一种无线传感器网络安全方案*

赵永安，王福豹，段渭军
(西北工业大学 宽带网络技术研究所，西安 710072)

摘 要：提出了一种无线传感器网络安全方案。它不但提供了一般的安全手段，还支持网内安全处理以延长网络生命期以及概率性多路径冗余传输来识别恶意节点。

关键词：无线传感器网络；安全方案；概率性多路径冗余传输
中图分类号：TP393 文献标志码：A 文章编号：1001-3695(2007)11-0135-04

Security scheme for wireless sensor networks

ZHAO Yong-an, WANG Fu-bao, DUAN Wei-jun
(Institute of Broadband Network, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: This paper introduced a security scheme for wireless sensor networks. It not only provided general security ways, but also offered secure in-network processing to prolong the lifetime of WSNs and probabilistic multi-path redundancy transmission to identify the malicious nodes.

Key words: wireless sensor networks; security scheme; probabilistic multi-path redundancy transmission

随着无线传感器网络越来越多的新应用出现，它的应用也越来越广泛。但是，很多传感器网络都布置在无人地区或敌方地区。这些应用的实现对无线传感器网络应用的开发人员来说存在一个很大的问题，就是如何保证这些传感器网络的安全通信。没有足够的安全性，无线传感器网络就不可能广泛应用。因此，提供安全保障机制对很多传感器网络应用来说是非常重要的。近年来，国外提出了许多用于传感器网络的安全管理方案[1~16]。

安全管理包含了安全体系建立(即安全引导)和安全体系变更(即安全维护)两个部分。安全体系建立表示一个传感器网络如何从一些独立的节点，或者说一个完全裸露的网络通过一些共有的知识和协议过程，形成一个安全的网络。安全体系变更主要是指在实际运行中，最初的安全平衡因为内部或者外部的因素被破坏，传感器网络识别并去除这些异构的恶意节点，重新恢复安全防护的过程。这种平衡的破坏可能由敌方进行外部攻击造成，也可能由敌方俘获合法的无线传感器节点造成。还有一种变更的情况是增加新的节点到现有网络中以延续网络生命期的网络变更。

本文提出了一种包括密钥管理方法和数据加密方法的安全管理方案。它除了提供一般的密钥删除与更新和数据机密以外，还支持通过使用簇密钥进行安全的网内处理，在不降低安全性的情况下，减少网络通信量，提高网络生存期。同时还能通过多层次概率性冗余路径传输发现恶意节点的窜改、丢弃等行为，并将其逐出网络。

1 攻击类型

目前针对无线传感器网络的攻击类型包括以下几种[17]：

a) 虚假路由信息。通过欺骗、窜改和重发路由信息，攻击者可以创建路由环，吸引或者拒绝网络信息流通量，延长或者缩短路由路经，形成虚假错误消息，以分割网络，增加端到端的时延。

b) 选择转发攻击。多跳传感器网络通常是基于参与节点可靠地转发其收到信息这一假设的。在选择转发攻击中，恶意节点可能拒绝转发特定的消息并将其丢弃，以使得这些数据包不再进行任何传播。然而，这种攻击者冒着邻近节点可能发现这条路由失败并寻找新路由的危险。另一种更狡猾的表现形式是攻击者修改特定节点传送来的数据包，并将其可靠地转发给其他节点，从而降低被怀疑的程度。当恶意节点在数据流传输路径上时选择转发攻击最有威胁。

c) Sinkhole 攻击。在这种攻击中，攻击者的目标是通过声明高质量路由来吸引一个区域内的所有数据流通过攻击者控制的节点，然后与其他攻击(如选择攻击、窜改数据包的内容等)结合起来，达到攻击网络的目的。由于无线传感器网络自身中所有的数据包都共享同一目的地，一个被入侵的节点只需提供一条高质量路由，就能够影响大量节点的通信。因此，传感器网络对 Sinkhole 攻击非常敏感。

d) Sybil 攻击。在这种攻击中，攻击节点向网络中的其他节点声明有多个身份，使其更易于成为路由路径中的节点，然后与其他攻击方法结合使用，达到攻击的目的。

收稿日期：2006-09-04；修返日期：2006-11-30 基金项目：国家自然科学基金资助项目(60472074)；西北工业大学研究生创业种子基金资助项目(Z200568)

