

文章编号:1001-9081(2011)10-2692-02

doi:10.3724/SP.J.1087.2011.02692

具有抗合谋攻击能力的自治愈群组密钥管理方案

曹 帅, 张串绒, 宋程远

(空军工程大学 电讯工程学院, 西安 710077)

(Shuaics187@163.com)

摘要:通过为每个会话时段产生随机数和构造广播多项式,使得合法用户根据自身秘密信息和当前广播消息,可以独立地恢复遗失的组密钥,而且能够抵抗被撤销节点和新加入节点的合谋攻击;此外,赋予被撤销节点新的秘密信息,使其能够重新加入群组参与会话。安全分析和性能分析表明:在保证安全属性的前提下,该方案具有较小的通信开销,能够适用于移动自组网。

关键词:组密钥管理;自愈;合谋攻击;移动自组网

中图分类号: TN918.91; TP309.2 **文献标志码:**A

Self-healing group key management scheme with collusion resistance

CAO Shuai, ZHANG Chuan-rong, SONG Cheng-yuan

(Telecommunication Engineering Institute, Air Force Engineering University, Xi'an Shaanxi 710077, China)

Abstract: Random number and broadcast polynomial for every session were created. The legal nodes could recover the lost legal group keys by themselves independently according to their private information and broadcast messages, and the collusion attack between newly joined nodes and revoked nodes was resisted. New private information was distributed to revoked nodes so as to rejoin group in later sessions. Through the security and efficiency analysis, the scheme has less communication cost yet still achieves security property, suitable for mobile Ad Hoc network.

Key words: group key management; self-healing; collusion attack; mobile Ad Hoc network

0 引言

移动自组网不需要固定的基础设施,组网方便快捷,被广泛地应用于军事、抢险救灾、科学探索等领域。然而正是这种优势导致其很容易受到攻击者的各种破坏,若不能提供有效安全机制将制约移动自组网的进一步发展。因此移动自组网的安全问题成为当前研究的热点,其中群组密钥管理是移动自组网安全研究的主要任务之一。

移动自组网的群组密钥管理需要在节点被撤销和加入时,及时更新群组会话密钥以满足组密钥的安全需求。由于移动自组网的工作环境恶劣,网络存在较大延迟,而且节点不可避免地会暂时无法连通到网络,导致节点离开时拥有的群组密钥成为历史组密钥;重新连通到网络后为了恢复遗失的组密钥,需要请求组管理者(Group Manager, GM)重发遗失的密钥更新消息,这样不仅增加了网络中的流量和组管理者的负担,还容易遭到恶意攻击者对组管理者的拒绝服务攻击。为了有效地避免这种攻击,需要在群组密钥管理中实现组密钥自愈功能。

文献[1]首次提出密钥自愈分发机制:合法节点利用自身存储的秘密信息和当前广播消息可以恢复出组密钥,而被撤销的和未授权的非法用户是无法根据广播消息获得组密钥,重新连通到网络的合法节点不借助GM可以独立地恢复出遗失的组密钥。文献[2-4]在文献[1]基础上提出了密钥自愈分发机制的形式化定义和需要满足的安全属性。但是在以上方案中,被撤销的节点不允许参与到之后的群组会话。文献[5-7]基于Hash链,提出计算上安全的自愈群组密钥分发机制,使广播的信息中不再包含历史组密钥的冗余关联。

信息,降低了网络通信代价和节点存储代价,但被撤销节点和新加入节点能够合谋恢复出对它们来说是非法的组密钥。文献[8]在实现密钥自愈的同时,能够抵抗合谋攻击,但通信代价较大。文献[9]假定组控制者预先设定了节点的生命周期,给出了能够抵御合谋攻击的密钥自愈分发方案。但节点被要求只能在生命周期结束后退出网络,不适合移动自组网的动态性。

本文提出具备抵御合谋攻击能力的自治愈组密钥管理方案。它能够容忍不可靠信道下密钥更新消息的丢失,实现自愈;被撤销节点和新加入节点合谋也无法计算出它们不应该知道的组密钥;同时,允许被撤销的节点重新加入群组参与会话。

1 相关知识

单向密钥链^[10]是反复用一个单向散列函数H作用到一个随机密钥种子上而产生的密钥链,散列函数H能够把任意长的二元字符串转换成固定长的二元字符串,它满足以下属性:

- 1) 给定 x ,计算出 $y = H(x)$ 是容易的;
- 2) 给定 y ,要计算出满足 $H(x) = y$ 的 x 是困难的;
- 3) 给定 x ,很难寻找到一个 y ,且 $y \neq x$,使得 $H(x) = H(y)$ 。

