无人值守无线传感器网络中可靠数据生存恢复方案

黄谊拉^{1,2}, 熊 焰¹, 陆琦玮¹

(1. 中国科学技术大学计算机学院, 合肥 230027; 2. 安徽艺术职业学院基础教育部, 合肥 230011)

摘 要: 无人值守无线传感器网络(UWSN)通常部署在环境恶劣或敌对环境中,在静态汇聚节点(或基站)部署困难的情况下,感知节点无法完成感知信息的实时汇聚传输,需暂时维持感知数据的生存状态。为增强数据生存概率,提高感知数据的抗损坏、擦除和篡改能力,在建立攻击模型假设的基础上,针对失效节点攻击假设,提出一种基于中国剩余定理加密密钥分割机制的可靠数据生存恢复方案。利用门限密钥分割存储机制增强密钥分割存储安全性,确保数据加密分割生存的可靠性,针对恶意节点攻击所造成的不可靠数据恢复威胁,构建基于恢复不一致性的恶意恢复攻击检测方案及基于多数表决的恶意恢复攻击识别机制,确保数据恢复的安全、可靠。

关键词: 无人值守无线传感器网络;数据生存;一致性恢复;中国剩余定理;门限秘密共享;恶意攻击

中文引用格式:黄谊拉,熊 焰,陆琦玮. 无人值守无线传感器网络中可靠数据生存恢复方案[J]. 计算机工程, 2015, 41(4):145-150,155.

英文引用格式:Huang Yila, Xiong Yan, Lu Qiwei. Dependable Data Survival Recovery Scheme in Unattended Wireless Sensor Network[J]. Computer Engineering, 2015, 41(4):145-150, 155.

Dependable Data Survival Recovery Scheme in Unattended Wireless Sensor Network

HUANG Yila^{1,2}, XIONG Yan¹, LU Qiwei¹

(1. School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China;
2. Basic Education Department, Artistic Vocational College of Anhui, Hefei 230011, China)

【Abstract】 Unattended Wireless Sensor Network(UWSN) are usually deployed in a bad or hostile environment. The deployment of static aggregation node (or base station) is difficult, resulting in real-time information aggregation impossible. Hence the node should undertake the mission of self-sustaining the data temporarily. In order to improve the probability of data survival, on the basis of a clear assumption of the adversary model, this paper proposes a reliable data survival scheme with the failure node hypothesis, using the Chinese Remainder Theorem(CRT) based threshold secret share mechanism. The malicious nodes recovery attack detection mechanism is proposed based on the property of recovery inconsistency. Furthermore, the identification scheme towards malicious attack based on majority voting mechanism is also designed. Therefore, it can ensure the robust data survival well.

【Key words】 Unattended Wireless Sensor Network (UWSN); data survival; consistent recovery; Chinese Remainder Theorem(CRT); threshold secret sharing; malicious attack

DOI:10.3969/j.issn.1000-3428.2015.04.027

1 概述

无线传感器网络(Wireless Sensor Network, WSN)由大量传感器节点组成,监测物理世界并获取感知数据,现已被广泛用以民用(如环境监测)及军事战争等领域。由于传感器节点往往部署于环境恶劣甚至敌对的环境中,通常无人值守,节点易遭损坏、俘获,失效概率高,因此有关无人值守无线传

感器网络(Unattended WSN, UWSN)中感知数据的有效生存和收集一直是学术界研究的热点。在诸如灾害和战争监测等实际应用中,因感知节点失效和损坏而由此导致的数据损失问题后果将非常严重。因此,研究此类条件下的数据生存显得非常必要。

在传统的WSN中,计算和存储能力都较强的基站将充当数据汇聚节点(Sink节点),固定存在于网络中以实时收集感知数据。在此情况下,感知节点能将感知

基金项目:国家自然科学基金资助重点项目“未来无线网络体系结构与关键技术”(61232018)。

作者简介:黄谊拉(1978-),女,讲师、硕士,主研方向:无线传感器网络;熊 焰,教授、博士;陆琦玮,博士。

收稿日期:2014-03-14 **修回日期:**2014-05-27 **E-mail:**hyila@ustc.edu.cn

数据及时汇聚传递给基站。然而,在 UWSN(部署于一些偏远的沙漠、高原、战场等恶劣敌对环境)中,上述静态汇聚节点部署困难且安全性无法得到可靠保证。汇聚节点(Sink 节点)仅能每隔一段时间(周期性)出现并与感知节点进行数据汇聚传输,因此感知节点由于无法实时地与汇聚节点或基站进行通信,无法实时完成感知数据的汇聚传输任务。在 Sink 节点未到来或汇聚传输条件未得到满足时,感知节点需自我负责维持数据的有效生存状态。显然,在恶劣的环境中,在感知数据汇聚传输成功之前,感知数据的生存将受到节点电源耗尽、自然灾害以及敌手破坏等问题挑战,感知数据将可能遭到更改、擦除等损害。因此,本文中数据生存问题即研究保证感知数据尽可能长时间保持完整、可恢复,并随后进行良好传输汇聚。

