文章编号:1001 - 9081(2006)03 - 0574 - 03

一个基于权限的移动自组网门限信任模型

许 峰[1,2],谢冬莉[2],黄 皓[1],王志坚[2]
(1. 南京大学 计算机科学与技术系,江苏 南京 210093; 2. 河海大学 计算机及信息工程学院,江苏 南京 210098)
(njxufeng@163.com)

摘 要:探讨了移动自组网所特有的安全威胁,将 Shamir 秘密分割模型和权限思想相结合,提出了一个基于权限的门限信任模型,并提出了一种新的私钥分量刷新技术。分析结果表明,该模型在可信节点剩余很少时仍能完成网络中节点的认证,亦可避免攻击者获取足够的私钥分量进行非法认证。

关键词:移动自组网;信任模型;密钥更新
中图分类号: TP393.08 **文献标识码**:A

Threshold trust model based on weight in mobile ad hoc network

XU Feng[1,2], XIE Dong-li[2], HUANG Hao[1], WANG Zhi-jian[2]
(1. *Department of Computer Science and Technology, Nanjing University, Nanjing Jiangsu* 210093, *China*;
2. *College of Computer & Information Engineering, Hohai University, Nanjing Jiangsu* 210098, *China*)

Abstract: The security threaten for MANET(mobile ad hoc network) was discussed. Combined the secret dividing model and the weight idea, a threshold trustful model based on weight was proposed. A new refurbishing method for private key weight was put forward. The analysis shows that this model can avoid attackers getting enough weight for the private key for lawlessly validating and validate the network nodes when trust nodes remain small.

Key words: mobile ad hoc network; trust model; secret refresh

0 引言

移动自组网(Mobile Ad hoc Network,MANET)是一种新型的无线移动网络,与传统的无线移动网络不同, MANET 不依赖于固定的基础设施,而是一种完全自组织的网络。在 MANET 中,在同一无线覆盖范围内的节点(主机)可以直接通信,不在同一无线覆盖范围内的节点要通过其他接点路由,因此,在 MANET 中每个节点既是主机又是路由器。MANET 有以下特点:完全自组织;拓扑结构经常变化;信任分散;带宽有限;能源有限。

1 信任问题

在基于 PKI 的网络中采用“信任第三方”方案。在这种机制下,所有的节点都拥有一个公开/秘密密钥对,它们彼此用公开密钥来鉴别对方,但公开密钥的真实性却不一定能保证。所以,就需要有一个可信任的实体来管理所有的公开密钥,这个可信任实体叫作证书授权机构(CA)。这个可信的 CA 给每个节点签发一个证书用来绑定用户标识和公开密钥。这个 CA 本身有一个公开/秘密密钥对,并且所有的节点都知道 CA 的公开密钥。这样,如果节点之间要进行通信,它们可以从 CA 上获得对方的公开密钥来鉴别对方。然而,在 MANET 网络中情况要复杂一些,因为所有的节点都容易受到攻击,也容易被俘获。如果在 MANET 中采用一个 CA 来管理整个网络节点的公开密钥,那么,这个 CA 节点要是被俘获了,整个网络也就崩溃了。因此在 MANET 中采用信任分散的思想,即单独的节点是不可信的,节点的集合是可信的。

2 Shamir 的 (T,N) 门限模型[1]

设 $S(S \geqslant 0)$ 为密钥,把 S 秘密分割成 n 份,任意 t 个密钥分量能恢复出密钥,Shamir 秘密分割方法可描述为:

1) 选取素数 $P > \max(S,n)$, 定义 $a_0 = S$;

2) 随机选取素数 $a_1, a_2, \cdots, a_{t-1}$, $0 \leqslant a_j \leqslant P-1, 0 \leqslant j \leqslant t-1$;

3) 构造多项式 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$;

4) 计算 $yi = f(xi) \bmod P, 1 \leqslant x_i \leqslant n$,把 (xi, yi) 分配给节点 Pi, 销毁 $a_0, a_1, a_2, \cdots, a_{t-1}$。