GM首先随机选取一个密钥种子 s^F ,然后计算出一条长度为 m 的密钥链 $K_1 = H(s^F), K_2 = H(K_1) = H^2(s^F), \dots, K_m = H(K_{m-1}) = H^m(s^F)$ 。由于散列函数H的单向性,已知 K_i ,对于任意 $j < i$,得出 K_j 在计算上是不可行的,但对于任意 $j > i$,能有效计算出 $K_j = H^{j-i}(K_i)$ 。

收稿日期:2011-04-11;修回日期:2011-06-21。 基金项目:国家自然科学基金资助项目(60873233);。

作者简介:曹帅(1987-),男,甘肃平凉人,硕士研究生,主要研究方向:信息安全、移动自组网络安全; 张串绒(1965-),女,陕西眉县人,教授,博士,主要研究方向:密码学、信息安全; 宋程远(1987-),女,山东东营人,硕士研究生,主要研究方向:信息安全、传感器、网络安全。

2 抗合谋攻击的自治愈群组密钥管理方案

设群组中的节点集合为 $U = \{U_1, U_2, \dots, U_n\}$, GM 的公私钥为 (PK, SK) , 节点 U_i 的公私钥为 (PK_i, SK_i) , 并将网络划分为 m 个会话阶段, 其中 j 时段的组密钥为 K_j 。该方案分为以下 4 个部分。

2.1 建立

GM 从有限域 F_q 随机选取前向密钥种子 s^F 和安全的散列函数 $H(\cdot) : F_q \rightarrow F_q$, 随机选择 m 个独立不相关的 t 阶多项式 $\{f_j(x) = a_{j,0} + a_{j,1}x + \dots + a_{j,t}x^t\}_{j=1,2,\dots,m} \in F_q[x]$ 。假设节点 U_i 是在会话 j_1 时段加入到群组中, 则 GM 为节点 U_i 计算秘密份额 $f_j(id_i)_{j=j_1,\dots,m}$ 和前向散列值 $k_{j_1}^F = H^{j_1}(s^F)$, 其中 id_i 是 GM 为节点 U_i 随机选择的秘密身份信息。之后 GM 用其公私钥和文献[11] 中的签密算法, 签密消息 $\{f_j(id_i)_{j=j_1,\dots,m}, id_i, s_{j_1}^F\}$ 发送给 U_i 。 U_i 用它的公私钥解签密消息之后将 $\{f_j(id_i)_{j=j_1,\dots,m}, id_i, s_{j_1}^F\}$ 作为它的秘密信息。

2.2 广播

GM 为 j 时段的会话选择随机数 β_j , 计算 $K_j = \beta_j + s_j^F$ 作为会话 j 时段的组密钥。

设 R_j 为在会话 j 时段被撤销的节点的集合, $|R_j|$ 表示集合 R_j 中的元素个数, 其中 $|R_j| \leq t$ 。记 $U' = U - R_j$ 为当前会话群组中未被撤销的合法节点集合。GM 计算并广播消息:

$$\beta_j = \{p_i(x) = A_i(x)\beta_i + f_i(x)\}_{i=1,2,\dots,j} \quad (1)$$

其中: $A_j(x) = \prod_{x \in U'} (x - id_x) + 1$ 为撤销多项式, id_x 为在会话 j 时段所有合法节点的秘密身份信息。显然, 若节点 $U_i \in U'$, 则 $A_j(x) = 1$; 否则, $A_j(x)$ 为随机数。

2.3 组密钥的计算

若节点 U_i 在 j_1 时段加入群组, 在会话 j 时段若还未被 GM 撤销 ($1 \leq j_1 \leq j$), 则节点 U_i 可以根据 j 时段的广播消息 B_j 和自身存储的秘密信息, 通过以下步骤计算得到 j 时段的组密钥 K_j :

1) 节点根据自己秘密身份信息 id_i , 可以从式(1)中计算得到 $p_j(id_i)$ 和 $A_j(id_i)$, 然后根据 $f_j(id_i)$, 可以计算出:

$$\beta_j = \frac{p_j(id_i) - f_j(id_i)}{A_j(id_i)} \quad (2)$$

2) 根据私密信息 $s_{j_1}^F$, 计算前向 Hash 值:

$$k_{j_1}^F = H^{j-j_1}(s_{j_1}^F) \quad (3)$$

3) 计算会话 j 时段的组密钥 $K_j = \beta_j + k_{j_1}^F$ 。

2.4 新节点的加入

如果一个节点 U_k (可以是会话 j 时段之前被撤销的节点) 在会话 j_1 时段加入群组, 通过 GM 的认证之后, GM 随机选择一个从未使用过的 id_k , 计算 $f_j(id_k)_{j=j_1,\dots,m}$ 和 $s_{j_1}^F$ 。用签密的方式发送秘密信息 $\{id_k, f_j(id_k)_{j=j_1,\dots,m}, s_{j_1}^F\}$ 给 U_k 。

