范大学学报(自然科学版), 2017, 42(01): 47-53.
- KE G. An efficient key management scheme for wireless network groups[J]. Journal of Southwest China Normal University (Natural Science), 2017, 42(1): 47-53.
- [20] WANG Q. A security and privacy review of VANET[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(6): 2985-2996.
- [21] POTTEIGER L, et al. Vulnerability of transportation networks to traffic-signal tampering[C]//International Conference on Cyber-Physical Systems. IEEE Press, 2016: 16.
- [22] 毛传武, 程阳, 余文明, 等. 动态实时身份认证的方法研究[J]. 网络与信息安全学报, 2016, 2(3): 76-85.
- MAO C W, CHENG Y, YU W M, et al. Research on dynamic real-time identity authentication method[J]. Journal of Network and Information Security, 2016, 2(3): 76-85.
- [23] 王良民, 李婷婷. 基于车辆身份的车联网结构与安全[J]. 网络与信息安全学报, 2016, 2(2): 41-54.
- WANG L M, LI T T. Structure and security of vehicle network based on vehicle identity[J]. Chinese Journal of Network and Information Security, 2016, 2(2): 41-54.

[作者简介]



刘俊杰(1993-), 女, 河南人, 北京交通大学硕士生, 主要研究方向为车载自组织网络、隐私保护、密钥管理。



赵佳(1980-), 女, 内蒙古呼和浩特人, 博士, 北京交通大学副教授, 主要研究方向为网络空间安全、可信计算、隐私保护。



张强(1980-), 男, 河北石家庄人, 主要研究方向为网络空间安全、区块链、态势感知。



刘吉强(1973-), 男, 山东海阳人, 博士, 北京交通大学教授、博士生导师, 主要研究方向为密码学、可信计算、隐私保护技术。



韩磊(1983-), 男, 内蒙古呼伦贝尔人, 博士, 信息保障技术重点实验室博士后, 主要研究方向为分布式非对称密钥管理、区块链、态势感知。