密钥恢复过程可描述为:根据拉格朗日差值定理,任 t 个不同的点 (xi, yi) 可以计算出多项式 $f(x)$ 系数 a_j:

$$f(x) = \sum_{i=1}^{t} yi \prod_{j=1, j\neq i}^{t} \frac{x - xj}{xi - xj} (\bmod P) \quad (1)$$

$$S = f(0) = \sum_{i=1}^{t} yi \prod_{j=1, j\neq i}^{t} \frac{-xj}{xi - xj} (\bmod P) \quad (2)$$

这样多于或等于 t 个密钥分量能生成认证密钥而少于 t 个密钥分量不能生成认证密钥。用系统公钥验证秘密分割的正确性。

3 移动自组网中基于权限的门限信任模型

用 $M(m, n, t)$ 表示模型,m 代表网络中节点数;n 代表系统私钥被秘密分割的份数;t 代表在 n 份密钥分量中大于等于 t 个密钥分量能完成系统签名,认证。这里 $m \leqslant n, t \leqslant n$。

3.1 基于权限的门限信任模型的思想

现有的文献对秘密分割门限模型的研究中一般将 n 份密

收稿日期:2005 - 09 - 17 **修订日期**:2005 - 11 - 21
基金项目:国家自然科学基金资助项目(60473091);国家 863 计划项目(2003AA142010)

作者简介:许峰(1975 -),男,陕西府谷人,博士研究生,主要研究方向:分布式计算、信息安全; 谢冬莉(1977 -),女,河南郑州人,硕士研究生,主要研究方向:网络信息安全; 黄皓(1957 -),男,江苏海门人,教授,博士生导师,主要研究方向:计算机网络、信息安全; 王志坚(1958 -),男,江苏扬州人,教授,博士生导师,主要研究方向:软件自动、分布式计算.

钥分量分给 n 个节点,但在实际应用中,有时各个节点不能同等对待,如在战场上战斗机和普通坦克不应作为平等的节点来对待,将军和士兵应具有不同权限。因此在使用 Shamir 的 (T,N) 门限模型秘密分割私钥时,网络中 m 个节点应具有不同权限,权限的大小用拥有的密钥分量的个数决定,如节点 A(主席) 拥有 2 个密钥分量,节点 B(成员) 拥有 1 个密钥分量,则节点 A 的权限大于节点 B,只要有 t 个没被攻破的密钥分量就能完成系统的认证。

3.2　基于权限的门限信任模型的实现

假设:1) 系统由 m 个节点组成,系统中每个节点都有一对公私密钥对(Ki, ki),系统有一对公私秘钥(K, k),K 是公开的,k 用 *Shamir* 秘密分割方法分割成 n 份$(s1,s2,s3\cdots,sn)$;2) 对系统初始化是在安全的环境中进行;3) 节点被攻破后不会泄漏认证私钥和私钥分量给攻击者;4) 系统按照安全策略把 n 份密钥分量分给 m 个节点;5)系统中节点知道网络中所有节点的公钥;6)以 RSA 为签名方法为例。

如图 1 所示,节点 A 要和节点 B 通信,节点 A 首先要得到 B 的公钥,而节点 B 公钥的可信性要通过信任模型来验证。

1) 节点 A 向系统发出请求 request,包括节点 A 和节点 B 的标识等。

2) 系统中每个节点检查 request 的合法性,并对自己存储的关于 B 的信息(m) 用自己的私钥分量签名 $Si(m)$,如果该节点有 x 份密钥分量,则分别用这些密钥分量对 m 签名,然后发送给密钥恢复服务器 C(C 可以是系统中任意节点也可另行商定)。

3) 密钥恢复服务器 C 随机选取 t 个组成系统的签名,发送给 A。

4) 节点 A 用系统公钥验证系统签名,如果正确则接受 B 的公钥。

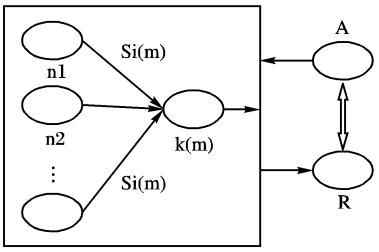

图 1　基于权限的门限信任模型

以 RSA 为例,说明模型签名的过程:

