基于可转换三元多项式的WSN密钥管理方案

方赵林[1] 谢红军[2]

(浙江工业大学网络中心 杭州 310023)[1] (浙江工业大学计算机科学与技术学院 杭州 310023)[2]

摘 要 基于三元多项式的无线传感器密钥管理方案,由于拥有相同多项式的节点使用同一共享会话密钥,很难抵御节点捕获攻击,又由于通信开销大而不具有可扩展性。为了克服这些不足,提出了基于可转换三元多项式无线传感器网络(WSN)动态密钥管理方法,它保证拥有相同多项式的所有节点能够获得相同的管理密钥,拥有相同多项式的任意两个节点能够获得不同的共享会话密钥。分析表明,与基于三元多项式的方案相比,该方法总体上增强了抵御节点捕获攻击的能力,降低了通信开销。

关键词 可转换三元多项式,EBS,无线传感器网络

Key Management Scheme for WSN Based on Convertible Ternary Polynomial

FANG Zhao-lin[1] XIE Hong-jun[2]

(Campus Network Center, Zhejiang University of Technology, Hangzhou 310023, China)[1]

(Department of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China)[2]

Abstract Because all nodes having the same polynomial use the same shared session keys, schemes designed for wireless sensor networks based on the ternary polynomial are vulnerable to the node capture attacks. They are lack of performance scalability in terms of communication overhand. To address these limitations, a new dynamic key management proposal was designed for wireless sensor networks based on the convertible ternary polynomial, which can guarantee that all nodes having the same polynomial can get the same administration keys and two nodes having the same polynomial can get shared session keys. Compared with the schemes based on the ternary polynomial, the proposed scheme can greatly defend against the node capture attacks overall and reduce communication overhand.

Keywords Convertible ternary polynomial, Exclusion base system, Wireless sensor networks

1 概述

无线传感器网络(Wireless Sensor Networks, WSN)是由大量分布式传感节点组成的面向任务型自组织网络。无线传感器网络有可能被部署在敌占区域。为了保证节点之间的通信安全,需要对节点之间的通信进行加密。

目前常用的对称密钥管理方案主要有:①基于密钥预分配方案[1-3],②基于多项式密钥分配方案[4-9]。普通EBS密钥管理方法[3],由于密钥在拥有相同密钥的节点之间共享,无法抵抗节点捕获攻击。基于三元多项式的无线传感器网络密钥管理方法[4]用三元多项式密钥代替EBS中的普通密钥,增加了计算密钥的难度,但具有相同多项式的节点仍然共享相同的会话密钥。管理密钥主要用于会话密钥的更新和节点的驱除,会话密钥主要用于节点之间通信信息的加密。相对于管理密钥,会话密钥使用更加频繁,具有相同多项式的节点共享相同的会话密钥严重影响了这种方案总体抵抗节点捕获攻击的能力。本文提出了基于可转换三元多项式WSN密钥管理方案。具有相同多项式的节点有相同的管理密钥。具有相同多项式的任意两个节点的会话密钥都不相同。本方案能够比较方便地增加和驱除节点,动态更新管理密钥和会话密钥。与基于三元多项式的WSN密钥管理方案相比,它总体上增强了抵抗节点捕获攻击的能力,降低了通信开销,非常适合大规模无线传感器网络。

1.1 可转换三元多项式

定义1 $f(x,y,z)$为$t+1$阶可转换三元多项式,若$f(x,y,z)=cz(x_c-z) \bmod q$,其中$x_c$为一常数,$c,a_{ij}$属于有限域$F(q)$($q$是一个大素数)。可转换三元多项式具有两条重要的性质:

①当$z=x_c$时,多项式$f(x,y,z)$值为常数cx_c。

②$f(x,y,z)=f(y,x,z)$。

对小于$2t+1$个相同系数的多项式进行计算是无法求出多项式系数的,所以多项式$f(x,y,z)$是$2t+1$安全的。

2 基于可转换三元多项式的WSN密钥管理方案

利用可转换三元多项式代替由Eltoweissy等[3]提出的EBS中的普通密钥,提出了一种新的动态密钥管理方法,并将这种方法应用于无线传感器网络。文中的无线传感器网络采用层次化模型,由基站、簇头、普通节点组成。整个网络分若干簇,每个簇由若干普通节点组成。簇内密钥管理与簇间密钥管理相同,本文只考虑由基站、簇头构成的簇间密钥管理,

