

文章编号:1001-9081(2016)09-2432-06

doi:10.11772/j.issn.1001-9081.2016.09.2432

可及时确定受攻击节点的无线传感器网络数据聚合方案

王洁*, 卢建朱, 曾小飞

(暨南大学 信息科学技术学院, 广州 510632)

(*通信作者电子邮箱 ada0608@126.com)

摘要: 无线传感器网络(WSN)中,当传感器节点受到攻击导致网络数据和传输受到干扰,及时确定受攻击的传感器节点并采取相应措施以保障整个网络的安全性尤为重要。因此,提出一种可及时确定受攻击节点的无线传感器网络数据聚合方案。首先使用状态公钥加密和对称公钥加密结合伪随机函数和消息认证码对数据进行两次加密,其次,在簇头节点进行认证,将假数据过滤后,解密,并将假数据节点编号发送给基站;最后在基站进行解密认证,恢复明文数据。该方案的提出解决了由于受攻击节点导致的错误聚合值问题,而且还实现了及时过滤假数据并确认受攻击的传感器节点。理论分析表明,提出的基于安全的单向函数、消息认证码和椭圆曲线上的离散对数难题的方案是安全的,并大大降低了网络的通信成本和计算成本。仿真实验表明,该方案的计算成本、通信成本和确认受攻击节点时间比使用状态公钥加密的无线传感器网络安全聚合方案分别降低了至少 19.96%、36.81% 和 28.10%。

关键词: 无线传感器网络; 数据聚合; 消息认证码; 伪随机函数; 同态加密

中图分类号: TP309.7 **文献标志码:**A

Data aggregation scheme for wireless sensor network to timely determine compromised nodes

WANG Jie*, LU Jianzhu, ZENG Xiaofei

(College of Information Science and Technology, Jinan University, Guangzhou Guangdong 510632, China)

Abstract: In Wireless Sensor Network (WSN), when the compromised sensor nodes disturb network data and transmission, it is particularly important to determine the compromised sensor nodes in time and take appropriate measures to ensure the security of the entire network. Therefore, a data aggregation scheme for wireless sensor network was proposed to timely determine the compromised sensor nodes. First, the state public key encryption, the symmetric public key encryption, the pseudo random function and the message authentication code were used to encrypt the plaintext twice. Secondly, the cluster head node authenticated the ciphertext and filtered false data. Then, the cluster head node decrypted the ciphertext, and the numbers of the compromised nodes were sent to the base station. At last, the base station decrypted the ciphertext to recover the plaintext and authenticated the data. The proposed scheme solves the problem of the error aggregation value problem caused by the compromised nodes, filters the false data in time and determines the compromised sensor nodes. The analysis shows that the proposed scheme is secure under the secure one-way hash function, the message authentication code and the assumption of the Discrete Logarithm Problem (DLP), and also greatly reduces the communication cost and computational cost. Simulation result shows that, compared with the secure aggregation scheme for WSN using stateful public key cryptography, the computational cost, the communication cost and the time consumption of determining the compromised sensor nodes of the proposed scheme is decreased by at least 19.96%, 36.81% and 28.10%, respectively.

Key words: Wireless Sensor Network (WSN); data aggregation; message authentication code; pseudo-random function; homomorphic encryption

0 引言

无线传感器网络(Wireless Sensor Network, WSN)已经被广泛地应用于环境监测、医疗保健、交通运输等领域^[1]。在 WSN 中,节点通常是由能量非常有限的电池供电,因此,研究如何使节点能够在保证可用性的前提下尽量降低能量消耗,对 WSN 长时间工作显得尤为必要^[2]。此外,传感器节点是被放置在公共的、不可信甚至可被恶意入侵的现实环境中,且无线传输本身数据易于被捕获和侦听。数据聚合技术作为降

低数据通信成本的重要技术之一,将节点的感应数据进行聚合之后发送给基站,以减少能量消耗^[3]。

为了提高数据聚合的安全性,人们通常会采用某种加密技术。传统的安全数据聚合方案多采用逐跳聚合加密^[4-6],其数据聚合过程中频繁的加解密操作往往会影响聚合效率,也增加了相应的额外能量支出和延时。针对这一情况,引入了同态加密技术^[7-9]使得计算运算可以在密文之上执行,数据聚合过程变得更有效率。基于公钥的同态加密技术,可应用于高端传感器的数据安全聚合;而对于一般的低端传感器

收稿日期:2016-02-17;修回日期:2016-04-21。 基金项目:国家自然科学基金资助项目(61373125, 61272415, 61070164);广东省自然科学基金资助项目(S2011010002708, 2010B090400164);暨南大学科技创新基金资助项目(11611510)。

作者简介: 王洁(1993—),女,河北邯郸人,硕士研究生,主要研究方向:信息安全、网络通信; 卢建朱(1965—),男,湖南桂阳人,副教授,博士,主要研究方向:信息安全、网络通信; 曾小飞(1990—),女,江西赣州人,硕士研究生,主要研究方向:信息安全、网络通信。

更青睐于基于对称加密算法的同态加密技术。在基于对称加密算法的同态加密技术中,根据 WSN 的特点,设计一个资源消耗较低且同时提供数据机密性和完整性服务的方案是一个非常有挑战的问题^[10]。基于文献[11]的对称加密生成的密文数据聚合,Boudia 等^[12]通过一个转发阶段定义传感器节点 S_{ij} 的当前状态 St_{ij} ,利用基于状态的对称密钥实现加密数据聚合的机密性和完整性;当加密数据聚合操作中受到攻击,该方案中基站发现聚合数据无效,但没有给出确定受攻击节点的方法。为了保障 WSN 的正常运行,震慑攻击者的攻击行为,设计一种保证加密数据聚合的机密性和完整性、且能及时确定所受攻击的节点的数据聚合方案是十分必要的。