文献[1]提出了数据生存问题。文献[2]进一步将针对数据生存的攻击进行分类:数据隐私攻击,数据删除攻击和伪造,篡改数据攻击。文献[3-4]提出了基于数据复制的数据生存方案,但对于副本创建后的分发策略缺乏有效讨论。文献[5]提出了一种基于随机数据复制的数据生存方案,当节点从邻居节点接收到数据时,分别以概率 p, q 进行存储或者转发操作(p, q 相互独立)。文献[6]基于节点信誉度量机制来研究了数据复制概率 p, q 的合理设定。然而,上述基于数据复制的方案均依赖于数据副本的直接全复制,副本的存储、分发过程需消耗较大的网络和节点资源,且无法防止伪造、篡改攻击,抵御攻击能力有限。

文献[7-8]中针对上述伪造、篡改攻击设计了基于加密密码机制的数据生存方案,具体将感知数据加密并利用门限密码机制将加密密钥进行分割并分布式存储至节点中,利用攻击者必须俘获门限数目的节点方可重组加密密钥,因此数据的安全性可基本得到保障。然而,上述方案均采用了基于 Shamir 的秘密共享机制^[9],指数运算效率较低,对节点的计算能力要求较高。文献[10]基于中国剩余定理(Chinese Remainder Theorem, CRT)秘密共享机制设计了初步的加密数据生存方案,且研究解决了文献[7-8]中密钥分割存储的无效性问题。然而,文献[10]仅考虑了被攻破节点成为失效节点假设,并未考虑恶意节点参与数据恢复重建所将导致的错误数据恢复问题,即攻击者可通知攻陷并篡改节点内数据,并控制节点进行恶意反馈,从而达到有效的有效主动攻击目的,导致合法汇聚节点无法获得正确恢复结果,而恶意节点可顺利恢复获取数据。

本文对上述问题进行研究,提出网络模型和攻击假设。针对失效节点假设给出可靠数据加密分割生存方案,并提出基于恢复不一致性的恶意节点恢

复攻击检测方案以及基于多数表决的恶意节点恢复攻击识别机制。

2 模型假设

2.1 网络模型

假设网络中共有 n 个传感器节点,节点集合为 $V = \{v_1, v_2, \dots, v_n\}$,每个节点有唯一 ID,节点间可直接或间接通信,节点 $v_i (1 \leq i \leq n)$ 的邻居节点集为 $N_i (1 \leq i \leq n)$ 。假设感知节点每隔时间周期 T 可将数据汇聚传输给汇聚节点,网络中节点可松散同步,假设每当汇聚数据的同时进行完成同步,即同步时间间隔 T 。感知节点在每次汇聚周期中进行固定 r 轮感知采集数据,即间隔 T/r 时间采集一单位的感知数据。每个感知节点都有充足的空间,可以存储在 2 次汇聚周期内感知的所有数据。节点间假设已建立起完好的共享密钥设施^[4,8,11]。

2.2 攻击假设

结合先前相关攻击模型和工作^[1-6,10],本文将由于传感器节点无人值守,攻击者(ADV)每攻破并控制一个节点,可实施的攻击阐述如下:(1)被动攻击(数据隐私攻击)。读取所有存储数据及密钥,监视和记录所有节点的通信,这将导致缺乏保密机制的数据生存方案私密性遭到破坏,攻击者成功获得隐私感知数据。(2)主动攻击(数据可靠性攻击)。删除、破坏和篡改节点内数据,导致的攻击效果可根据被攻破节点的状态细分为以下 2 种:1)失效节点攻击。被攻破节点成为失效节点,不参与数据恢复重建,这将导致数据恢复的潜在失败(不满足门限无法恢复);2)恶意节点攻击。被攻破节点被控制成为恶意节点,继续响应数据恢复重建,将导致错误(或不公平)的数据恢复结果,即合法汇聚节点无法获得正确恢复结果,但恶意节点可顺利恢复获取数据。

下文用到的主要符号如表 1 所示。

表 1 本文常用符号

符号	说明
n	网络中节点个数
$v_1, v_2, \dots, v_n$	网络中节点集合
$N_1, N_2, \dots, N_n$	各节点邻居节点集合
$d_1, d_2, \dots, d_n$	各节点的感知数据
$K_{i,j} (1 < i \neq j < n)$	节点 i, j 间的共享密钥
$\xrightarrow{CRT} / CRT_1 \cdot $	秘密分割/恢复
$\xrightarrow{EC} / EC \cdot $	纠错码对数据编码分割/恢复
m	秘密/数据分割后分量数
t	恢复门限
$S_1, S_2, \dots, S_m$	密钥分割结果向量
$\overline{S_1}, \overline{S_2}, \dots, \overline{S_m}$	纠错编码后数据分割向量
t	被攻占节点个数
$\varphi_1, \varphi_2, \dots, \varphi_e$	被攻占节点集合

3 数据加密分割方案

本文的数据生存方案将使用数据加密传输来确保数据分存的私密性,进而防御被动攻击,为确保数据加密密钥的安全性,将同时利用秘密共享机制分割存储密钥,基于中国剩余定理的秘密分割和恢复机制能提高数据分割和恢复过程的效率,此外使用 HMAC 报文鉴别码机制^[12]来确保感知数据的完整性,用基于门限的 (t, m) 纠错码机制(如 RS 编码^[13]或信息扩散算法^[14])来实现可靠加密数据分割和存储。