方赵林(1972—),男,副主任,主要研究方向为网络技术及应用、计算机仿真,E-mail:fzl@zjut.edu.com;谢红军 男,硕士生。

包括密钥预分配、簇间会话密钥协商、节点增加和驱除、密钥更新。

2.1 密钥预分配

假如共有 n 个簇头节点，那么采用 EBS(n,k,m)，其中 k 表示分给每个节点多项式的个数，$k+m$ 表示密钥总数。基站随机生成 $k+m$ 个 $t+1$ 阶可转换三元多项式 $f_l(x,y,z)=c_l z+\sum_{i,j=0}^{t} a_{ij}x^i y^j(x_d-z)$。$l=1,2,\cdots,k+m$，系数互不相同。基站从中抽取 k 个多项式分配给每个簇头节点 CHa，将节点的标识 ID 代入多项式中计算得到 $t+1$ 阶二元多项式 $f(ID,y,z)$，存入簇头节点 CHa 中。基站广播自己的标识 ID_{BS} 和 x_d，当簇头节点 CHa 收到基站广播的报文后，将 $y=ID_{BS}$，$z=x_d$ 代入多项式 $f_l(ID,y,z)$ 中，生成管理密钥 $K=f(ID,ID_{BS},x_d)=c_l\cdot x_d$。

2.2 簇间会话密钥协商

在 $EBS(n,k,m)$ 中，任何两个簇头节点之间都至少存在一个系数相同的多项式。每个簇头都将自己的标识和一组多项式序号广播出去，当两个簇头具有相同的多项式序号时，这两个簇头就能够协商它们之间的共享会话密钥。假如簇头 CHa 广播报文：$\{ID_a,a_1,a_2,\cdots,a_k\}$，簇头 CHb 广播报文：$\{ID_b,b_1,b_2,\cdots,b_k\}$，其中 ID_a，ID_b 分别为簇头 CHa，CHb 的标识，$a_1,a_2,\cdots,a_k$ 为 CHa 拥有多项式的序号，$b_1,b_2,\cdots,b_k$ 为 CHb 拥有多项式的序号。若存在 $a_i=b_j;i=1,\cdots,k;j=1,\cdots,k$，拥有一个相同序号 a_i 的多项式 $f(x,y,z)$，当双方的 z 取默认值 0 时，三元多项式就转换成了二元对称多项式，簇头 CHa 将 ID_b 代入多项式 $f(ID_a,y,0)$ 中，簇头 CHb 将 ID_a 代入多项式 $f(ID_b,y,0)$ 中。这样簇头 CHa，CHb 就拥有共享会话密钥 $key=f(ID_a,ID_b,0)=\sum_{i,j=0}^{t} a_{ij}x_c ID_a^i ID_b^j=\sum_{i,j=0}^{t} a_{ij}x_c ID_b^i ID_a^j=f(ID_b,ID_a,0)$。

2.3 节点增加和驱除

2.3.1 新节点增加

基站从 $k+m$ 个多项式中取出 k 个多项式分给新增节点，新增节点通过 Hello 报文广播自己的标识和多项式序号，相邻节点收到它的 Hello 报文后，也广播自己的标识和一组多项式序号。这样新增节点与每个相邻节点之间就拥有了一个系数相同的多项式，通过计算以后，就能够获得共享密钥。

2.3.2 节点驱除

当网络中的入侵检测系统发现某个节点 CH_a 被捕获，基站发送 m 个数据包更新这个节点所拥有的 k 个多项式 $f_{aj}(ID_a,y,z)$，$j=1,2,\cdots,k$，其中的系数 C，从而驱除这个节点 CH_a。$b_1,b_2,\cdots,b_m$ 表示不包括在节点 CHa 中的多项式的序号，m 个数据包为 $x_{bi}||E_{Cbi}(x_{a1}||E_{Ca1}(c'_{a1}),\cdots,x_{ak}||E_{Cak}(c'_{ak}))$，$c'_{a1},c'_{ak}$ 为新的系数。当同时有 t 个节点被捕获时，每次发送 m 个数据包更新节点所拥有的 k 个多项式，逐一将节点驱除。

2.4 密钥更新

两个节点通过密钥协商拥有共享密钥，用这个密钥加密通过这两个节点的数据。为了延长网络的寿命，保证数据的安全，必须更新这个共享密钥，也就是更新二者拥有的相同系数的多项式。

方法与密钥预分配相似。基站广播 $k+m$ 个数据报，$x_i||E_{Ci}(x_1||E_{C1}(c'_{a1}),\cdots,x_k||E_{Ck}(c_k'))$，$i=1,2,\cdots,k+m$。