3 方案分析

3.1 密钥的自愈性

假设节点 U_i 在会话 j_1 时段加入群组, 并在会话 j_2 时段之后被撤销。由于网络原因, 节点 U_i 未收到 $(j_1 < j < j_2)$ 时段的组密钥更新消息, 只接收到了 j_2 时段的组密钥更新消息 B_{j_2} 。

由于 U_i 在会话 $j_1 < j < j_2$ 时段只是临时掉线, 并未被 GM 撤销, 则其还是合法的群组成员。

显然 U_i 利用 j_2 时段的广播消息 $B_{j_2} = \{p_i(x) = A_i(x)\beta_i + f_i(x)\}_{i=1,2,\dots,j_2}$ 和自己的秘密信息 $\{f_j(id_i)_{j=j_1,\dots,m}, id_i, s_{j_1}^F\}$, 根据式(2)~(3) 可计算出正确的 β_j 和 s_j^F ($j_1 < j < j_2$), 从而计算出丢失的 $(j_1 < j < j_2)$ 时段组密钥 $K_j = \beta_j + k_j^F$ 。因此该方案实现

了组密钥的自愈性。

3.2 安全性分析

3.2.1 前向安全性

若节点 U_i 在 j_2 时段被撤销, 根据自己的秘密信息和 j ($j_2 < j$) 时段的广播信息 B_j 计算出 j 时段的组密钥是不可能的。因为 U_i 在 j 时段不是合法用户, 撤销多项式 $A_j(x)$ 的值将是一个随机数, 所以 U_i 无法计算出新的组密钥 K_j , 即实现了组密钥的前向安全性。

3.2.2 后向安全性

对于在 j_1 时段新加入的节点 U_k , 想得到会话 j_1 时段之前的组密钥:首先, 必须得到 j 时段的随机数 β_j ($j < j_1$), 显然在会话 j 时段该节点在非法节点集合中, 无法得到正确的 β_j ; 其次, 根据 Hash 函数的单向性, 是无法从自身的私密信息 s_{j+1}^F 计算得到 s_j^F 的。因此, 用户 U_k 无法计算出加入群组之前的会话组密钥, 从而实现了组密钥的前向安全性。

3.2.3 抗被撤销节点和新加入节点的合谋攻击

设 $B \subseteq (R_{j_1} \cup R_{j_1-1} \cup \dots \cup R_1)$ 表示在会话 j_1 时段和其之前被撤销节点的集合, 其中 $C \subseteq (J_{j_2+1} \cup J_{j_2+2} \cup \dots)$ 表示在会话 j_2 时段之后加入群组的节点集合, 其中 $|B \cup C| \leq t$, $j_1 < j_2$ 。如图 1, 合谋攻击就是在 j_1 时段及该时段之前被撤销的节点和在 j_2 时段之后新加入的节点合谋想得到它们本不应该知道灰色部分会话 $(j_1 < j < j_2)$ 时段的组密钥。要获得 $(j_1 < j < j_2)$ 时段的组密钥 K_j , 必须知道该时段的 β_j 和 s_j^F : 显然集合 B 中节点能够计算出 s_j^F , 然而 $B \cup C$ 中的节点虽然拥有 $(j_1 < j < j_2)$ 时段的 $f_j(id_x)$ 和公共信道中的广播消息 B_j , 却无法获得正确的 β_j , 因为在 $(j_1 < j < j_2)$ 时段 $B \cup C$ 无法计算出正确的 β_j ; 此外, 若 $B \cup C$ 想通过恢复 j 时段的多项式 $f_j(x)$ 来暴力破解得到 j 时段合法成员的 id , 需要多项式 $f_j(x)$ 上的 $t+1$ 个点, 然而 $|B \cup C| \leq t$, 所以 $B \cup C$ 是无法恢复多项式 $f_j(x)$ 的。通过上面的分析可看出, $B \cup C$ 合谋是无法得到会话 $(j_1 < j < j_2)$ 时段的组密钥 K_j 。因此, 方案能够抵抗撤销节点和新加入节点的合谋攻击。