作者简介：赵永安(1979-)，男，陕西人，硕士研究生，主要研究方向为无线传感器网络与安全技术(zhaoyongan@mail.nwpu.edu.cn)；王福豹(1963-)，男，山西人，教授，博士，主要研究方向为计算机网络、流媒体、传感器网络等；段渭军(1962-)，男，陕西人，副教授，博士，主要研究方向为流媒体、无线通信等.

e) Wormholes 攻击。攻击者把在网络的某个区域中收到的消息用隧道传输,并且在网络的其他区域中重放这些消息。Wormholes 攻击最为常见的形式是两个相距较远的恶意节点互相勾结,通过攻击者自有的数据传输隧道进行转发,以两个节点间貌似较短的距离来吸引路由。最简单的例子就是两个节点串通合谋进行攻击。一个恶意节点在基站附近,另一个相距较远。这个节点声称自己与基站附近节点可以建立低时延高带宽的链路,以吸引其他节点把其数据包发往这里。在这种情况下,远离 sink 的那个恶意节点其实也是一个 Sinkhole。Wormholes 攻击可以与其他攻击方式如选择性地转发或 Sybil 攻击结合使用。

f) HELLO flood 攻击。由于许多协议要求节点广播 HELLO 数据包来发现其邻近节点,收到该包的节点将确信它在发送者的传输范围内,即两者在同一个簇内。假如攻击者使用足够大功率的无线设备广播 HELLO 或其他信息,它就能够使网络中的部分甚至全部节点确信攻击者就是其邻近节点。这样,网络中的节点都试图使用这条路由与基站进行通信。但由于一部分节点距离攻击者相当远,加上传输能力有限,发送的消息根本不可能被攻击者接收而造成数据包丢失,从而使网络陷入一种混乱状态。

g) 确认欺骗攻击。一些传感器网络路由算法依赖于潜在的或者明确的链路层确认。恶意节点窃听发往邻居的分组,发送伪造的链路层确认,使发送者相信一个弱链路是健壮的,或者相信一个已经失效的节点还是可以使用的。

综上所述,不难发现网络传感器网络攻击方式:通过一(多)个节点或大功率的通信设备等方法,营造出真实存在的或者是虚假的通往基站或另一个区域的高质量路由,使被攻击者控制的节点看起来对周围基于一定路由算法的节点更具有吸引力;这样攻击者周围的每个节点就很可能会把转发目的地的数据包交给攻击者传输,并且向各自相邻的节点传播这个路由消息;然后攻击者把通过它传输的数据包进行窜改、丢弃、重播或者改变目的地等方法以造成网络的失效和瘫痪。

2 安全方案

为了便于描述,假定了下列符号:

S	密钥池(从整个密钥空间中随机选出的子集)
$\|S\|$	密钥池的大小
n	网络的节点数目
m	节点密钥环中密钥的数目
d	节点能够建立起安全连接的数目
$\|\|$	连接符
id	节点的 id 号
nonce	一个随机数
c	计数器 C 是初始向量(IV)
CH	簇首
CM	簇成员
$\{M\}_{key,c}$	消息 M 以密钥 key 和初始向量 c 加密
MAC{ key, M}	对消息 M 以密钥 key 进行认证

2.1 密钥分配

由于传感器有限的能量供给、计算和通信能力,使得其成网后计算、分配密钥是不现实的。目前在无线传感器网络中,引导密钥(bootstrapping secret keys)的最实用方法就是使用预分配密钥方法,也即密钥在节点被散布前就装载入每个节点。这样就免去了传感器节点很多的计算、通信能量,使网络的生命期更长。