3 安全和性能分析

3.1 安全分析

簇头之间的会话密钥是通过计算二元对称多项式 $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x_l x_i y^j$，其中 x_l 为常数，得到的。会话密钥的安全性与二元对称多项式的安全性是一致的。二元对称多项式 $f(x,y)$ 的安全阈值 t，两个节点之间的会话密钥泄露不会影响具有相同多项式的其他节点之间会话密钥的安全。基于三元多项式的方案中，拥有相同多项式的节点共享同一个会话密钥，若具有相同多项式的任意两个节点之间的会话密钥被破解，其他节点之间的通信都能够被破解。

基站与簇头之间的管理密钥是通过计算可转换三元多项式得到的。管理密钥的安全性由可转换三元多项式的安全性决定。假如采用的 EBS 为 $EBS(n,k,m)$，被捕获的节点数为 N，任意一个多项式被分配给节点的概率为 $p=k/(k+m)$，在捕获的 N 个节点中，有 i 个节点拥有相同系数多项式的概率为 $f(i)=\binom{N}{i}p^i(1-p)^{N-i}$。由于可转换三元对称多项式是 $2t+1$ 安全的，因此当 $N<2t+1$ 时，多项式的系数是无法破解的。当 $N\geqslant 2t+1$ 时，多项式被破解的概率 $P(N)=1-\sum_{i=0}^{2t+1} f(i)$。

与基于三元多项式的方案比较，本方案增强了会话密钥的安全性，总体上提高了节点抵抗被捕获攻击的能力。

3.2 计算开销分析

本方案中，通过两步计算分别得到管理密钥和会话密钥。

(1)获取基站的广播报文中的 z，通过 $2(t+1)$ 次加法运算和 $2(t+1)(t+2)$ 次乘法运算得到 $c\cdot z$。

(2)将密钥协商双方的节点标识 ID，代入 $f(x,y,0)=\sum_{i,j=0}^{t} x_c x^i y^j$，经过 $(t+1)(t+2)$ 次乘法运算和 $t+1$ 次加法运算得到会话密钥。

本方案与基于三元多项式方案的计算开销基本相同。

3.3 通信开销分析

基于三元多项式的方案需要基站广播 $k+m$ 个数据包即 $\{x_{ci}||E_{Ci}(S_0),i=1,\cdots,k+m\}$，通过解密获得会话密钥 S_0，这一过程需要的通信开销随着 $k+m$ 值呈线性增加。本方案与基于三元多项式的方案在会话密钥协商过程中的通信开销基本相同。本方案的通信开销低于基于三元多项式的方案。

结束语 本文提出了基于可转换三元多项式 WSN 密钥管理方案。与基于三元多项式的 WSN 密钥管理方案相比，在没有增加计算开销的基础上，它总体上增强了抵抗节点捕获攻击能力，降低了通信开销。继续研究节点多项式分配优化方法，进一步增强抵抗节点捕获攻击能力。

参 考 文 献

[1] Jolly G, Kuscu M C, Kokate P, et al. A low-energy management

protocol for wireless sensor networks[J]. IEEE,2003:335-340

[2] Nguyen H T T, Guizani M, Jo M, et al. An Efficient Signal-Range-Based Probabilistic Key Predistribution Scheme in a Wireless Sensor Network[J]. IEEE Transactions on Vehicular Technology,2009,58(5)

[3] Eltoweisy M, Heydari H, Morales L, et al. Combinatorial optimization of key management in group communications[J]. Journal ol Network and Systems Management,2004,12(1):33-50

[4] 孔繁瑞,李春丈,丁青青,等. 一种基于 EBS 的无线传感器网络动态密钥管理方法[J]. 电子与信息学报,2009,31(5)

[5] 孔繁瑞,李春文,焦飞,等. 基于 EBS 的动态密钥管理方法共谋问题[J]. 软件学报,2009,20(9)

[6] 黄少清,李继国. 基于二元对称多项式的 WSN 密钥管理方案[J]. 计算机工程,2010,36(16):145-147

[7] 肖德贵,杨金,罗娟. 基于多项式和分组的无线传感器网络密钥管理方案[J]. 计算机应用研究,2009,26(2)

[8] Cheng Y, Agrawal D P. A improved key distribution mechanism for large-scale hierarchical wireless sensor networks[J]. Journal of Ad Hoc Networks,2007,5(1):35-48

[9] Shen A-N, Guo Song, Chien H Y, et al. A scalable key pre-distribution mechanism for large-scale wireless sensor networks [Z]. Wiley InterScience. DOI:10.1002/cpe.142, April 2009

(上接第 55 页)