具体完整方案分为数据保护、密钥、密文分割和分发存储以及数据恢复重构3个阶段。

3.1 数据保护

当感知节点 v_i 采集到数据 d_i 后,节点按照如下步骤进行操作,以保护数据的完整性和机密性。

(1)利用节点自身的随机密钥生成器产生随机会话密钥 K_i ,用以下文保护感知数据的完整性和私密性操作。

(2)使用密钥 K_i 计算感知数据 d_i 的 HMAC 报文鉴别码: $MAC = H_{K_i}(d_i)$,以保护感知数据 d_i 的完整性,抵抗中间攻击者的对数据的篡改。

(3)使用步骤(1)中生成的随机密钥 K_i 对感知数据和鉴别码的联合信息 $\{d_i || MAC\}$ 进行对称加密,生成密文 $D_i = E_{K_i}\{d_i || MAC\}$,保护数据的机密性。

3.2 密钥、密文分割和分发存储

密钥、密文分割和分发存储步骤如下:

(1)节点 v_i 选择 $m(m \leq n-1)$ 个节点(除去 v_i 自身)构成待分发集合 $Set_i = \{v_{j_1}, v_{j_2}, \dots, v_{j_m}\}$,如采用文献[6,9]中的节点信誉度降序机制,并使用中国剩余定理门限秘密共享机制将密钥 K_i 分割成子密钥。假设采用的门限参数为 (t, m) ,则密钥 K_i 将被分割成 m 个子密钥,具体为: $K_i \xrightarrow{CRT} \{S_1, S_2, \dots, S_m\}$ 。

(2)类似的,节点 v_i 使用 (t, m) 纠错码(如 RS 编码^[13]或信息扩散算法^[14])对密文数据 D_i 纠错编码分割为 m 份,具体为: $D_i \xrightarrow{EC} \{S_{j_1}, S_{j_2}, \dots, S_{j_m}\}$ 。

(3)节点 v_i 对分发集合中的节点 $\{v_{j_1}, v_{j_2}, \dots, v_{j_m}\}$ 分发上述步骤分割完毕的密钥和密文,假设节点 v_i 向 $v_{j_k}(1 \leq k \leq m)$ 分发上述分量,报文格式中包含节点 v_i 的 ID、报文序列号 $seqno$ 、子密钥 S_{j_k} 和密文分量 S_{j_k} ,并用节点 v_i 和 v_{j_k} 间的共享对称密钥 K_{i,j_k} 加密,具体如下: $v_i \rightarrow v_{j_k}: M_k = \{v_i || seqno || S_{j_k} || S_{j_k}\}_{K_{i,j_k}}$ 。

在分发分存之后,节点 v_i 将所有感知数据 d_i ,随机密钥 K_i 以及所有中间结果 $S_1, S_2, \dots, S_m, S_1,$

$S_2, \dots, S_m$ 销毁。可以看出,此后密文数据 D_i 以及加密密钥 K_i 都将受到门限保护。

3.3 数据恢复重构

数据恢复重构步骤如下:

(1)汇聚节点首先从不低于门限的 $l(l \geq t)$ 个节点处收集其与节点 v_i 的共享对称密钥 $K_{i,j_1}, K_{i,j_2}, \dots, K_{i,j_l}$ 以及存储内容 $M_1, M_2, \dots, M_l$ 。

(2)利用密钥 $K_{i,j_k}(1 \leq k \leq l)$ 对 $M_k(1 \leq k \leq l)$ 进行解密: $D_{K_{i,j_k}}\{M_k\} = \{v_i || seqno || S_{j_k} || S_{j_k}\}$ 。

(3)根据上述分存信息 $S_{j_k}(1 \leq k \leq l)$ 部分,利用中国剩余定理门限秘密共享机制重构密钥 K_i ,具体为: $K_i = CRT_l(S_{j_1}, S_{j_2}, \dots, S_{j_l})$ 。

(4)使用 (t, m) 纠错码对密文数据分割分量 $S_{j_k}(1 \leq k \leq l)$ 进行密文数据恢复,具体为: $D_i = EC\{S_{j_1}, S_{j_2}, \dots, S_{j_m}\}$ 。

(5)利用密钥 K_i 对 D_i 进行解密,具体如下: $D_{K_i}\{E_{K_i}\{d_i || MAC\}\} = \{d_i || MAC\}$ 。

(6)检查数据的完整性 $MAC \stackrel{?}{=} H_{K_i}(d_i)$ 。

可以看到,上述数据加密分割生存方案将感知数据 d_i 加密并将感知数据生存问题转化为加密密钥 K_i 的生存问题,随后利用 (t, m) 门限密码机制将加密密钥 K_i 进行分割并分存至各个节点中,利用攻击者必须俘获不低于门限 t 个节点方可重组加密密钥来确保数据的隐私保密。具体的,攻击者可通过某些手段(如攻破节点 v_i)获得节点间的通信密钥 $K_{i,j_1}, K_{i,j_2}, \dots, K_{i,j_l}$,进而按照步骤(2)解密所攻占 C 个节点 $\varphi_1, \varphi_2, \dots, \varphi_c$ 内存储的信息 $D_{K_{i,\varphi_k}}$