针对 Boudia 等^[12]提出方案的不足,本文将伪随机函数、安全消息认证码和转发阶段定义传感器节点 S_{ij} 的当前状态 St_{ij} 相结合,使簇节点能及时验证其属下传感器发送的密文数据,这样基站接收的密文是簇节点验证有效的密文数据的聚合。簇节点的验证结果可及时过滤无效的密文数据,确定受攻击的节点,方便相关部门采取措施及时维护网络的安全运行。

1 本文设计方案

本章将椭圆曲线上的点加法与散列函数相结合,设计了一种可及时确定受攻击的传感器节点的数据聚合方案,可及时检测接收数据的正确性,并及时确定受攻击的传感器节点。该方案由系统初始化、状态转发和数据聚合阶段组成,每个阶段的具体操作将在下面描述。

1.1 系统初始化

假设 G 是定义在数域 F_p 中椭圆曲线 $E_p(a, b)$ 上的加法群, P 是 G 的 q 阶生成元。令传感器网络中的最大节点数目为 n ,采集数据的长度为 μ 比特,正整数 M 不小于 $2^{\mu n}$ 。系统选取一个伪随机函数的 $f(\cdot)$ 和一个安全消息认证码 $mac_{\cdot}(\cdot)$,并为基站(Base Station, BS)配置一对私钥 x 公钥 (x, Y) ,其中 $Y = xP, x \in \mathbf{Z}_q^*$, 基站 BS 与每一个传感器节点 S_{ij} 建立一个共享密钥 SK_{ij}^{BS} 。

1.2 转发阶段

节点部署后,传感器节点 S_{ij} 与其所在簇的簇头 CH_j 建立一个共享的对称密钥 K_{ij}^{CH} 。在每次执行数据聚合前,BS 广播一个严格单调递增的一次性随机数 t (如,取 BS 当前的时间),部署的传感器节点执行一个转发操作,以生成一个一次性的状态,这是一些传感器网络^[13-15]通常采用的方法。隶属于不同簇的传感器节点不能与基站直接通信,需要通过所在簇的簇头转发来执行这一操作。

隶属于簇 CH_j 的第 i 个节点 S_{ij} 执行算法 1,然后将结果经簇头转发给 BS。即, CH_j 将 St_{ij} 和消息认证码 mac_{ij} 转发送给 BS。为了确保 BS 能够提取到所有密钥,要求簇头转发所有的数据包。

算法 1 Forwarding phase(S_{ij})。

输入: $para, SK_{ij}^{BS}, t$;

输出: St_{ij}, mac_{ij} 。

- 1) 生成随机数 $r_{ij} \in [1, q - 1]$;
- 2) 计算 $St_{ij} = r_{ij}P$;

- 3) 计算 $K_{ij} = f(St_{ij} \parallel r_{ij}Y \parallel SK_{ij}^{BS}, t)$;
- 4) 计算 $mac_{ij} = mac_{K_{ij}}(St_{ij})$ 。

接收到信息 (St_{ij}, mac_{ij}) 后,基站 BS 使用私钥 x 计算出与节点 S_{ij} 的共享密钥 $xSt_{ij} = xr_{ij}P = r_{ij}Y$,调用算法 2,检查该状态信息的有效性和完整性。BS 将认证结果通过其簇头 CH_j 转发给节点 S_{ij} ,若信息 (St_{ij}, mac_{ij}) 被 BS 接受,则节点 S_{ij} 将 (St_{ij}, mac_{ij}) 作为其状态,此状态用于随后的数据聚合过程;否则,该节点重新执行算法 1。转发阶段的最终结果是基站同网络中参加数据聚合的每一个节点 S_{ij} 之间共享一个状态 St_{ij} 和执行簇数据聚合操作的序号 o_i 。

算法 2 Verification(BS)。

输入: $para, t, (St_{ij}, mac_{ij}), SK_{ij}^{BS}, x$;

输出: mac verification。

对每个节点 S_{ij}

- 1) 计算 $K_{ij} = f(St_{ij} \parallel xSt_{ij} \parallel SK_{ij}^{BS}, t)$;
- 2) 计算 $mac'_{ij} = mac_{K_{ij}}(St_{ij})$;
- 3) 若 $mac'_{ij} = mac_{ij}$ 成立则接受;否则拒绝。

1.3 数据聚合阶段

数据的聚合阶段在转发阶段之后进行,包含数据加密、数据聚合和数据恢复与认证三个过程。具体地,在数据加密过程中,节点感测数据,将所得结果加密发送至簇头;在数据聚合过程,簇头接收密文数据并验证数据的正确性,簇头将簇中采集的有效数据进行聚合传送给基站;在数据的恢复与认证过程,基站对簇头发来的有效数据进行解密和认证。

1.3.1 数据加密过程

据加密前,传感器节点 S_{ij} 先将感知到的数据 m_{ij} 用类似于文献[16]的编码方式进行编码,与之不同的是编码之后的 e_{ij} 使用对称加密算法,其速度比非对称加密更快并且支持较短的密文。

由 $f(\cdot)$ 生成两个密钥 K_{ij1} 和 K_{ij2} ,其中 $K_{ij1} < M$ (M 是传感器节点部署前预装载的大整数,正整数 M 不小于 $2^{\mu n}$)。数据加密过程中,传感器节点 S_{ij} 使用 K_{ij1} 加密编码之后的数据 e_{ij} , K_{ij2} 则用来生成相应的验证码 MAC_{ij} ;传感器节点与簇头共享的密钥 K_{ij}^{CH} 则可分割为两个子密钥 K_{ij1}^{CH} 和 K_{ij2}^{CH} ; K_{ij1}^{CH} 用来对已经加密的数据进行第二次加密, K_{ij2}^{CH} 则是生成再次加密之后密文和 MAC_{ij} 对应的验证码,具体的加密过程如算法 3。

算法 3 Encrypt phase(S_{ij})。

输入: $m_{ij}, (r_{ij}, St_{ij}), SK_{ij}^{BS}, K_{ij}^{CH}, t$;