表 3 纵深防御关键技术

类型	名称	技术说明
信息加密技术	加密算法	采用加密算法包括:对称/非对称密码算法、公开密钥数字签名算法、数字签名与数字信封、数字证书等
	公钥基础设施(PKI)	由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成,主要包括:X.509 格式证书和证书废止列表 CEL、CA/RA 操作协议、CA 管理协议和 CA 政策制定四个部分
	数据库加密	主要通过操作系统(OS)、数据库管理系统(DBMS)内核层和外层实现对数据库数据的加密
	虚拟专用网(VPN)	VPN 的重要意义在于"虚拟"与"专用",实现其技术的要点包括:隧道、相关隧道协议(PPTP、L2F、L2TF、VTP)和数据安全协议
网络隔离技术	物理隔离	实现物理隔离的常见技术包括:双网机隔离与交换技术、单主板安全隔离计算机技术、网络安全隔离卡技术和物理隔离集成器技术等
	防火墙	主要包括:包过滤、应用级网关、电路级网关和规则检测防火墙四种类型,需要依据实际需求具体使用
主动防御技术	入侵检测系统(IDS)	入侵检测系统分为:基于主机的 IDS(HIDS)和基于网络的 IDS(NIDS)。HIDS 主要用于防止对单机节点的入侵,检测目标主要是主机系统和本机用户;NIDS 主要用于防止对网络的入侵,从防火墙内部或外部监视整个网络运行
	入侵防御系统(IPS)	入侵防御系统分为:基于主机的 IPS(HIPS)和基于网络的 IPS(NIPS),实现功能包括:识别非授权业务流;主动阻断或降低对所识别的非授权业务流的服务;实时记录业务流状况,并及时向网络管理员发出警报;提供与异常数据包相关的分析数据等
	蜜罐	蜜罐可分为产品型蜜罐和研究型蜜罐,产品型蜜罐的目的在于为网络提供安全保护,包括检测攻击、防止攻击造成破坏及帮助管理员对攻击做出正确的响应;研究型蜜罐则是专门用于对黑客攻击的捕获和分析,分析和追踪黑客攻击能捕获黑客的键击记录,从而掌握其攻击目的、心理状态等信息
	蜜网	蜜网是在蜜罐技术基础上发展起来的,又称为诱捕网络,构成一个黑客诱捕网络体系架构
	安全审计	主要对操作系统、数据库、网络设备、防火墙等项目的安全审计,从而有针对性地对网络运行状态和过程进行记录、跟踪和审查
	信息取证	其目的为阻止和减小攻击事件带来的影响,根据攻击者行动留下的痕迹寻找到攻击证据,最终找到攻击者,主要包括现场保护、数据分析、结果提交、数据恢复等过程
系统抗毁技术	容灾	利用地理上的分散性,在异地建立和维护一个备份系统以保证数据对"灾难"事件的抵御能力,可分为数据容灾和应用容灾两个层次
	容侵	目的是保证系统在遭受入侵攻击发生故障时也能正常工作,或以一种无害的、非灾难性的方式停止,主要包括入侵容忍和错误触发两方面

结束语 防空信息网络安全问题事关整个防空体系作战效能的发挥,因此是信息化条件下空防对抗作战对防空体系提出的新挑战与新课题。论文分析了防空信息网络安全的脆弱性,以及所面临威胁的严峻性,从而提出了构建防空信息网络纵深防御体系,建立了纵深防御广度模型和深度模型,并对纵深防御技术体系进行了初步探索,研究了相关关键技术。论文仅抛砖引玉,防空信息网络安全问题是一个复杂的系统问题,将随着攻防对抗技术和对抗手段的发展而不断发展,因此需要不断地探索与完善。

参 考 文 献

[1] 王凤山,王福田. 防空信息战概论[M]. 北京:航空工业出版社,2002

[2] 吕登明. 信息化战争与信息化军队[M]. 北京:解放军出版社,2004

[3] 姚红星,温柏华. 美军网络战研究[M]. 北京:国防大学出版社,2010

[4] 李雄伟. 网络对抗系统及其关键技术研究[D]. 北京:北京邮电大学,2005

[5] 吴晓平,陈泽茂,等. 信息对抗理论与防御[M]. 武汉:武汉大学出版社,2008

[6] 张菊荣,周俊佑. 美国"舒特"机载战场网络攻击系统透视[R]. 西安:空军工程大学,2010

[7] 郭庆丰. 透过美国空军"舒特"计划探析战场网络战[J]. 空军装备研究,2010,4(2):58-61

[8] 秦立军. 信息安全保密系列谈[M]. 北京:金城出版社,2002

[9] 赵磊. 校园网纵深防御体系的研究与实现[D]. 北京:北京交通大学,2009

[10] 张世永. 网络安全原理与应用[M]. 北京:科学出版社,2003

[11] 李建. 美国海军计算机网络防御体系分析及启示[C]//知远战略与防务研究所,《网络战研讨会》论文集. 盐城,2010:50-67