$\{M_k\} = \{v_i || seqno || S_{\varphi_k} || S_{\varphi_k}\}$,然而当攻占节点数低于恢复门限 $(c < t)$ 时,攻击者无法顺利完成随后步骤(3)中所述的密钥 K_i 恢复,进而无法达到恢复获取感知数据的目的。此外,基于中国剩余定理秘密共享机制提高并消除解决了文献[7-8]中密钥分割存储的低效问题。然而,上述方案也仍然仅仅适用被攻破节点的失效假设,并未考虑恶意节点参与数据恢复重建提供错误分量将导致的错误数据恢复问题。也就是说,攻击者仍可通过攻陷并篡改节点内数据、控制节点进行恶意反馈,导致合法汇聚节点无法获得正确恢复结果,但恶意节点可顺利恢复获取数据。

为了解决这个问题,下文将进一步设计提出可靠数据恢复检测方案,以抵御恶意节点的攻击情形,合法汇聚节点能对潜在的恶意节点攻击导致的数据恢复扭曲进行发现识别,恢复数据的可靠性将可得

到保证,从而实现更加可靠的数据生存恢复。

4 可靠数据恢复检测方案

根据上述的分析可知,数据恢复的可靠性主要依存于加密密钥 K_i 的正确恢复,根据中国剩余定理秘密共享机制^[15],将密钥 K_i 视作秘密 S ,利用 (t, m) 门限分割机制 $\xrightarrow{CRT}$ 分割 K_i 获得子密钥:

$$S_i = S \bmod m_i$$

其中, $1 \leq i \leq m$, $\{m_i\}_{i \in \{1, 2, \dots, m\}}$ 为公共模数参数,彼此互素。因此,数据恢复可靠性所依存的中国剩余定理恢复秘密过程 $CRT_i(\cdot)$ 可表示为从不低于门限的 $l(l \geq t)$ 的分量中选取 t 个分量构建如下模数方程组:

$$\begin{cases} S \equiv s_{i_1} \pmod{m_{i_1}} \\ S \equiv s_{i_2} \pmod{m_{i_2}} \\ \dots \\ S \equiv s_{i_t} \pmod{m_{i_t}} \end{cases} \quad (1)$$

根据中国剩余定理,可以解得:

$$S = \sum_{k=1}^t s_{i_k} M'_{C, i_k} M_{C \setminus \{i_k\}} \pmod{M_C}$$

其中, $M_C = \prod_{i \in C} m_i$; $M_{C \setminus \{i_k\}} = \prod_{j \in C, j \neq i_k} m_j$; $M'_{C, i_k} \equiv M_{C \setminus \{i_k\}}^{-1} \pmod{m_{i_k}}$ 。

下面介绍恶意节点受控之后在数据恢复阶段可进行的数据恢复攻击。

4.1 恶意节点数据恢复攻击

根据前面的分析,攻击者攻占并控制恶意节点,在数据恢复阶段可以进行的攻击根据所控制的恶意节点数可分为:

(1) 基本恢复攻击。恶意节点数低于门限 ($c < t$), 此时根据恢复式(1), 恶意节点集合 $\varphi_1, \varphi_2, \dots, \varphi_c$ 无法恢复得到秘密 S (加密密钥 K_i), 此时恶意节点 $\varphi_1, \varphi_2, \dots, \varphi_c$ 可提供恶意的篡改信息分量 $s'_{\varphi_1}, s'_{\varphi_2}, \dots, s'_{\varphi_c}$, 这样将导致凡选取恶意篡改分量后参与式(1)运算的数据恢复结果将遭遇错误 S' 。

(2) 增强恢复攻击。恶意节点数不低于门限 ($c \geq t$)。此时恶意节点集合 $\varphi_1, \varphi_2, \dots, \varphi_c$ 可将恢复得到秘密 S (加密密钥 K_i), 并根据 $S_i = S \bmod m_i, 1 \leq i \leq m, \{m_i\}_{i \in \{1, 2, \dots, m\}}$ 获知其余节点存储的秘密分量。因此, 此时恶意节点 $\varphi_1, \varphi_2, \dots, \varphi_c$ 可进行更加聪明细致的信息分量篡改 $s'_{\varphi_1}, s'_{\varphi_2}, \dots, s'_{\varphi_c}$, 以期通过相关检测方案。同低于门限情况, 将导致错误恢复结果 S' 。

4.2 基于恢复不一致性的恶意节点恢复攻击检测

为了确保有效数据生存, 针对潜在的恶意节点提供篡改信息 $s'_{\varphi_1}, s'_{\varphi_2}, \dots, s'_{\varphi_c}$ 导致的欺骗攻击行为, 合法汇聚节点在数据恢复过程中需及时针对该

攻击行为进行检测判断。类似的, 假设汇聚节点从不低于门限的 $l(l \geq t)$ 个节点处收集信息并试图从 l 个秘密分量中选取 t 个分量构建如式(1)中恢复方程组。发现存在恶意节点恢复攻击的恢复结果将容易导致 CRT 秘密恢复结果的不一致性^[16]。类似文献[16]中有关 Shamir 方案的讨论, 下面首先给出有关中国剩余定理的有关秘密恢复一致性的定义。

定义(中国剩余定理秘密恢复的一致性) 对于一个 (t, m) ($m \geq t$) 的门限 CRT 秘密共享方案, 秘密分割操作所得秘密分量 $\{s_1, s_2, \dots, s_m\}: S \xrightarrow{CRT} \{s_1, s_2, \dots, s_m\}$ 。恢复过程 $CRT_t(\cdot)$ 的一致性定义为: 对于包含 t 个秘密分量的恢复集合 $\tau = \{T_1, T_2, \dots, T_u\}$ (其中, $u = \binom{m}{t}$); $|T_i| = t; 1 \leq i \leq u$) 中任意元素 T_i ($1 \leq i \leq u$) 的秘密恢复结果 $Rec_i = CRT_t(T_i)$, 满足一致(相等)的恢复结果: $S = Rec_1 = \dots = Rec_u$ 。