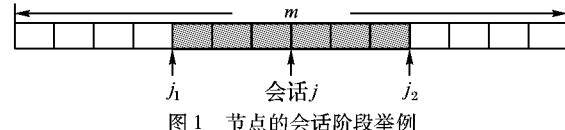


图 1 节点的会话阶段举例

3.3 性能分析

在自治愈组密钥管理方案中, 节点的计算代价由多项式运算和 Hash 运算组成, 由于多项式运算和 Hash 运算易于计算, 耗时短, 对于移动自组网的节点来说是完全可以承受的。因此这里只进行存储代价和通信代价的分析和比较。

3.3.1 节点的存储代价

节点 U_i 在会话 j 时段加入群组, 组管理者为其发送私密信息 $\{f_j(id_i)_{j=j_1,\dots,m}, id_i, s_{j_1}^F\}$, 因此节点的存储代价为 $(m - j + 3) \times \text{lb } q$ 。

3.3.2 网络通信代价

在该方案中, GM 在会话 j 时段广播的消息 B_j 包含 j 个 t 阶多项式, 因此通信代价为 $(t + 1)j \text{ lb } q$ 。由于在 j 时段广播的消息 B_j 中包含之前会话的组密钥更新信息, 该方案的通信代价较基于 Hash 链的自治愈密钥分发方案有所增加。

3.4 方案对比

表 1 给出了几种自愈密钥分发方案的比较。可看出, 文献[1~3, 8]的方案虽然能够抵御合谋攻击, 但是存储代价和通信代价比本文方案大, 且不支持被撤销节点的重新加入群组参与会话; 基于 Hash 链的文献[5, 7]方案虽然通信代价比本文方案小, 但却无法抵御合谋攻击。(下转第 2777 页)

好的应用价值和知识挖掘能力。

参考文献:

- [1] 孙吉贵, 刘杰, 赵连宇. 聚类算法研究 [J]. 软件学报, 2008, 19(1): 48–61.
- [2] 石剑飞, 闫怀志, 牛占云. 基于凝聚的层次聚类算法的改进 [J]. 北京理工大学学报, 2008, 28(1): 66–69.
- [3] SAVARESI S M, BOLEY D. A comparative analysis on the bisecting K-means and the PDDP clustering algorithms [J]. Intelligent Data Analysis, 2004, 8(4): 345–362.
- [4] 郭蕴华, 陈定方. 基于模糊聚类分析的客户分类算法研究 [J]. 计算机应用研究, 2005, 22(4): 52–53, 57.
- [5] JONYER I, COOK D J, HOLDER L B. Graph-based hierarchical conceptual clustering [J]. Journal of Machine Learning Research, 2002, 2: 19–43.
- [6] YU XIAOGAO, JIAN YIN. A new clustering algorithm based on KNN and DENCLUE [C]// Proceedings of 2005 International Conference on Machine Learning and Cybernetics. [S. l.]: MENDELEY, 2005, 4: 2033–2038.
- [7] 贺玲, 蔡益朝, 杨征. 高维数据聚类方法综述 [J]. 计算机应用研究, 2010, 27(1): 23–26, 31.
- [8] TAN PANG-NING, STEINBACH M, KUMAR V. 数据挖掘导论 [M]. 范明, 范宏建, 译. 北京: 人民邮电出版社, 2006: 336.
- [9] 蒋盛益, 李庆华. 一种基于引力的聚类方法 [J]. 计算机应用, 2005, 25(2): 286–288, 300.
- [10] RAVI T V, GOWDA K C. Clustering of symbolic objects using gravitational approach [J]. IEEE Transactions on Systems, Man, and Cybernetics, 1999, 29(6): 888–894.
- [11] 苏守宝, 刘仁金. 基于佳点集遗传算法的聚类技术 [J]. 计算机应用, 2005, 25(3): 643–645.
- [12] 谢储晖, 刘韬. 基于 K 均值和免疫算法的聚类分析 [J]. 兰州理工大学学报, 2005, 31(5): 87–90.
- [13] LI JUNLIN, FU HONGGUANG. Molecular dynamics - like data clustering approach [J]. Pattern Recognition, 2011, 44(8): 1721–1737.
- [14] WANG LEI, JI HUAN. An artificial immune cell model based C-means clustering algorithm [C]// Proceedings of the 7th World Congress on Intelligent Control and Automation. Piscataway, NJ: IEEE Press, 2008: 825–829.
- [15] 荣秋生, 颜君彪, 郭国强. 基于 DBSCAN 聚类算法的研究与实现 [J]. 计算机应用, 2004, 24(4): 45–46, 61.
- [16] EISEN M B, SPELLMAN P T, BROWN P O, et al. Cluster analysis and display of genome-wide expression patterns [J]. Proceedings of National Academy of Sciences of the United States of America, 1998, 95(25): 14863–14868.
- [17] GOLUB T R, SLONIM D K, TAMAYO P, et al. Molecular classification of cancer: Class discovery and class predication by gene expression monitoring [J]. Science, 1999, 286(5439): 531–537.
- [18] UC IRVINE MACHINE LEARNING REPOSITORY [EB/OL]. [2011-01-10]. <http://archive.ics.uci.edu/ml/datasets/Iris>.
- [19] Analysis of the microRNA that involved the tuberculosis or latent TB infection II [EB/OL]. [2011-01-10]. <http://www.ncbi.nlm.nih.gov/projects/geo/query/acc.cgi?acc=GSE25435>.