1) 初始化。选取大素数 p 和 q,计算 $n = pq$ 和 $\varphi(n) = (p-1)(q-1)$,选择 $K \in Z_{\varphi(n)}$ 且和 $\varphi(n)$ 互素,利用欧几里德扩展算法计算出 $k \in Z\varphi(n))$ 且 $Kk \equiv 1 \bmod \varphi(n)$。

2) 随机生成一个$(T-1)$ 阶多项式:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} \bmod \varphi(n)$$

其中 $a_0 = k$, $a_i \in Z*_{\varphi(n)}(i = 0,1,2,\cdots,T-1)$。

3) 随机选择互异的元素 $x_1, x_2, \cdots, x_N \in Z*_{\varphi(n)}$。计算 $y_i = f(x_i) \bmod \varphi(n)(i = 1, 2, \cdots, N)$。

4) 公开 n, K, $xi(i = 1, 2, \cdots, N)$, 并将 yi 秘密发送给相应的系统成员。

系统中节点签名 $si(m) = m^{yi} \bmod n$,计算 α_i和最终对消息 m 的签名:

$$\alpha_i = \prod_{j=1,\, j\neq i}^{t} \frac{-xi}{xi - xj} \bmod \varphi(n) \tag{3}$$

$$S(m) = \prod_{i=1}^{t} s_i^{\alpha_i}(m) \ (\bmod n) \tag{4}$$

证明签名的正确性:

$$m^{f(0)} = m\sum_{i=1}^{t} yi \prod_{j=1,\, j\neq i}^{t} \frac{-xj}{xi - xj} \bmod \varphi(n) =$$

$$\prod_{i=1}^{t} m^{y_i\alpha_i} = \prod_{i=1}^{t} s_i^{\alpha_i}(m) \ (\bmod n) = s(m) \tag{5}$$

3.3　密钥刷新技术

在移动自组网中基于权限的门限信任模型中,假设节点被攻破后不会泄漏密钥给攻击者,但实际应用中,攻击者完全有能力获得节点的私钥及私钥分量,甚至能在有限时间内获得 t 个密钥分量,从而可以假冒系统进行非法签名,认证。Lidong Zhou 等人采用如下的密钥刷新思想对系统的密钥分量进行周期性刷新[2~4]。

3.3.1　Lidong Zhou 密钥刷新思想

设$(s_1, s_2, s_3, \cdots, s_n)$ 是 $k1$ 的密钥分量,$(d_1, d_2, d_3, \cdots, d_n)$ 是 $k2$ 的密钥分量,则 $k1 + k2$ 的密钥分量表示为$(s_1 + d_1, s_2 + d_2, s_3 + d_3, \cdots, s_n + d_n)$,如果 $sum(d_1, d_2, d_3, \cdots, d_n) = 0$ 则代表 $k2 = 0$。因此如果 $k2 = 0$,则$(s_1 + d_1, s_2 + d_2, s_3 + d_3, \cdots, s_n + d_n) = (s_1, s_2, s_3, \cdots, s_n) + (d_1, d_2, d_3, \cdots, d_n)$ 仍是 $k1$ 密钥分量,表示为 $k1 = k1 + k2$。如图 2,设系统 $M(m,n,t)$, $(s_1, s_2, s_3, \cdots, s_n)$ 为系统的密钥分量,节点 S 拥有 s_i 节点 S 随机生成 0 的(T,N) 密钥分量$(s_{i1}, s_{i2}, s_{i3}, \cdots, s_{in})$, $sum(s_{i1}, s_{i2}, \cdots, s_{in}) = 0$, 即图中第 i 列,将每个 s_{ij} 安全分送给拥有 s_j 的节点,则拥有 s_j 的节点得到$(s_{1j}, s_{2j}, \cdots, s_{ij}, \cdots, s_{nj})$ 新密钥 $s_j' = s_j + sum(s_{1j}, s_{2j}, \cdots, s_{ij}, \cdots, s_{nj})$,从而完成密钥分量的刷新。