输出: $(c'_{ij}, mac'_{ij}), MAC_{ij}$ 。

- 1) 对数据进行编码 $e_{ij} = m_{ij} \parallel 0^z$,其中 $z = \mu(o_i - 1)$;
- 2) 计算 $K_{ij} = f(St_{ij} \parallel r_{ij}Y \parallel Y, t)$,拆分 K_{ij} 为 $K_{ij1} \parallel K_{ij2}$;
- 3) 生成密文 c_{ij} 和对应认证消息 MAC_{ij} ,其中 $c_{ij} = e_{ij} + K_{ij1} \bmod M, MAC_{ij} = mac_{K_{ij2}}(c_{ij})$;
- 4) 拆分 K_{ij}^{CH} 为 $K_{ij1}^{CH} \parallel K_{ij2}^{CH}$,计算 $c'_{ij} = c_{ij} \oplus K_{ij1}^{CH}, mac'_{ij} = mac_{K_{ij2}^{CH}}(c'_{ij} \parallel MAC_{ij})$ 。

1.3.2 数据聚合过程

收到节点 S_{ij} 的信息 (c'_{ij}, mac'_{ij}) 和 MAC_{ij} 后,簇头 CH_j 首先验证其有效性。具体地,簇头 CH_j 将与 S_{ij} 的共享密钥 K_{ij}^{CH} 拆分成 $K_{ij1}^{CH} \parallel K_{ij2}^{CH}$,由 K_{ij2}^{CH} 计算 c_{ij} 和 MAC_{ij} 的消息认证码 mac''_{ij} ,只有当 mac''_{ij} 与接收的 mac'_{ij} 匹配时才执行对 c'_{ij} 的解密,恢复密文 c_{ij} ;如果不匹配,则要求节点 S_{ij} 重新发送。

假设在限定的时间内有 η 个节点没有传送有效的数据给

簇头 CH_j , 其中 $0 \leq \eta \leq n/3$ 。不失一般性, 令这 η 个节点为 $S_{1j}, S_{2j}, \dots, S_{\eta j}$ 。对接收到的 $n - \eta$ 个有效数据, 簇头 CH_j 执行密文数据的聚合操作得到 C_{agg} 。类似地, 该簇头将 $n - \eta$ 个有效数据对应的消息认证码进行异或聚合得到 MAC_{agg} 。最后, 簇头将 (C_{agg}, MAC_{agg}) 和没有传送有效数据的节点标识符 $\{S_{1j}, S_{2j}, \dots, S_{\eta j}\}$ 转发给基站。上述两个操作的具体实现见算法 4。

算法 4 Homomorphic aggregation(CH_j)。

- 输入: $((c'_{ij}, mac'_{ij}), MAC_{ij})$, 其中 $i \in \{1, 2, \dots, n\}$;
 输出: (C_{agg}, MAC_{agg}) 。
- 1) 认证每个接受信息 (c_{ij}, MAC_{ij})
 - ① 计算 $mac''_{ij} = mac_{K_{ij}^{CH}}(c'_{ij} \parallel MAC_{ij})$,
 - ② 若 $mac''_{ij} \neq mac'_{ij}$, 则要求相应节点重发,
 - ③ 否则, 解密 $c_{ij} = c'_{ij} \oplus K_{ij}^{CH}$;
 - 2) 当簇中的节点信息有效时, 对簇中有效的 $n - \eta$ 个密文 $(c_{(\eta+1)j}, c_{(\eta+2)j}, \dots, c_{nj})$ 执行聚合计算 $C_{agg} = \sum_{i=\eta+1}^n c_{ij} \bmod M$;
 - 3) 由 $n - \eta$ 个消息验证码 $(MAC_{(\eta+1)j}, MAC_{(\eta+2)j}, \dots, MAC_{nj})$ 执行聚合得到 $MAC_{agg} = MAC_{(\eta+1)j} \oplus MAC_{(\eta+2)j} \oplus \dots \oplus MAC_{nj}$ 。

1.3.3 数据的恢复与认证

基站 BS 接收到每个簇 CH_j 发送来的聚合数据 (C_{agg}, MAC_{agg}) 和 $\{S_{1j}, S_{2j}, \dots, S_{\eta j}\}$ 后, 对它们进行解密和认证两个操作。

令 $L = \{\eta + 1, \eta + 2, \dots, n\}$, 对每个 $i \in L$ 及其对应节点 S_{ij} , BS 读取转发阶段与其共享的状态 St_{ij} , 计算对应节点的密钥 K_{ij} , 并将该密钥拆分成 $K_{ij1} \parallel K_{ij2}$; 然后, 通过计算 $C_{agg} - \sum_{i=\eta+1}^n K_{ij1} \bmod M$ 得到解密的明文 e_{agg} , 由 e_{agg} 的结构可得到传感器节点 S_{ij} 的数据 m_{ij} , 其中 $i = \eta + 1, \eta + 2, \dots, n$, 结合序号 o_i 和密钥 K_{ij2} , 可生成 m_{ij} 的消息认证码 MAC'_{ij} , 将 $n - \eta$ 个 MAC'_{ij} 异或操作的结果为 MAC'_{agg} , 如果 $MAC'_{agg} = MAC_{agg}$ 成立, 则簇头 CH_j 下的 $n - \eta$ 个节点感测数据 $\{m_{(\eta+1)j}, m_{(\eta+2)j}, \dots, m_{nj}\}$ 是真实有效的, 否则要求对应簇头 CH_j 重发。具体的恢复与认证操作实现见算法 5。