(上接第 2693 页)

表 1 几种自愈密钥分发方案对比

方案	存储代价	通信代价	是否抵御合谋攻击	是否支持被撤销节点的重新加入
文献[1]方案	$(m-j+1)^2lb\ q$	$(mt^2 + 2mt + m + t)lb\ q$	✓	
文献[2]方案	$(m-j+1)lb\ q$	$(2t+1)jlb\ q$	✓	
文献[3]方案	$(m)lb\ q$	$jt(1+t)lb\ q$	✓	
文献[5]方案	$(m-j+1)lb\ q$	$(t+1)lb\ q$		
文献[7]方案	$(v-l+3)lb\ q$	$(t+1)lb\ q$		✓
文献[8]方案	$(m-j+2)lb\ q$	$(t+1)j+jlb\ q$	✓	
本文方案	$(m-j+3)lb\ q$	$(t+1)jlb\ q$	✓	✓

4 结语

针对移动自组网无线信道的不可靠性和常见的节点间的合谋攻击, 本文提出一种可以抵抗合谋攻击的自治愈合群组密钥管理方案。通过分析看出: 在本方案中, 节点能够容忍密钥更新消息的丢失, 独立地恢复出遗失的组密钥, 实现了组密钥的自治愈性; 而且方案能够抵抗被撤销节点和新加入节点的合谋攻击, 解决了被撤销的节点重新参与后续会话的需求; 能够满足移动自组网络在较高丢包率的无线通信环境下的群组密钥管理安全属性。同时, 方案具有较小的存储和通信开销, 能够适应节点资源受限的移动自组网。但是随着网络中会话数的增多, 通信开销也随之递增, 因此降低方案的通信量是我们下一步工作的重点。

参考文献:

- [1] STADDONE J, MINERE S, FRANKLIN M, et al. Self-healing key distribution with revocation [C]// Proceedings of IEEE Symposium on Security and Privacy '02. Piscataway, NJ: IEEE Press, 2002: 241–257.
- [2] LIU D, NING P, SUN K. Efficient self-healing key distribution with revocation capability [C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 231–240.
- [3] BLUNDO C, ARCOP D, LISTO M. A new self-healing key distribution scheme [C]// Proceedings of the 8th IEEE Symposium on Computers and Communications. Piscataway, NJ: IEEE Press, 2003: 803–808.
- [4] BLUNDO C, ARCOP D, LISTO M. Design of self-healing key distribution schemes [J]. Designs, Codes and Cryptography, 2004, 32(1/2): 15–44.
- [5] DUTTA R, CHANG E C, MUKHOPADHYAY S. Efficient self-healing key distributions with evocation for wireless network using one way key chains [C]// Proceedings of the 5th International Conference on Applied Cryptography and Network Security. Berlin: Springer-Verlag, 2007: 385–400.
- [6] JIANG C, LIN M, SHI, SHEN X. Self-healing group key distribution with time-limited node revocation for wireless sensor networks [J]. Ad Hoc Networks, 2007, 5(1): 14–23.
- [7] 杜春来, 胡铭曾, 张宏莉, 等. 基于双向散列链具有撤销能力的自愈组密钥分发机制 [J]. 通信学报, 2009, 30(6): 33–36.
- [8] DU W, HE M, X. Self-healing key distribution with revocation and resistance to the collusion attack in wireless sensor networks [C]// Proceedings of the 2nd International Conference on Provable Security. Berlin: Springer-Verlag, 2008: 345–359.
- [9] DUTTA R, MUKHOPADHYAY S, DOWLING T. Generalized self-healing key distribution in wireless Ad Hoc networks with trade-offs in user's pre-arranged life cycle and collusion resistance [C]// Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks. Berlin: Springer-Verlag, 2009: 80–87.
- [10] LAMPORT L. Password authentication with insecure communication [J]. Communications of the ACM, 1981, 24(11): 770–772.
- [11] 张串续, 张玉清, 李发根, 等. 适应于 Ad Hoc 网络安全通信的新签密算法 [J]. 通信学报, 2010, 31(3): 31–36.