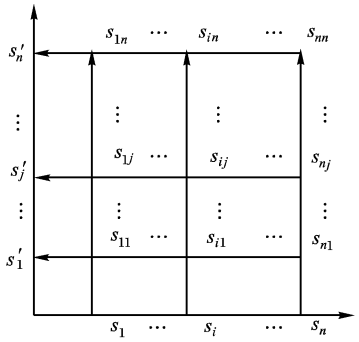

图 2　密钥分量更新过程

这样周期地刷新密钥,更新后的密钥和更新前的密钥不能恢复出系统私钥,攻击者只有在系统刷新密钥的周期间隔内收集到 t 个密钥分量才能恢复出系统密钥,合理的周期刷新时间能避免攻击者获得 t 个当前时间有效密钥分量。系统的密钥刷新还可以周期性地更换系统内节点,从而形成一个新的系统。但是,这种密钥刷新技术涉及到大量的计算,系统中每个节点到要生成 0 的密钥分量,如果某节点有很多份密钥,则该节点就要计算很多密钥分量。为此,我们在上述密钥刷新的基础上提出一种新的密钥刷新思想。

3.3.2　基于权重的密钥刷新思想

设系统 $M(m, n, t)$, $(s_1, s_2, s_3, \cdots, s_n)$ 为系统的密钥分量,节点 S 拥有 s_i,设在某密钥刷新周期内我们根据欺负算法[5] 的思想选取一个可信节点,由该节点产生 0 的密钥分量 $(w_1, w_2, \cdots, w_n)$ 并安全地按节点的权重分发该系统内节点,新的密钥分量 $s_i' = s_i + w_i$。

设系统中某时刻节点的性能(*capbility*) 用节点的计算能力(V_{cal})、权重(V_{wei}) 和安全性(V_{sec}) 来衡量,我们定义:$capbility = V_{sec} * R_{sec} + V_{cal} * R_{cal} + V_{wei} * R_{wei}$,其中 R_{sec} 代表

安全的比率;R_{cal} 代表计算能力的比率;R_{wei} 代表该节点的权重所占的比率。

假设 t 时刻系统中有 8 个节点,每个节点都维护这一张记录系统中其他节点的 *capbility* 的表,这张表在每个密钥刷新末更新。系统初始化时选取 *capbility* 最大的节点产生 0 的密钥分量(w_1, w_2, …, w_n) 并安全的按节点的权重分发该系统内节点,新的密钥分量 $s_i' = s_i + w_i$。如果在系统运行期间该节点被占领或改节点的 *capbility* 下降到指定门限值则用欺负算法的思想重新选取一个可信节点来产生 0 的密钥分量(w_1, w_2, …, w_n),以拥有 *capbility* = 7 的节点变得不可用时新节点选取情况为例。

当拥有 *capbility* = 7 的节点被攻破的情况:拥有 *capbility* =4 的节点首先发现拥有 *capbility* = 7 的节点被攻破,则它发起选举请求,系统中各节点重新计算各自的 *capbility* 并广播给其他节点,收到消息的节点会根据消息的内容更新 *capbility* 表,并查找出最大的 *capbility* 值的节点,则拥有当前最大 *capbility* 值的节点为选举出的下一轮产生 0 的密钥分量(w_1, w_2, …, w_n) 的节点。

当拥有 *capbility* = 7 的 *capbility* 下降到指定门限值的节点的情况和上述情况类似,只是发起选举的节点为它本身。

通过这种密钥刷新技术刷新系统密钥,可以减少节点的计算量,同时进一步保证密钥刷新计算过程的高效性,每次选取的可信节点如果在密钥刷新时间被攻破,则通过下一次的密钥刷新过程来刷新系统密钥。

4 结语

目前,针对移动自组网中的信任模型问题,国际上主要有 Shamir 提出的门限秘密分享方案;Feldman 提出的可验证秘密分享方案(VSS);Canetti 提出的主动秘密分量更新方案以及可变门限秘密分享和分布式产生秘密的秘密分享方案等。在国内,中国科学院、上海交通大学、武汉大学、华中科技大学、解放军理工大学及西安电子科技大学 ISN 国家重点实验室等诸多研究机构就移动自组网中的信任模型、密钥协商、密钥分发和密钥托管等进行研究,提出了各自的方案。但已有的方案都假设移动自组网系统中节点都是平等的,而在实际应用中节点有可能是不平等的。

本文针对网络中节点不平等的 MANET 提出了一种基于权限的门限信任模型,该模型在可信节点剩余很少时仍能完成网络中节点的认证,同时在已有的密钥刷新技术的基础上提出了一种新的密钥刷新思想。

参考文献:

[1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612 - 613.