算法 5 End-to-end verification(BS)。

- 输入: $(C_{agg}, MAC_{agg})_j$ 无效数据节点 $\{S_{1j}, S_{2j}, \dots, S_{\eta j}\}$, 其中 $j \in \{1, 2, \dots, n\}$;
 输出: MAC verification。
- 1) 对有效节点 $\{S_{(\eta+1)j}, S_{(\eta+2)j}, \dots, S_{nj}\}$ 计算密钥 $K_{ij} = f(St_{ij} \parallel xSt_{ij} \parallel Y, t)$, 并拆分成 $K_{ij1} \parallel K_{ij2}$;
 - 2) 依据 CH_j 的信息 $(C_{agg}, MAC_{agg})_j$
 - ① 计算 $e_{agg} = C_{agg} - \sum_{i=\eta+1}^n K_{ij1} \bmod M$,
 - ② 解码 $(e_{agg}, \{o_1, o_2, \dots, o_{n-\eta}\}, \mu)$:
 $m_{ij} = e_{agg}[(o_i - 1) * \mu, \mu * o_i - 1]$, 其中 $\{o_1, o_2, \dots, o_{n-\eta}\}$ 是 $\{1, 2, \dots, n - \eta\}$ 的置换,
 - ③ 对明文 $e_{ij} = m_{ij} \parallel 0^{\mu(o_i-1)}$ 计算 $MAC_{ij} = mac_{K_{ij2}}(e_{ij} + K_{ij1} \bmod M)$, 执行聚合 $MAC'_{agg} = MAC_{(\eta+1)j} \oplus MAC_{(\eta+2)j} \oplus \dots \oplus MAC_{nj}$,
 - ④ 当 $MAC'_{agg} = MAC_{agg}$ 时, 接受 e_{agg} ; 否则对应簇头 CH_j 重发。

2 安全性分析

2.1 数据机密性分析

本节将讨论本文方案的安全性, 其安全性是基于伪随机函数、安全的单向函数、消息认证码和椭圆曲线上的离散对数

难题。

本文方案加密数据聚合的安全性可归约到文献[11] 方案的安全性。在文献[11] 设计的加密数据聚合方案由下述 4 个算法组成:

- $$\begin{aligned} \text{KeyGen}(\lambda, n) &\rightarrow ek_i = f_k(i); \\ \text{Encrypt}(ek_i, m) &\rightarrow c_i = (m_i + f_{ek_i}(r)) \bmod p; \\ \text{Aggregation}(c_1, c_2, \dots, c_n) &\rightarrow c = (c_1 + c_2 + \dots + c_n) \bmod p; \\ \text{Decrypt}\left(\sum_{i=1}^n ek_i, c\right) &\rightarrow x = (c - \sum_{i=1}^n f_{ek_i}(r)) \bmod p. \end{aligned}$$

作者在文献[11] 的定理 6.2 证明了文中方案可抵抗至多 $(n - 1)$ 个参加者的共谋攻击。具体描述如下:

定理 1^[11] 若 $f_k(\cdot) : \{0, 1\}^\lambda \rightarrow \{0, 1\}^\lambda$ 是一个伪随机函数, r 是一个一次性的整数, 则上述加密数据聚合方案可安全地抵抗至多 $(n - 1)$ 参加者的共谋攻击。

定理 2 若 $f(\cdot) : \{0, 1\}^\lambda \rightarrow \{0, 1\}^\lambda$ 是一个伪随机函数, 且在子群 $\langle P \rangle$ 求解离散对数问题是难的, 则本文加密数据聚合方案 Γ 可安全地抵抗至多 $(n - \eta - 1)$ 参加者的共谋攻击, 其中 $n - \eta$ 是提供有效聚合数据的参加者。

证明 用反证法证明上述定理, 即若攻击者能从本文加密聚合的密文获取明文, 则他能攻破文献[11] 设计的加密数据聚合方案 A 。特别地, 取 $\eta = 0$, 存在共谋攻击者 A_1, A_2, \dots, A_{n-1} 在时间 γ 内使得 $\Pr[A_{A_1, A_2, \dots, A_{n-1}}(C_{agg}, MAC_{agg}) = \sum_{i=1}^n e_{ij}] > \varepsilon$, 由于文献[11] 已证 $\Pr[A_{A_1, A_2, \dots, A_{n-1}}(C_{agg}) = \sum_{i=1}^n e_{ij}] > \varepsilon$, 它们攻击方案 A 的耗时为 $\gamma + O(n(t_f + t_p))$, 其中 t_f 和 t_p 是分别计算伪随机函数和椭圆曲线上的点乘各自执行一次所需的时间。

由于在子群 $\langle P \rangle$ 求解离散对数问题是难的, 攻击者 A_1, A_2, \dots, A_{n-1} 从 $St_{ij} = r_{ij}P$ 和 $Y = xP$ 分别得到整数 r_{ij} 和密钥 x 的概率是可忽略不计。又 t 是一次性的, 令 $ek_{ij} = St_{ij} \parallel r_{ij}Y \parallel Y$, 则 $K_{ij} = f_{ek_{ij}}(t) = f(ek_{ij}, t)$; 拆分密钥 K_{ij} 为 $K_{ij1} \parallel K_{ij2}$, 即 K_{ij1} 为 $f_{ek_{ij}}(t)$ 的高位部分, 记为 $K_{ij1} = f_{ek_{ij}}^h(t)$, 这样 $c_{ij} = e_{ij} + f_{ek_{ij}}^h(t) \bmod M$ 。聚合密文可表示为 $C_{agg} = \sum_{i=1}^n c_{ij} \bmod M = \sum_{i=1}^n e_{ij} + \sum_{i=1}^n f_{ek_{ij}}^h(t) \bmod M$ 。解密操作为 $\sum_{i=1}^n e_{ij} = C_{agg} - \sum_{i=1}^n f_{ek_{ij}}^h(t) \bmod M$ 。当所有参加者提供有效的聚合数据时, 即 $\eta = 0$, 从 1 取值到 n , 则攻击者可获得 $m_i = e_{ij}$ 聚合的消息 $\sum_{i=1}^n m_i$, 故 $\Pr[A_{A_1, A_2, \dots, A_{n-1}}(C_{agg}) = \sum_{i=1}^n e_{ij}] > \varepsilon$ 。

在利用本文加密数据聚合方案 Γ 攻击文献[11] 设计的方案 A 过程中, 攻击者计算 $St_{ij} = r_{ij}P, Y = xP$ 和 ek_{ij} 中的 $r_{ij}Y$ 耗时为 $(2n + 1)t_p$; 又利用伪随机函数生成密钥 $K_{ij} = f(ek_{ij}, t)$ 耗时为 nt_f , 这里 i 从 1 取值到 n 。因而攻击方案 A 的总时间为 $\gamma + (2n + 1)t_p + nt_f = \gamma + O(n(t_p + t_f))$ 。