如果网络使用全局密钥,即整个网络使用同一个密钥来进行数据加密。这样可以节省节点的内存并且减少节点为了协商密钥而进行的通信开销。但是使用全局密钥是很危险的,如果某一个节点被破解,就会导致整个网络的通信失去机密性。如果网络使用成对密钥,即每个节点提前装载网络剩余节点与之通信的密钥,这样网络的安全性被大大提高了。某一个节点被破解只能影响与它有关的通信,网络中其他节点之间的通信还是具有机密性。但成对密钥的代价是,每个节点要存储 $n-1$ 个密钥。当网络中节点数目很大时,这种存储代价对于存储量有限的传感器节点是不可接受的。所以本方案使用基于概率的密钥预分发方式进行节点散布前的密钥装载。

在本方案中,密钥分配由三个阶段组成,分别是密钥预分发、共享密钥发现和多跳密钥建立。

密钥预分发阶段由以下两个步骤组成:

a) 从整个密钥空间中随机选取 $|S|$ 个密钥和每个密钥的标志,产生密钥池 S。

b) 从 S 中随机抽取 k 个密钥和它们的标志,建立节点的密钥环,将密钥环装载入每个节点的内存。

根据文献[1]可知,在合适的密钥池的大小、密钥环的数目和网络密度条件下,就可以得到非常高的任意两节点有一个共享密钥的概率(如 0.999 9)。

共享密钥发现阶段发生在网络散布后初始化时,每个节点在无线通信范围内发现与它共享密钥的邻居。

c) 对于任意两个节点,每个节点都广播它们的密钥环上的密钥标志列表。收到广播的节点,比较接收到的密钥环和自己的密钥环,看是否有相同的密钥标志符即密钥。如果发现有共同密钥,则发送用该共同密钥加密的自己的 id 号给那个广播密钥环的节点。广播密钥环的节点收到数据包后,用共享密钥解密,读取 id 号;并存储节点 id 和密钥标志之间的对应关系,方便以后的使用。

A ——〉* : ID

C ——〉A : $\{\text{nonce, id}\}_{k,c}$

在共享密钥发现阶段以后,还有一些节点之间因为没有共享密钥而无法建立安全通信。但是它们被两条或多条链路连接。可以通过多跳密钥建立阶段为这些节点建立一个多跳密钥。

d) 对于一对在无线通信范围内没有共享密钥但被两条或多条链路连接的传感器节点,当它们发现在共享密钥阶段结束后,它们之间还没有建立共享密钥,但可以找到一个中间节点。该中间节点与这一对节点都有共享密钥,并各自建立了一条链路。这时,源节点可以发送一个包含 nonce 的数据包给中间节点,并以它们之间的密钥加密。

A ——〉D : $\{\text{nonce, id}\}_{k,c}$

e) 中间节点解密后,再用它与另外一个节点共享的密钥加密,发送给目标节点。

D ——〉C : $\{\text{nonce, id}\}_{k,c}$

f) 目标节点接收后,解密数据包,然后回复包含 nonce 的数据包给源节点,并以新密钥加密。源节点接收到数据包后,

查看 nonce 是否与它设定的相同。如果相同, 则建立多跳密钥成功。

两者之间的密钥有多种方法确定: (a) 由源节点指定, 放在发送给中间节点的数据包中, 由中间节点传递给目标节点; (b) 由中间节点确定, 然后分别告诉原节点和目标节点, 这时中间节点充当 server 的角色; (c) 把中间节点与原节点和目标节点的密钥异或, 中间节点只将另一个密钥告诉两个节点, 由它们自己合成。

g) 执行分簇算法。选举簇首后, 由簇首确定一个簇密钥 (簇首可以异或自己的密钥环来产生自己的簇密钥) ; 然后簇首用与每个簇成员共享的密钥加密簇密钥, 分别发送给每个簇成员。每个簇成员接收到后保存簇密钥。

$$CH \longrightarrow CM_i: \{k_{cluster}\}\, k_i$$

2.2　加密通信

当节点需要与另一个节点通信时, 通过共享密钥和两个不同的碰撞自由的单向散列函数计算加密密钥和认证 (MAC) 密钥; 然后使用这两个密钥对要发送的数据包进行加密。