根据定义中给出的有关的一致性定义, 一致性检测方案设计可先计算出任意恢复结果 Rec , 然后利用该结果对其他秘密分量进行检验即可。下面给出包含数据恢复一致性检测的数据恢复流程:

(1) 同 3.3 节中步骤(1)、步骤(2), 合法汇聚节点首先从不低于门限的 $l(l \geq t)$ 个节点处收集并获取信息 $\{v_i | 1 \leq i \leq l\} \cup \{S_{j_k} | 1 \leq j_k \leq l\}$;

(2) 从 $l(l \geq t)$ 个分存信息 $S_{j_k} (1 \leq k \leq l)$ 中随机选取一个大小为 t 的子集, 不妨为 $T = \{S_{j_1}, S_{j_2}, \dots, S_{j_t}\}$, 利用中国剩余定理重构密钥 $S = K_i = CRT_t(T) = CRT_t(S_{j_1}, S_{j_2}, \dots, S_{j_t})$;

(3) 利用恢复得到的密钥 S 对剩余的 $(l-t)$ 个秘密分量进行一致性检测, $S \stackrel{?}{=} S_{j_k} \pmod{m_{j_k}} (t+1 \leq k \leq l)$ 。当且仅当上述等式皆满足时才通过一致性检测;

(4) 继续 3.3 节中步骤(4)~步骤(6)步操作。

显然, 上述一致性检测方案流程的适用性与汇聚节点数 l , 恶意节点数 c 以及门限值 t 有关。此外, 还与恶意节点的不同攻击程度相关。

定理 1(恢复攻击的一致性检测适用条件) (1) 针对 4.1 节中的基本恢复攻击, 当且仅当 $l \geq t+1$ 时, 恢复一致性检测方案可检测出攻击; (2) 针对 4.1 节中的增强恢复攻击, 当且仅当 $l-c \geq t$ 时, 恢复一致性检测方案可检测出攻击。

证明:

(1) 根据恢复一致性的定义, 此时存在恢复结果数 $u = \binom{l}{t}$, 根据上述基本恢复攻击描述, 恶意节点无

法预知其余的秘密分量,因此若存在基本恢复攻击,在 $u = \binom{l}{t}$ 个恢复结果中必然存在不一致情况,因此只需条件 $l \geq t + 1$ 即可。即充分性得证。另外显然 $l = t$ 是不满足条件的,因此该条件是紧的,是必要条件。

(2)充分性。当 $l - c \geq t$ 时,即完好的秘密分量个数不低于门限值,必然存在包含 t 个完好秘密分量集合 G ,因此根据定义,必然可恢复出 $S = Rec_G = CRT_l(G)$ 。若存在攻击必然存在另外的一个非完好集合 G' , $S' = Rec_{G'} = CRT_l(G') \neq S$,因此存在不一致情况。

(3)必要性。若放松条件至 $l - c = t - 1$ 。则根据定义,不存在一个包含 t 个完好秘密分量集合 G ,即任何包含 t 个秘密分量集合 G 都至少包含一个恶意分量。不失一般性,不妨假设在恢复方程组中存在恶意节点集合为 $\varphi_1, \varphi_2, \dots, \varphi_c$:

$$\begin{cases} S \equiv s'_{\varphi_1} \pmod{m_{i_1}} \\ \dots \\ S \equiv s'_{\varphi_c} \pmod{m_{i_c}} \\ S \equiv s_{i_{c+1}} \pmod{m_{i_{c+1}}} \\ \dots \\ S \equiv s_{i_t} \pmod{m_{i_t}} \end{cases}$$

根据增强恢复攻击描述,恶意节点集合 $\varphi_1, \varphi_2, \dots, \varphi_c$ 可预知计算出其余所有完好秘密分量 $s_{i_{c+1}}, s_{i_{c+2}}, \dots, s_{i_t}$, 并从它们自身的原始分量 $s_{\varphi_1}, s_{\varphi_2}, \dots, s_{\varphi_c}$ 出发构建合适的恶意秘密分量 $s'_{\varphi_1}, s'_{\varphi_2}, \dots, s'_{\varphi_c}$, 同时达到以下 2 个目的:(1)任何大小为 t 的秘密分量集合 G' 恢复结果均不等于原始正确恢复秘密: $S' = Rec_{G'} = CRT_l(G') \neq S$; (2)逃避上述恢复一致性检测协议的检测。下面给出具体构建过程。根据之前的工作^[17], CRT 秘密共享机制满足 $(\oplus, \oplus), (\otimes, \otimes)$ -同态特性,因此,恶意节点集合可根据有原始秘密分量 $s_{\varphi_1}, s_{\varphi_2}, \dots, s_{\varphi_c}$ 先恢复计算出原始秘密 S , 随后进行秘密变换 $S' = S \times \Delta x + \Delta y$, 其中:

$$\begin{cases} \Delta x \equiv 1 \pmod{m_{i_{c+1}} m_{i_{c+2}} \dots m_{i_t}} \\ \Delta x \neq 1 \pmod{m_{\varphi_k}} (1 \leq k \leq c) \\ \Delta y \equiv 0 \pmod{m_{i_{c+1}} m_{i_{c+2}} \dots m_{i_t}} \\ \Delta y \neq 1 \pmod{m_{\varphi_k}} (1 \leq k \leq c) \end{cases}$$