2.2 数据完整性分析

本文加密数据聚合方案 Γ 的数据完整性是基于消息认证码 MAC 和伪随机函数 $f(\cdot)$ 生成的密钥 K_{ij} 。由于 $ek_{ij} = St_{ij} \parallel r_{ij}Y \parallel Y$, 攻击者不可能获得 ek_{ij} 中的 $r_{ij}Y$; 又因 St_{ij} 是一次性的, 所以攻击者想获取 ek_{ij} 的概率很小, 从而它们计算密钥 $K_{ij} = f(ek_{ij}, t)$ 的概率可忽略不计。依据消息认证码 MAC 的安

全性可知,攻击者在没有密钥 $K_{ij} = K_{j1} \parallel K_{j2}$ 的情形下形成一个消息 e_{ij} 对应的消息认证码 $MAC_{ij} = mac_{K_{j2}}(e_{ij} + K_{j1} \bmod M)$ 的概率可忽略不计的。

3 性能分析

本文方案与文献[12]都是基于椭圆曲线上的 Diffie-Hellman 密钥协商算法、消息认证码、伪随机函数和椭圆曲线上的离散对数难题。假设 BS 的计算能力和存储空间能够满足系统的设计要求,下文着重分析与传感器相关的性能。相对于椭圆曲线上的点乘、消息认证码和伪随机函数计算,哈希函数、异或运算、模的加法运算和字符串的串接操作的耗时可忽略不计。

3.1 计算成本分析

在本文方案实现中,使用带密钥的伪随机函数生成相关信息的消息认证码,即执行一次消息认证码或伪随机函数计算操作所耗费的时间相同。令 t_p 和 t_f 分别表示执行 1 次椭圆曲线上的点乘和执行 1 次伪随机函数计算所耗费的时间。

传感器节点 S_{ij} 计算各自状态 $St_{ij} = r_{ij}P$ 和密钥 $K_{ij} = f(St_{ij} \parallel r_{ij}Y \parallel SK_{j1}^{BS}, t)$ 需各自执行 1 次椭圆曲线上点乘操作 t_p ,密钥生成与消息认证码生成 $mac_{ij} = mac_{K_{j2}}(St_{ij})$ 各自执行 1 次伪随机函数操作 t_f 。在转发阶段的相关操作执行次数及时间消耗与文献[12]相似,因此,转发阶段本文方案与文献[12]的时间总消耗均为: $2(t_f + t_p)$ 。

在数据聚合阶段,传感器 S_{ij} 加密数据,而簇头对它管辖传感器发送的数据执行数据聚合。在数据加密过程中,传感器 S_{ij} 生成密钥 $K_{ij} = f(St_{ij} \parallel r_{ij}Y \parallel Y, t)$ 用于加密原始数据 e_{ij} ,需要计算 $r_{ij}Y$ 和执行 1 次伪随机函数操作,所耗费时间共计为 $t_p + t_f$ 。传给基站的密文 $c_{ij} = e_{ij} + K_{j1} \bmod M$, S_{ij} 利用与簇头 CH_j 的共享密钥 K_{j1}^{CH} 加密 c_{ij} 得到 $c'_{ij} = c_{ij} \oplus K_{j1}^{CH}$,再分别生成对应的消息验证码 $MAC_{ij} = mac_{K_{j2}}(c_{ij})$ 和 $mac'_{ij} = mac_{K_{j2}^{CH}}(c'_{ij} \parallel MAC_{ij})$,此过程,传感器 S_{ij} 需要执行 2 次生成消息验证码的操作,所耗费时间为 $2t_f$ 。综上,传感器 S_{ij} 耗费总时间为 $t_p + 3t_f$ 。文献[12]的每个传感器所需要的时间耗费是 $t_p + 2t_f$,但是当某个传感器 S_{i_0j} 发送给簇节点的信息 (c_{i_0j}, MAC_{i_0j}) 受到篡改等攻击时,基站通过解密验证只能发现本次聚合数据无效,却不能定位传感器节点 S_{i_0j} 受到攻击;这样,基站为了获取正确的数据聚合,只好向网络所在簇的所有节点重新收集数据,其传感器节点计算成本为 $(t_p + 2t_f)\delta$,其中 δ 是重新收集数据的次数。本文方案通过了簇节点的认证可确定受攻击的节点 S_{i_0j} ,并对攻击节点及时采取了相应的措施,使重新收集数据的次数一般不超过 2 次,克服了文献[12]中的不足。

在数据聚合过程中,簇头 CH_j 只对传感器 S_{ij} 的有效数据进行聚合,以降低通信成本,减少基站的对无效数据的解密操作。接收来自传感器 S_{ij} 的信息 $((c'_{ij}, mac'_{ij}), MAC_{ij})$ 后, CH_j 利用与 S_{ij} 的共享密钥 K_{j1}^{CH} 计算 c'_{ij} 对应的消息验证码 $mac''_{ij} = mac_{K_{j2}^{CH}}(c'_{ij} \parallel MAC_{ij})$,再通过 mac''_{ij} 与接收的 mac'_{ij} 是否匹配来验证接收信息的有效性,此时需要进行 1 次消息认证码操作,所耗费时间为 t_f 。假设每个 CH_j 最大节点数为 L ,则 CH_j 需要进行 L 次消息认证码操作,对应的时间耗费为 $t_f L$,即簇头 CH_j 耗费总时间。本文方案和文献[12]方案的时间消耗对比分析如表 1 所示,其中 $\delta \geq 2$, L' 为有效节点个数且 $L' \leq L$,簇

CH_j 中的传感器标识符满足 $1 \leq o_i, i \leq L$,且对同一网络中相同节点 $o_i = i$ 。

表 1 计算成本对比

方案	转发阶段	聚合阶段	
		节点 S_{ij}	簇头 CH_j
本文方案	$2(t_f + t_p)$	$2(t_p + 3t_f)$	$2t_f L$
文献[12] 方案	$2(t_f + t_p)$	$\delta(t_p + 2t_f)$	—