接收节点收到数据包以后, 同样计算两个密钥, 然后解密。

$$A \longrightarrow C: \{\{M\}_{k,c}, MAC\{k, c \mid \{M\}_{k,c}\}$$

在无线传感器网络中有一个独特的需要注意的问题, 即密钥加密方法对网内处理的影响。在很多应用中, 网络中的传感器被要求进行数据融合 (aggregation) 、冗余删除 (duplicate elimination) 和被动加入 (passive participation) 来提高效率和网络的生命周期。从某几个节点上收集的读数或信息会在一个数据融合节点进行数据处理, 然后压缩成一个更加紧凑的格式传送给中央处理节点。被动加入是另一种网内处理, 它使节点能够监听信息, 然后采取特定的行动。比如节点可以在监听到邻节点报告了相同事件时, 取消报告该事件。加密方法可能会阻碍或降低网内处理的效能。为了支持被动加入, 中间节点必须能够解密或认证在另外两个节点上传输的加密信息。因此, 只有多个节点共享加密和认证的密钥才能提供被动加入。

在需要网内处理的信息收集时间内, 节点可以采用簇密钥加密信息, 然后根据路由算法返回给数据处理中心。每个转发的节点接收到数据包后, 解密数据包, 然后再用自己的簇密钥加密。由于采用节点的簇密钥加密, 这样途经的节点及这些节点的簇成员可以看到信息内容, 就可以很方便地进行对信息的精简和再加工, 减少网络的流量, 延长网络的生存时间。

$$A \longrightarrow C: \{\{M\}_{k,c}, MAC\{k, c \mid \{M\}_{k,c}\}$$

2.3　概率性多路径冗余传输

节点每发送一个消息, 就同时产生一个随机数字, 然后把这些数字累计相加。当和大于一定门限值时, 就把当前的数据以加密方式分别传送给每个相邻节点, 由各个相邻节点通过自己的路由传送回 sink 节点, 由 sink 节点把数据返回给数据处理中心。数据处理中心可以通过比较该数据的多个版本来检察网络中是否有恶意节点, 并且网络中使用频率高、信息流量大的区域(这种区域往往是敌方的攻击重点) 被检查的概率大一些, 使用频率低、信息流量小的区域(这种区域不是敌方的攻击重点) 被检查的概率小一些, 这样既动态地检查了网络安全性, 通信开销也没有太大的增长。

每次产生的都是随机数字, 就算敌方通过捕获节点获得了门限值, 也无法正确地估计每个节点进行多路径冗余传输的具体时间, 所以恶意节点的行为无法避免被数据处理中心发现, 进而被驱逐出网络。

对于重要信息, 数据包在经过随机跳数以后, 当前的接收节点把数据再分别以安全方式传送给每个相邻节点; 然后由各个相邻节点通过自己的路由传送回 sink 节点, 由 sink 节点把数据返回给数据处理中心。这样多层次概率性多路径冗余传输扩大了冗余传输的成功率, 可以使同一个数据包由更多的路径回到数据处理中心, 方便数据处理中心检查该信息路由路径上有没有恶意节点。

2.4　密钥撤销

由于传感器节点是散布在敌方地区, 传感器节点可能被捕获或破坏, 从而导致密钥泄露。网络安全体系应能够撤销那个节点密钥环上的所有密钥集合。数据处理中心在分析数据接收器(sink) 节点回传的数据以后, 如果对某个节点产生怀疑, 就通过 sink 节点广播一个撤销投票命令, 使得与该节点相邻的所有节点发起一个投票选举; 如果撤销票数超过一定门限值, 就由数据处理中心发起对该节点的节点 id 和密钥集合的撤销。

数据处理中心通过 sink 节点, 向与 sink 节点相邻的簇首发送一个包含被撤销节点的节点 id 和密钥环上的 k 个密钥标志列表的撤销信息。撤销信息使用 sink 节点与其相邻簇首的共享密钥加密和认证。收到消息的簇首节点分别用簇密钥和共享密钥加密的信息通知自己的簇成员和与自己相连的簇首。这样撤销消息就传达到了整个网络, 并且网络信息流量较少, 大大节省了能量。