上述变换保证新生成的秘密分量扭曲 $s' \equiv s'_{\varphi_k} \pmod{m_{i_1}} \neq s_{\varphi_k} (1 \leq k \leq c)$, 进而导致任意大小为 t 的秘密分量集合 G' 恢复结果一致且较原始秘密 S 扭曲,即 $CRT_l(G') = S' = S \times \Delta x + \Delta y \neq S$ 。因此, $l - c = t - 1$ 时,恶意节点的增强恢复攻击可逃脱上述一致性检测检测。故应对增强恢复攻击的适用必要条件为 $l - c \geq t$ 得证。

4.3 基于多数表决的恶意节点恢复攻击识别

在一定的适用条件下,恶意节点攻击检测可顺利检测出恶意节点所实施的恢复攻击。在检测出存在恶意恢复攻击的情况下,在满足一定条件时,可进一步设计有效的恶意节点恢复攻击识别方案,即识别出具体实施攻击的恶意节点。具体为在不一致的恢复结果中,当正确的恢复结果占多数时,可通过多数表决机制^[16]识别出正确恢复结果,进而识别出导致错误恢复结果的错误分量和恶意节点。

具体恶意节点恢复攻击识别过程如下:

(1)从现有不低于门限的 $l (l \geq t)$ 个秘密分量集合中统计任意大小为 t 的恢复集合 $\tau = \{T_1, T_2, \dots, T_u\}$ (其中, $u = \binom{l}{t}$, $|T_i| = t, 1 \leq i \leq u$) 中任意秘密恢复结果 $Rec_i = CRT_l(T_i)$, 并将统计结果最频繁的恢复结果 Rec_f 作为正确恢复结果 S ;

(2)利用恢复得到的密钥 S 对秘密分量依次进行检查, $S \equiv s_{j_k} \pmod{m_{j_k}} (1 \leq k \leq l)$ 。等式不成立的节点识别为恶意节点。

类似恶意节点攻击检测协议,下面具体给出上述基于多数表决的恶意攻击节点识别方案的适用条件。

定理 2(恢复攻击多数识别适用条件) (1)针对 4.1 节中的基本恢复攻击,当且仅当 $l - c \geq t$ 时,恢复攻击识别方案可准确识别恶意攻击节点;(2)针对 4.1 节中的增强恢复攻击,当且仅当 $l - c = t - 1$ 时,恢复攻击识别方案可准确识别恶意攻击节点。

证明:

(1)根据定义,此时统计得出的正确恢复结果数为 $\binom{l-c}{t}$, 根据 4.2 节中的基本恢复攻击描述,恶意节点无法预知其余的秘密分量,因此若存在基本恢复攻击,其余错误恢复结果必然两两不同,只需条件 $\binom{l-c}{t} > 1$ 即可支撑多数识别协议的正确性,因此, $l - c \geq t$ 的充分性可以显然得出。另外显然 $l - c \geq t$ 也是必要条件,否则一旦放松 $l - c = t$ 时, $\binom{l-c}{t} = 1$ 将导致上述识别协议的无法识别。

(2)同样统计得出的正确恢复结果 S 的次数为 $\binom{l-c}{t}$ 。根据 4.2 节中的增强恢复攻击描述,恶意节点集合 $\varphi_1, \varphi_2, \dots, \varphi_c$ 可通过恢复出 S 来预知其余节点秘密分量,为逃避并挫败基于多数原则的攻击识别协议,恶意节点需最大化错误恢复结果 S' 的统计次数,具体通过结合 $t - 1$ 个完好秘密分量(假设为 $s_1, s_2, \dots, s_{t-1}$) 来篡改自身分量 $s_{\varphi_1}, s_{\varphi_2}, \dots, s_{\varphi_c} \rightarrow$

$s_{\varphi_1}, s_{\varphi_2}, \dots, s_{\varphi_c}$ 。具体构建过程同定理1中(2)恶意节点集合篡改构建过程,秘密变换 $S' = S \times \Delta x + \Delta y$, 其中:

$$\begin{cases} \Delta x \equiv 1 \pmod{m_{i_{c+1}} m_{i_{c+2}} \dots m_{i_t}} \\ \Delta x \not\equiv 1 \pmod{m_{\varphi_k}} (1 \leq k \leq c) \\ \Delta y \equiv 0 \pmod{m_{i_{c+1}} m_{i_{c+2}} \dots m_{i_t}} \\ \Delta y \not\equiv 1 \pmod{m_{\varphi_k}} (1 \leq k \leq c) \end{cases}$$