3.2 通信成本分析

令 $|x|$ 表示二进制字符串的长度。取函数 $f(\cdot)$ 和 $mac_{(\cdot)}(\cdot)$ 输出长度为 160 比特,感应数据信息长度 $|\mu| = |m_{ij}| = 160$ 比特。

转发阶段,各节点 S_{ij} 要将各自状态 St_{ij} 与消息验证码 mac_{ij} 通过簇头节点 CH_j 转发给 BS。其中 $|mac_{ij}| = |St_{ij}| = 160$ 比特,且假设传感器节点个数为 L ,则转发阶段每个传感器节点需要发送数据长度为 $|mac_{ij}| + |St_{ij}| = 320$ 比特,而簇头节点 CH_j 则需要转发的数据长度为 $L(|mac_{ij}| + |St_{ij}|) = 320L$ 比特。转发阶段发送数据操作与文献[12]相似,同理,转发阶段本文方案与文献[12]的总通信消耗相同且均为: $(L + 1)(|mac_{ij}| + |St_{ij}|) = 320(L + 1)$ 比特。

数据加密过程,对数据编码后得到 $|e_{ij}| = |m_{ij}| \parallel 0^{\mu(o_i-1)}| = 160o_i$ 比特,对其加密后密文 $|c_{ij}| = 160o_i$ 比特, S_{ij} 利用与簇头 CH_j 的共享密钥 K_{j1}^{CH} 加密 c_{ij} 得到 $c'_{ij} = c_{ij} \oplus K_{j1}^{CH}$,故 $|c'_{ij}| = |c_{ij}|$;分别生成对应的消息验证码 $MAC_{ij} = mac_{K_{j2}}(c_{ij})$ 和 $mac'_{ij} = mac_{K_{j2}^{CH}}(c'_{ij} \parallel MAC_{ij})$, MAC_{ij} 和 mac'_{ij} 的长度为函数 $mac_{(\cdot)}(\cdot)$ 输出长度, $|mac'_{ij}| = |MAC_{ij}| = |mac_{(\cdot)}(\cdot)| = 160$ 比特。由此本文方案的数据加密过程传感器节点 S_{ij} 发送消息长度为 $|c'_{ij}| + |mac'_{ij}| + |MAC_{ij}| = 160(2 + o_i)$ 比特,文献[12]数据加密阶段传感器节点消息长度为 $|c_{ij}| + |MAC_{ij}| = 160(1 + i)$ 比特。但是当某个传感器 S_{i_0j} 发送给簇节点的信息 (c_{i_0j}, MAC_{i_0j}) 受到篡改等攻击时,同理,数据加密过程中本文方案传感器节点的消息长度一般不超过 $320(2 + o_i)$ 比特,文献[12]传感器节点的消息长度为 $160\delta(1 + i)$ 比特。

假设每一个簇中最多有 L 个节点,其中有效节点数为 L' 。数据聚合过程对密文 c_{ij} 和对应消息验证码 MAC_{ij} 进行聚合,分别得到 $|c_{agg}| = ((n - \eta)160 + 160)$ 比特 $= (L' + 1)160$ 比特,和 $|MAC_{agg}| = 160$ 比特。在数据聚合过程簇头 CH_j 发送消息的长度为 $|c_{agg}| + |MAC_{agg}| = (L' + 2)160$ 比特,文献[12]数据聚合阶段簇头发送消息长度为 $|c_{agg}| + |MAC_{agg}| = (L + 2)160$ 比特。同理,当某个传感器 S_{i_0j} 发送给簇节点的信息 (c_{i_0j}, MAC_{i_0j}) 受到篡改等攻击时,在数据聚合过程中,本文方案中簇头 CH_j 发送消息的长度一般不超过 $320(L' + 2)$ 比特,文献[12]簇头 CH_j 发送消息的长度为 $160\delta(L + 2)$ 比特。通信成本对比分析如表 2 所示。

表 2 通信成本对比 比特

方案	转发阶段	聚合阶段	
		节点 S_{ij}	簇头 CH_j
本文方案	$320(L + 1)$	$320(2 + o_i)$	$320(L' + 2)$
文献[12] 方案	$320(L + 1)$	$160\delta(1 + i)$	$160\delta(L + 2)$

3.3 确定受攻击节点时间分析

本文提出的数据聚合方案中,转发阶段相关操作类似于

文献[12],由上一节理论分析可知,本文方案转发阶段的时间消耗和通信消耗与文献[12]相同,因此在确定受攻击节点时间分析时只考虑数据聚合阶段相关操作时间对比。

当传感器节点 S_i 将加密的数据发送至簇头节点 CH_j ,簇头节点 CH_j 对数据进行认证,如果该簇网络中存在受攻击节点,此时,簇头节点 CH_j 便可以确定受攻击节点,并将节点信息发送给 BS。假设,传输 1 比特的时间为 t_b ,传感器节点数为 L 。传感器节点 S_i 向簇头 CH_j 传输数据所消耗总时间为: $\sum_{i=1}^L 160(2+i)t_b = 80(L^2 + 5L)t_b$; 确认受攻击节点前各操作时间消耗为: $t_p + 3t_f$; 由此可知,簇头节点 CH_j 确定受攻击节点的消耗时间为: $t_p + 3t_f + 80(L^2 + 5L)t_b$; 当数据发生错误时需重新收集数据,重新收集数据次数一般不超过 2 次,因此,簇头 CH_j 确定受攻击节点消耗总时间一般不超过: $2(t_p + 3t_f + 80(L^2 + 5L)t_b)$ 。而 Boudia 等的方案中,当簇头节点 CH_j 将聚合信息发送至 BS,如果存在受攻击节点,BS 对聚合数据进行解密和认证后才会发现聚合数据值是错误的,且无法确定受攻击节点信息。由分析可知传感器节点 S_i 向簇头 CH_j 传输数据所消耗总时间为: $\sum_{i=1}^L 160(1+i)t_b = 80(L+3)Lt_b$; 簇头 CH_j 向 BS 发送消耗时间为: $160(L+2)t_b$; BS 发现错误聚合值前各操作时间消耗为: $(t_p + 2t_f) + (t_p + t_f)L$; 由此可知,BS 发现错误聚合值的时间消耗为: $80(L+3)Lt_b + 160(L+2)t_b + (t_p + 2t_f) + (t_p + t_f)L = (t_p + 2t_f) + (t_p + t_f)L + 80(L^2 + 5L + 4)t_b$; 由于,当 BS 发现聚合值错误时,需要不断地重新收集数据,直到聚合值正确,因此,BS 发现存在受攻击节点消耗时间为: $\delta((t_p + 2t_f) + (t_p + t_f)L + 80(L^2 + 5L + 4)t_b)$, 其中 δ 为重新收集数据次数,且 $\delta \geq 2$,然而,当存在受攻击节点时,BS 无法得到最终正确的聚合值,同时也无法准确确认受攻击的传感器节点。由此可以得到确认受攻击的传感器节点的时间对比如表 3 所示。