在获得撤销信息后, 每个节点在它们自身的密钥环上查找这些节点 id 和密钥标志, 然后删除路由表中有关节点 id 的信息和密钥标志所对应的密钥。一旦从密钥环上删除了这些密钥, 一些链路可能会消失, 被影响的节点需要通过重新开启共享密钥发现机制来重新配置那些链路, 同样路径密钥也可能被重新建立。因为只有 k 个密钥被从密钥池中删除, 所以密钥撤销仅仅影响了一小部分其他的节点和它们密钥环上的一小部分密钥。但是这样却可以禁止被捕获节点的所有连通链路。

当删除的是簇首时, 被影响的簇重新进行簇组织。当簇重组后, 新的簇首重新确定一个簇密钥, 然后簇首用与每个簇成员共享的密钥加密簇密钥, 分别发送给每个簇成员。每个簇成员接收到后保存新的簇密钥。

2.5　密钥更新

尽管人们期望在传感器网络中两个节点之间的共享密钥的生存期长于两个节点的生存期, 但在一些情况下密钥的的生存期会耗尽而需要更新密钥。密钥更新相当于一个节点对自己的一个密钥进行撤销。在删除了耗尽生存期的密钥后, 受影响的节点重新进行共享密钥发现和路径密钥建立阶段。

3　安全分析

由于使用了簇密钥, 既大大降低了通信开销, 同时还保证了网内处理的安全; 除了在网络初始时节点广播密钥环以外, 其他时候的网络通信均是在共享密钥的加密下完成的, 所以很

好地保护了网络数据内容的机密性; 由于双方共享一个密钥, 由它计算出来的 MAC 认证密钥具有与数字签名相似的身份认证功能, 可以起到数据源认证功能, 保证数据的真实性; 同时根据散列函数的强无碰撞特性, MAC 认证可以发现对数据的任何微小的改动, 保证了数据的完整性; 由于通信使用计数器, 可以提供数据新鲜性、语义安全和防重放; 由于采用链路层加密机制, 尽可能早地发现拒绝服务攻击, 能很好地解决拒绝服务攻击。考虑到传感器节点本身的性能限制, 本文的加密算法采用对称加密算法。

大部分外部攻击通过简单的链路层加密和认证就可以防止。由于网络通信之前要建立安全链路, 而外部攻击节点没有相同密钥池中的密钥、密钥标志和节点 id, 无法通过建立安全链路来加入到网络中。外部攻击节点无法加入网络, 也就无法通过窜改、重发或丢弃路由信息来进行虚假路由信息攻击、选择转发攻击和确认欺骗攻击; 无法声明高质量的路由和多重身份来进行 Sinkhole 攻击和 Sybil 攻击; 因为在建立安全链接时, 收到攻击节点发送的 HELLO 包的节点发送给攻击节点的建立安全链接的数据包无法被攻击节点收到, 所以安全链路不会建立, 攻击节点也就不会被节点相信; 对于 Wormholes 攻击, 由于攻击节点没有密钥, 无法窜改经过的信息。而数据处理中心会从被概率性多路径冗余传输回来的信息中发现 Wormholes 攻击节点丢弃了的路由信息, 从而将其驱逐出网络。

当攻击者进行内部攻击时, 即攻击者俘获了网络中的某个节点, 获取了密钥, 重新把攻击者控制的节点放入网络中进行攻击时, 攻击者试图产生虚假信息以通过攻击节点周围的冗余节点发回来的信息由数据处理中心比较发现; 对于选择转发攻击和 Sinkhole 攻击, 本文的冗余传输可以很容易地发现; 由于节点都有节点 id, 如果多个 id 号出现在网络中, 会被数据处理中心发现, Sybil 攻击也无法实现; 由于需要恢复才能建立安全连接, 无法收到正常节点恢复的 HELLO flood 攻击者并不会被多个节点认为是朋友; 由于加密方案中有认证, 确认欺骗攻击也行不通; 对于 Wormholes 攻击, 如果不修改经过攻击节点的信息, 仅能造成局部路由混乱, 如果修改了信息, 就可以通过冗余传输来发现。对于识别出的恶意节点, 数据处理中心可以在网络中发布节点撤销和密钥撤销的命令。