[2] ZHOU L, HASS ZJ. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13(6): 24 - 29.

[3] FRANKEL Y, GEMEL P, MACKEZIE P, *et al*. Optimal resilience proactive public-key cryptosystems[A]. Proceedings of the 38th Symposium on Foundations of Computer Science[C]. Miami Beach, FL USA, 1997. 384 - 393.

[4] ZHOU L. Towards Fault-Tolerant and Secure On-Line Services[D]. Cornell University, 2001.

[5] ZHOU L, SCHNEIDER FB, van RENESSE R. Technical Report 2000-1828, COCA: A secure distributed on-line certification authority[R]. Department of Computer Science, Cornell University, Ithaca, NY USA, 2000.

(上接第 568 页)

6) 如发现协同入侵事件,则分发到已注册的监控引擎,同时将该事件存入协同入侵事件库中;

7) 当挖掘出新规则时,调度引擎负责调用目录服务模块进行规则分发;

8) 各监控引擎接收到新的规则时,将其转化为本地规则,添加到规则库中。

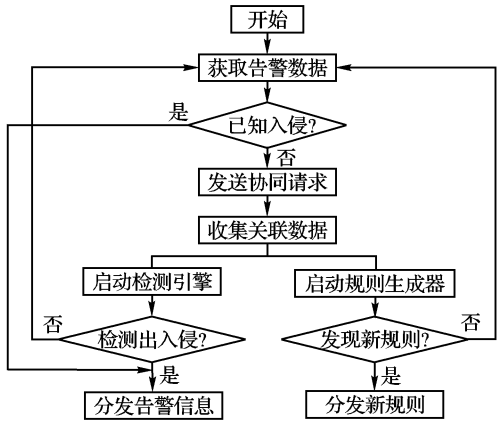

图 3 协同调度流程

2.8 协同机制的优点

单个入侵检测系统无法检测到的复杂攻击,可以通过协作,获取其相关事件,提供更全面丰富的数据支持,从而得出结论,这使得整个系统的检测能力获得提升。

告警信息的分发,是把在一处发现的攻击提前通知给其他监控引擎,使得能在入侵攻击的实施过程中检测到它,并采取相应的措施进行防御。

在控制中心,由基于数据挖掘的协同入侵检测模块所生成的新规则能及时地分发给所有监控引擎,快速地使系统抵御新的攻击。

3 结语

本文所讨论的开放式多主体协同入侵监控平台在传统检测引擎的基础上提出了包装器的概念和引擎间的协同机制,可以有效、方便地集成现有的入侵检测系统,也容易进行扩充。通过协同调度机制,使系统能实现对新的分布式攻击的检测,并能够快速地在整个系统内共享信息,使整个系统在检测性能、准确性、完备性和及时性等方面都有很大提升。

参考文献:

[1] PARK S-K, KIM K-Y, JANG J-S. Supporting Interoperability to Heterogeneous IDS in Secure Networking Framework [Z]. IEEE, 2003.

[2] WU J-S. The Neuron Security of Joint Defense for Network Intrusion Detection[Z]. IEEE, 2003.

[3] FEIERTAG R, RHO S, BENZINGER L. Intrusion Detection Inter-component Adaptive Negotiation[J]. Computer Networks, 2000, 34(4): 605 - 621.

[4] The Intrusion Detection Message Exchange Format draft-ietf-idwg-idmef-xml-12[S/OL]. http://www.ietf.org, 2005 - 04.

[5] The Intrusion Detection Exchange Protocol (IDXP) draft-ietf-idwg-beep-idxp-07[S/OL]. http://www.ietf.org, 2005 - 04.