表 3 确认受攻击节点时间消耗对比

方案	确认受攻击节点所消耗时间
本文方案	$2(t_p + 3t_f + 80(L^2 + 5L)t_b)$
文献[12]方案	$\delta((t_p + 2t_f) + (t_p + t_f)L + 80(L^2 + 5L + 4)t_b)$

本文方案中,簇节点 CH_j 对传感器节点 S_i 数据进行认证后,过滤错误数据,并将错误数据的传感器节点 S_i 信息发送给 BS,BS 可确定受攻击节点的信息。BS 对接收到的数据进行解密和认证,如果此时仍发现聚合值错误,则可知,受攻击的传感器节点为簇头节点 CH_j ,因此,该方案中,无论是普通传感器节点 S_i 还是簇头节点 CH_j 受到攻击,BS 都可以准确判断出受攻击的节点。若考虑信道的传输误差,当传感器节点 S_i 传输错误数据,在簇头节点 CH_j 认证时会及时发现数据错误,要求相应的传感器节点 S_i 重新发送数据;当簇头节点 CH_j 传输错误数据,BS 中消息认证错误,要求相应的簇头 CH_j 节点重新发送数据;如果在规定聚合时间内没有收到相应节点的正确信息,则将节点归为无效节点,不参与有效数据聚合操作以及其后在 BS 的解密和认证操作;因此,不正确的数据并不会影响无线传感器网络聚合数据的有效性。

在文献[12]中,若存在受攻击的传感器节点,BS 就无法获取通过认证的聚合数据,为了获取正确数据只能重新收集,因而其对应的重新收集数据次数 $\delta \geq 2$,因此,经理论分析可知,本文方案中,BS 不仅可以获取正确的聚合数据,而且确认受攻击节点的时间小于文献[12]方案,并且本文方案与文献

[12] 的方案相比,在计算成本和通信成本方面都有降低。

4 仿真实验

根据第 3 章的理论分析,对本文方案进行模拟实验,选取输出度为 160 比特的安全的单向 Hash 函数 SHA-1,并用这个 Hash 函数生成一个长度为 160 比特的随机数,采用安全的椭圆曲线 Curve P-192,即,基于 $|p| = 192$ 比特的素数域, F_p 的椭圆曲线, $E:y^2 = x^3 - 3x + b \bmod p$, 其素数阶 $|q|$ 为 192 比特^[17], 将无线传感器网络的传感器节点数目设置为 51, 其中簇节点个数为 1, 在如图 1 所示的网络结构下进行仿真实验。在不考虑网络拥塞控制的情况下,即在理想的网络状态下,无线网络传输速率可达 250 kb/s, 可知网络中传输 1 比特数据平均消耗时间为 $t_b = 1/250 \times 10^{-3}$ s = 0.4×10^{-5} s, 通过实验仿真测得执行 1 次椭圆曲线点乘消耗平均时间 $t_p = 0.346$ s 以及执行 1 次伪随机函数所需平均时间 $t_f = 0.638 \times 10^{-5}$ s, 通过实验仿真可得到各个阶段的计算成本实验数据和通信成本实验数据分别如表 4 和表 5 所示, 并且得到确认受攻击的传感器节点的时间结果如表 6 所示。在规定的时间周期内,由实验数据可得到,本文方案和文献[12]方案的总计算成本对比和总通信成本对比分别如图 2 和图 3 所示, 其中 $\delta \geq 2$, 当 δ 取值 3 和 4 时, 本文方案比文献[12]方案的计算成本分别降低了 19.96% 和 33.30%, 通信成本分别降低了 36.81% 和 52.32%, 确认受攻击节点时间降低了 94.41% 和 95.80%。随着重发次数 δ 的增加, 文献[12]方案时间消耗、通信消耗及确认受攻击节点的时间越来越大, 而本文方案则在要求第二次重发时已经确认受攻击节点。由仿真实验结果可知, 本文方案的计算成本、通信成本和确认受攻击节点时间比文献[12]方案分别降低了至少 19.96%、36.81% 和 94.41%。

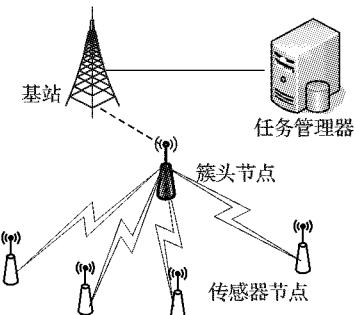


图 1 无线传感器网络结构

表 4 计算成本仿真实验结果

方案	转发阶段	聚合阶段	
		节点 S_i	簇头 CH_j
本文方案	0.69201	0.69203	0.638×10^{-3}
文献[12]方案	0.69201	0.34601	δ