上述变换保证在集合 $C = \{s_1, s_2, \dots, s_{t-1}; s_{\varphi_1}, s_{\varphi_2}, \dots, s_{\varphi_c}\}$ 中,任意大小为 t 秘密分量集合 $G' \subset C$ 恢复结果一致且较原始秘密 S 扭曲,即 $CRT_t(G') = S' = S \times \Delta x + \Delta y \neq S$,此时可导致最大的伪造 S' 统计次数为 $\binom{|C|}{t} = \binom{c+t-1}{t}$ 。故只需条件 $\binom{l-c}{t} = \binom{c+t-1}{t}$ 满足,即 $l-c = c+t-1$ 时基于多数表决的识别方案可确保正确性,因此, $l-c = c+t-1$ 的充分性可得证。另外显然 $l-c = c+t-1$ 也是紧的必要条件,否则 $l-c = c+t-1$ 时将导致上述识别方案的挫败。综上所述,识别恢复攻击的充要条件为 $l-c = c+t-1$ 。

5 方案分析

方案分析过程如下:

(1)第3节中设计的加密分割数据生存方案,将感知数据 d_i 加密并将感知数据生存问题转化为加密密钥 K_i 的生存问题,随后利用 (t, m) 门限密码机制将加密密钥 K_i 进行分割并分存至各个节点中,利用攻击者必须俘获不低于门限 t 个节点方可重组加密密钥来确保数据的隐私保密。在失效节点攻击假设下,可以有效确保数据生存的安全可靠性。基于中国剩余定理秘密共享机制提高并消除解决了文献[7-8]中密钥分割存储的低效问题,在不损失安全性情况下做到了密钥分割、恢复的高效。根据前面的分析,现有数据加密生存方案均基于文献[9]中的 Shamir 方案的秘密重建复杂度为 $O(t \lg^2 t)$ (门限为 t),且子密钥分割需进行一定量的指数运算,效率较低,对无线传感器节点造成一定的负担,而本文采用的基于中国剩余定理的方案秘密重建复杂度仅为 $O(t)$ 。

(2)本文4.2节中提出的恶意节点恢复攻击检测方案利用恶意节点恢复攻击将导致的秘密恢复结果的不一致性^[16],结合中国剩余定理秘密共享机制,可分别在 $l \geq t+1$ 和 $l-c \geq t$ 条件下有效进行针对4.1节中基本和增强恶意节点恢复攻击的检测,检测过程需遍历一遍分量集合,因此,复杂度为 $O(l)$ 。

(3)在不一致的恢复结果情况下,当正确的恢复

结果占多数时,利用多数表决机制^[16]可识别出正确恢复结果,进而识别出导致错误恢复得错误分量和恶意节点。本文4.3节中提出的恶意节点恢复攻击识别方案可分别在 $l-c \geq t$ 和 $l-c = c+t-1$ 条件下针对4.1节中基本和增强恶意节点恢复攻击进行有效识别定位,具体识别过程需计算含 t 个秘密分量的恢复集合 $\tau = \{T_1, T_2, \dots, T_u\}$ (其中, $u = \binom{l}{t}$, $|T_i| = t, 1 \leq i \leq u$) 中多数秘密恢复 $S = Rec_f$,过程复杂度为 $O\left(\binom{l}{t}\right)$ 。

6 结束语

为增强数据生存的概率,提高感知数据的抗损坏、擦除和篡改能力,本文建立了相关攻击模型假设,针对失效节点攻击假设提出一种基于中国剩余定理加密密钥分割机制的可靠数据生存方案,利用中国剩余定理门限密钥分割存储机制增强了密钥分割存储的安全性,给出了可靠数据恢复检测方案,包括基于恢复不一致性的恶意节点恢复攻击检测方案以及基于多数表决的恶意节点恢复攻击识别机制,从而确保数据恢复的安全、可靠。

参考文献

- [1] Pietro D R, Mancini L V, Soriente C, et al. Catch Me (If You Can): Data Survival in Unattended Sensor Networks [C]//Proceedings of the 6th Annual IEEE International Conference on PerCom. Washington D. C., USA: IEEE Press, 2001: 185-194.
- [2] Ma D, Soriente C, Tsudik G. New Adversary and New Threats: Security in Unattended Sensor Networks [J]. IEEE Network, 2009, 23(2): 43-48.
- [3] Vitali D, Spognardi A, Mancini LV. Replication Schemes in Unattended Wireless Sensor Networks [C]//Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security. Washington D. C., USA: IEEE Press, 2011: 1-5.
- [4] Vitali D, Spognardi A, Villani A, et al. MhRep: Multi-hop Replication Scheme for Data Survival in Unattended Wireless Sensor Networks [C]//Proceedings of the 30th IEEE Symposium on Reliable Distributed Systems Workshops. Washington D. C., USA: IEEE Press, 2011: 42-51.
- [5] Thi M Y V, Talim J. Random Distribution for Data Survival in Unattended Wireless Sensor Networks [C]//Proceedings of the 4th International Conference on Sensor Technologies and Applications. Washington D. C., USA: IEEE Press, 2010: 468-471.
- [6] 韩明军,熊焰,刘涛,等.无人值守 WSN 中数据概率复制生存仿真与研究 [J]. 计算机仿真, 2013, (7): 251-255.