4 结束语

本文介绍了无线传感器网络的常见攻击类型, 并对这些攻击类型作了分析, 总结出它们的共性; 然后提出了一种包括密钥管理方法和数据加密方法的安全管理方案, 描述了它的工作过程, 并对其安全性能进行了分析。它能够支持密钥建立、更新和撤销等过程, 提供网络数据内容的语义加密、数据源认证、数据完整性和数据新鲜。它还通过簇密钥支持如数据融合、冗余删除和被动加入等网内计算来精简网络数据, 降低网络通信量, 提高效率和网络生存期。同时, 它通过多层次概率性多路径冗余传输以较大的概率将一个使用频率高、信息流量大的区域(这种区域往往是敌方的攻击重点) 的数据冗余地传送回数据处理中心。这样可以更好地监控重要区域的安全情况, 尽早地发现恶意节点。

该方案提供对外部攻击方式和内部攻击方式的主动和被动防御, 识别恶意节点并将其驱逐出网络, 对无线传感器网络提供了很好的安全防护。

参考文献:

[1] SCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[M] . Washinigton D C: ACM Press, 2002: 41-47.

[2] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[M] . Berkeley, CA : IEEE Computer Society, 2003: 197-213.

[3] JOLLY G, KUSCU M C, KOKATE P, *et al*. A low-energy key management protocol for wireless sensor network[C] //Proc of the 8th IEEE Int Symposium on Computers and Communications. Turkey: [s. n.] , 2003: 335-340.

[4] CARMAN D, KRUUS P, MATT B. Constraints and approaches for distributed sensor network security, Technical Report #00-010[R] . [S. l.] : NAI Labs, 2000.

[5] PERRIG A, SZEWCZYK R, WEN V, *et al*. SPINS: security protocols for sensor networks[J] . Journal of Wireless Networks, 2002, 8(5) : 521-534.

[6] PERRIG A, CANETTI R, TYGAR J D, *et al*. The TESLA broadcast authentication protocol[J] . Cryptobytes, 2002, 5(2) : 2-13.

[7] ZHU S, SATIA S, JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks[C] //Proc of the 10th ACM Conference on Computers and Communications. Washington D C: ACM Press, 2003: 62-72.

[8] DU Wen-gang, DENG Jing, HAN Y S, *et al*. A pairwise key pre-distribution scheme for wireless sensor networks[M] . Washington D C: ACM Press, 2003: 1-10.

[9] BLOM R. An optimal class of symmetric key generation systems[M] . Paris: Springer-Verlag, 1985: 335-338.

[10] LIU Dong-gang, NING Peng, LI Rong-fang. Establishing pairwise keys in distributed sensor networks[M] . Washington D C: ACM Press, 2003: 52-61.

[11] BLUNDO C, SANTIS A D, HERZBERG A, *et al*. Perfectly-secure key distribution for dynamic conferences[M] . Santa Barbara, California: Springer-Verlag, 1993: 471-486.

[12] WADAA A, OLARIU S, WILSON L, *et al*. Scalable cryptographic key management in wireless sensor networks[M] . Tokyo: IEEE Computer Society, 2004: 796-802.

[13] DU Wen-liang, DENG Jing, HAN Y S, *et al*. A key management scheme for wireless sensor networks using deploying knowledge[C] //Proc of INFOCOM. Hong Kong: IEEE Computer Society, 2004: 172-183.

[14] LIU Dong-gang, NING Peng. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks[M] . San Diego, California: Internet Society Press, 2003: 263-276.

[15] BOHGE M, TRAPPE W. An authentication framework for hierarchical Ad hoc sensor networks[M] . San Diego, California: ACM Press, 2003: 79-87.

[16] MOHAMED G G, ELNOZAHY E N, HUANG C T, *et al*. Hop integrity in computer networks[J] . IEEE/ACM Transactions on Networking, 2002, 10(3) : 308-319.

[17] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countemeasures[C] //IEEE International Workshop on Sensor Network Protocols and Applications. 2003: 113-127.