表 5 通信成本仿真实验结果

方案	转发阶段	聚合阶段	
		节点 S_i	簇头 CH_j
本文	16320	440000	≤ 16640
文献[12]方案	16320	212000	δ

表 6 确认受攻击节点时间消耗仿真实验结果

方案	确认受攻击节点所消耗时间
本文方案	3.144
文献[12]方案	$18.528 \delta + 0.692$

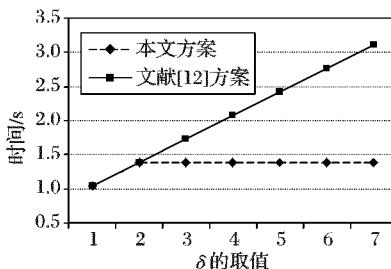


图2 本文方案与文献[12]方案总计算成本对比

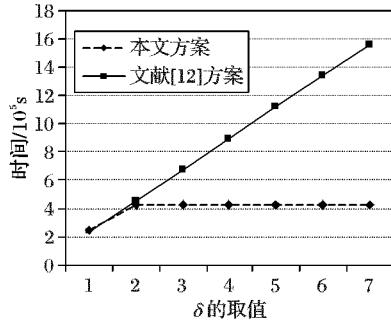


图3 本文方案与文献[12]方案总通信成本对比

理论分析和仿真实验可知,本文方案与文献[12]相比,降低了计算成本和通信成本,发现错误节点所需时间小于文献[12]方案所需时间,且能够准确发现错误节点信息。

5 结语

确定无线传感器网络中受攻击的节点可以及时对受攻击节点采取相应措施,以保障整个网络的安全性。本文针对Boudia等方案^[12]中存在的缺陷,提出了可及时确定受攻击的传感器节点的数据聚合方案。该方案通过消息认证码保障数据的完整性,并且可及时确定网络中受攻击的传感器节点信息。安全性和性能分析表明,本文方案能及时认证传感器发送的数据,过滤无效数据,确定受攻击节点并保证端到端的数据机密性和完整性。

参考文献:

- [1] CUBBI J, BUYYA R, MARUSIC S, et al. Internet of Things (IoT): a vision, architectural elements, and future directions [J]. Future Generation Computer Systems, 2013, 29(7): 1645–1660.
- [2] YICK J, MUKHERJEE B, GHOSAL D. Wireless sensor network survey [J]. Computer Networks, 2008, 52(12): 2292–2330.
- [3] AKKAYA K, DEMIRBAS M, AYGUN R S. The impact of data aggregation on the performance of wireless sensor networks [J]. Wireless Communications and Mobile Computing, 2008, 8(2): 171–193.
- [4] DU W, DENG J, HAN Y S, et al. A witness-based approach for data fusion assurance in wireless sensor networks [C]// Proceedings of the 2003 IEEE Global Telecommunications Conference. Piscataway, NJ: IEEE, 2003, 3: 1435–1439.
- [5] HU L, EVANS D. Secure aggregation for wireless networks [C]// Proceedings of the 2003 Applications and the Internet Workshops. Washington, DC: IEEE Computer Society, 2003: 384–391.
- [6] PRZYDATEK B, SONG D, PERRIG A. SIA: secure information aggregation in sensor networks [C]// SenSys '03: Proceedings of the 1st international Conference on Embedded Networked Sensor Systems. New York: ACM, 2003: 255–265.
- [7] WESTHOFF D, GIRAO J, ACHARYA M. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation [J]. IEEE Transactions on Mobile Computing, 2006, 5(10): 1417–1431.
- [8] CASTELLUCCIA C, MYKLETUN E, TSUDIK G. Efficient aggregation of encrypted data in wireless sensor networks [C]// MOBIQUITOUS '05: Proceedings of the the2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. Washington, DC: IEEE Computer Society, 2005: 109–117.
- [9] MYKLETUN E, GIRAO J, WESTHOFF D. Public key based cryptoschemes for data concealment in wireless sensor networks [C]// Proceedings of the 2006 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2006, 5: 2288–2295.
- [10] PETER S, WESTHOFF D, CASTELLUCCIA C. A survey on the encryption of convergecast traffic with in-network processing [J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(1): 20–34.
- [11] CASTELLUCCIA C, CHAN A C F, MYKLETUN E, et al. Efficient and provably secure aggregation of encrypted data in wireless sensor networks [J]. ACM Transactions on Sensor Networks, 2009, 5(3): Article No. 20.
- [12] BOUDIA O R M, SENOUCI S M, FEHAM M. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography [J]. Ad Hoc Networks, 2015, 32(C): 98–113.
- [13] CHEN S, WANG G, JIA W. Cluster-group based trusted computing for mobile social networks using implicit social behavioral graph [J]. Future Generation Computer Systems, 2016, 55: 391–400.
- [14] ZHANG Q Y, WANG R C, SHA C, et al. Node correlation clustering algorithm for wireless multimedia sensor networks based on overlapped FoVs [J]. Journal of China Universities of Posts and Telecommunications, 2013, 20(5): 37–44.
- [15] LIU Z, YUAN Y, GUAN X, et al. An approach of distributed joint optimization for cluster-based wireless sensor networks [J]. IEEE/CAA Journal of Automatica Sinica, 2015, 2(3): 267–273.
- [16] SUN H M, LIN Y H, HSIAO Y C, et al. An efficient and verifiable concealed data aggregation scheme in wireless sensor networks [C]// ICSESS '08: Proceedings of the 2008 International Conference on Embedded Software and Systems. Washington, DC: IEEE Computer Society, 2008: 19–26.
- [17] KERRY C F, SECRETARY A, DIRECTOR C R. FIPS pub 186-4 federal information processing standards publication Digital Signature Standard (DSS) [S]. Gaithersburg: National Institute of Standards & Technology, 2013.

Background

This work is partially supported by National Natural Science Foundation of China (61373125, 61272415, 61070164); the Natural Science Foundation of Guangdong Province (S2011010002708, 2010B090400164); the Science and Technology Innovation Foundation of Jinan University (11611510).

WANG Jie, born in 1993, M. S. candidate. Her research interests include information security, network communication.

LU Jianzhu, born in 1965, Ph. D., associate professor. His research interests include information security, network communication.

ZENG Xiaofei, born in 1990, M. S. candidate. Her research interests include information security, network communication.