(下转第 155 页)

性撤销的 CP-ABE 方案。该方案可以解决现有支持属性间接撤销的 CP-ABE 方案撤销代价与安全性难以兼顾的问题。如何将基于合数阶双线性群的构造方案转换为基于素数阶双线性群的构造方案,提出属性可撤销的 KP-ABE 方案是下一步的研究工作。

参考文献

- [1] Sahai A, Waters B. Fuzzy Identity-based Encryption[C]//Proceedings of Cryptology-EUROCRYPT' 05. Berlin, Germany; Springer, 2005:457-473.
- [2] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute-based Encryption [C]//Proceedings of IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2007:321-334.
- [3] Waters B. Ciphertext-policy Attribute-based Encryption: An Expressive, Efficient, and Provably Secure Realization[C]// Proceedings of PKC' 11. Berlin, Germany: Springer, 2011:53-70.
- [4] Goyal V, Pandey O, Sahai A, et al. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2006:89-98.
- [5] Attrapadung N, Imai H. Attribute-based Encryption Supporting Direct/indirect Revocation Modes [M]//Parker M G. Cryptography and Coding. Berlin, Germany: Springer, 2009:278-300.
- [6] 苏金树,曹 丹,王小峰,等. 属性基加密机制[J]. 软件学报, 2011, 22(6):1299-1315.
- [7] 胡海英,高 威. 一种可撤销的 KP-ABE 方案[J]. 计算机系统应用, 2013, 22(9):123-128.
- [8] 王鹏翮,冯登国,张立武. 一种支持完全细粒度属性撤销的 CP-ABE 方案[J]. 软件学报, 2012, 23(10):2805-2816.
- [9] Hanaoka Y, Hanaoka G, Shikata J, et al. Identity-based Hierarchical Strongly Key-insulated Encryption and Its Application [C]//Proceedings of Cryptology-ASIACRYPT' 05. Berlin, Germany: Springer, 2005:495-514.
- [10] Boldyreva A, Goyal V, Kumar V. Identity-based Encryption with Efficient Revocation [C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2008:417-426.
- [11] Ibraimi L, Petkovic M, Nikova S, et al. Mediated Ciphertext-policy Attribute-based Encryption and Its Application [C]//Proceedings of the 10th International Workshop on Information Security Applications. Berlin, Germany: Springer, 2009:309-323.
- [12] Lewko A, Okamoto T, Sahai A, et al. Fully Secure Functional Encryption: Attribute-based Encryption and (Hierarchical) Inner Product Encryption [C]//Proceedings of Cryptology-EUROCRYPT' 10. Berlin, Germany: Springer, 2010:62-91.
- [13] Lewko A, Waters B. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts [C]//Proceedings of the 7th Theory of Cryptography Conference, February 9-11, 2011, Zurich, Switzerland. Berlin, Germany: Springer, 2010:455-479.
- [14] 孙 瑾,胡予濮. 完全安全的基于属性的广播加密方案[J]. 西安电子科技大学学报, 2012, 39(4):23-28.
- [15] 孙 瑾. 标准模型下可证明安全的公钥广播密码研究[D]. 西安:西安电子科技大学, 2012.
- [16] Boneh D, Goh E J, Nissim K. Evaluating 2-DNF Formulas on Ciphertexts [M]//Micciancio D. Theory of Cryptography. Berlin, Germany: Springer, 2005:325-341.
- [17] Beimel A. Secure Schemes for Secret Sharing and Key Distribution [D]. Haifa, Israel: Israel Institute of Technology, 1996.
- [18] Yu Shucheng, Wang Cong, Ren Kui, et al. Attribute Based Data Sharing with Attribute Revocation [C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York, USA: ACM Press, 2010:261-270.
- 编辑 金胡考
-
- (上接第 150 页)
- [7] Ren Wei, Zhao Junge, Ren Yi. MSS: A Multi-level Data Placement Scheme for Data Survival in Wireless Sensor Networks [C]//Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing. Washington D. C., USA: IEEE Press, 2009:1-4.
- [8] Wang Qian, Ren Kui, Lou Wenjing, et al. Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance [C]//Proceedings of IEEE INFOCOM' 09. Washington D. C., USA: IEEE Press, 2009:954-962.
- [9] Shamir A. How to Share a Secret [J]. Communications of the ACM, 1979, 22(11):612-613.
- [10] 韩明军,熊 焰,陆琦玮,等. 无人值守 WSN 中基于中国剩余定理的可靠数据生存方案 [J]. 计算机应用, 2013, 35(5):1343-1346.
- [11] Blundo C, De Santis A, Herzberg A, et al. Perfectly-secure Key Distribution for Dynamic Conferences [C]//Proceedings of Advances in Cryptology-CRYPTO' 93. Berlin, Germany: Springer, 1993:471-486.
- [12] Krawczyk H, Canetti R, Bellare M. HMAC: Keyed-hashing for Message Authentication [S]. RFC 2104, 1997.
- [13] Rabin M O. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance [J]. Journal of the ACM, 1989, 36(2):335-348.
- [14] Reed I S, Solomon G. Polynomial Codes over Certain Finite Fields [J]. Journal of the Society for Industrial & Applied Mathematics, 1960, 8(2):300-304.
- [15] Asmuth C, Bloom J. A Modular Approach to Key Safeguarding [J]. IEEE Transactions on Information Theory, 1983, 29(2):208-210.
- [16] Harn L, Lin C. Detection and Identification of Vheaters in (t, n) Secret Sharing Scheme [J]. Designs, Codes and Cryptography, 2009, 52(1):15-24.
- [17] Lu Q, Xiong Y, Huang W, et al. A Distributed ECC-DSS Authentication Scheme Based on CRT-VSS and Trusted Computing in MANET [C]//Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Washington D. C., USA: IEEE Press, 2012:656-665.
- 编辑 索书志