一种基于IBE的WSNs选择转发攻击检测方案

陈丹伟 侯 楠 孙国梓

(南京邮电大学计算机技术研究所 南京 210003) (南京邮电大学计算机学院 南京 210003)

摘 要 无线传感器网络因节点能力的限制,通常采用多跳的方式进行节点间消息的互发,这种多跳路由协议为选择转发攻击提供了便利。基于此,提出一种基于随机检查点的多跳确认方案来检测无线传感器网络中的选择转发攻击,将IBE加密及LEACH路由协议引入其中,用以对选择转发攻击的检测方法加以改进。给出检测防御方案的总体框架,对其工作方式进行了具体描述。在NS2环境下,从检测点数目、计算速度与能耗、存储要求及健壮性等几方面对改进方案进行了仿真,以验证其对无线传感器网络安全性的提高。

关键词 无线传感器网络,位置绑定ID密钥,选择转发攻击,入侵检测

中图法分类号 TP393 **文献标识码** A

Novel Detection Scheme Based on IBE in WSNs Selective Forwarding Attacks

CHEN Dan-wei HOU Nan SUN Guo-zi

(Institute of Computer Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

(College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract Since nodes in wireless sensor networks have limited capabilities, messages are generally transmitted between nodes through multi-hop. The multi-hop routing protocols provide a lot of convenience for the selective forwarding attack. As a result, a random checkpoint-based multi-hop acknowledge scheme to detect selective forwarding attacks in WSNs was brought out. At the same time, IBE and LEACH were adopted to improve the formal detecting scheme. Firstly, the overall framework of defense scheme and its working method were given, then, the scheme was simulated in the NS2 environment, thinking about many factor, such as the number of checkpoints, the calculating speed and consumption, the storage requirements, the robustness and so on. The results show that the WSNs' security has improved.

Keywords Wireless sensor networks, Location ID key binding, Selective forwarding attacks, Intrusion detection

1 引言

无线传感器网络(Wireless Sensor Networks, WSNs)是一种由具有感知、计算和无线网络通信能力的微型低功耗传感器节点通过自组织的方式构成的网络[1]。一般的WSNs都会有一些能量和运算能力较高的基站(base station),它是整个网络与外界联系的枢纽,完成与其他网络互通消息或通过卫星向总部反馈消息等。普通传感节点因为能力的限制,在通信中一般采用多跳的方式,节点相互转发消息。这种网络系统在军事国防、生物医疗、环境监测、抢险救灾以及商业等领域有着广阔的应用前景。

WSNs中的传感器节点一般使用电池供电,其能量、存储能力和计算能力都十分有限,节点的脆弱性使构建一个有效且安全的网络架构成为挑战性的研究课题。这类网络很容易受到包括虫洞攻击(worm hole)、污水池攻击(sink hole)、女巫攻击(sybil)等各种入侵的攻击,其中由Karlof[2]最先提出的选择转发攻击(selective forwarding attacks)是最具代表性的一类攻击方式。在这类攻击中,被俘获的恶意节点在大多数时间内的表现和正常节点一样,但它们会有选择性地丢弃一些包含重要信息的包,具有很大的迷惑性,特别是当它与其它攻击相结合后,往往会变得更有破坏力,可以对WSNs运行的路由协议产生毁灭性打击。

国内外针对选择转发攻击提出的解决方法还很少,由Karlof提出的多路径转发方法可以在一定程度上缓解选择转发攻击的影响,但是其通信开销过大,无法在基站处防范攻击,因此可实施性并不高。BO和BIN[3]等提出通过基于检查点的多跳确认方案来检测选择转发攻击所导致的异常丢包,随机选取转发路径中的部分节点为检查点,负责包的确认,在保证检测能力的同时也提高了系统的健壮性,但其使用的是对称密码体制,需要密钥的预处理过程,节点变动时需要建立新的相邻节点密钥对,灵活性差,安全性相比非对称密码体制低一些。在此背景下,本文提出了一种基于IBE[4]的改进的

到稿日期:2009-06-02 返修日期:2009-09-08 本文受国家科技攻关项目(2007BAK34B06),国家自然科学基金(60703086),南京邮电大学攀登计划项目(NY208009)资助。

陈丹伟(1970—),男,博士,副教授,硕士生导师,主要研究方向为计算机通信网与安全、嵌入式系统及应用等;侯 楠(1984—),男,硕士生,主要研究方向为计算机通信网与安全;孙国梓(1972—),男,博士,副教授,硕士生导师,主要研究方向为计算机通信网与安全、计算机取证等,E-mail:sun@njupt.edu.cn。

公钥加密方法，该方法可以克服对称加密的缺陷，加入节点地理位置信息，并借鉴无线传感器网络经典路由协议LEACH[5]的簇头选择算法，在转发路径中随机选取监测点，解决了检测点的随机选取问题，提高了系统的健壮性。同时该方法计算量和开销处于传统非对称加密（如RSA）和对称加密（DES）体系之间。仿真及实验结论说明提出的方案是可行的。

2 改进的选择转发攻击检测

一般情况下，可通过有效地布置检测节点，对传输的数据包进行确认，该方法简单，但也可以在很大程度上检测出转发过程中不正常的丢包，发现导致丢包的可疑节点。

考虑到WSNs具有能量限制，采用了一种比较被动的检测方式。在BO和MIN提出的基于检测点的多跳确认机制基础上，提出了一种少量节点的被动检测方案，随机设置少量的检测节点，在传输的路径上对收到的数据包进行回报响应。除此之外，出于能耗与安全性平衡的考虑，引入了一种新的密钥技术。

2.1 位置绑定ID密钥技术

IBE（Identity-Based Encryption）[4]由Shamir 1984年首先提出，该算法的主要特征是加密用的公钥不是从公钥证书中提取，而是直接使用标示用户身份的字符串，目前可使用的IBE方案由Boneh和Franklin 2001年提出，安全性建立在BDH（Bilinear-Diffie-Hellman）困难问题之上，以超奇异椭圆曲线上的一个双线性映射（Weil pairing）为核心，具有双线性性、非退化性和可计算性等优势[6]。

在节点间通信或发送消息时，将节点的地理位置信息与节点唯一的ID号绑定在一起，使用改进密钥的IBE体系。加入地理位置信息后，可以有效解决被俘获节点冒充正常节点及入侵者仿造节点等问题。事实上，单单采用ID时是无法做到这一点的。

在部署阶段，可假设传感器网络处于完全安全状态，入侵者无法俘获我方节点。事实上，已有的传感器网络安全协议研究中同样具有该假设前提，并且可以证明在实际操作中，可通过采用适当的保护措施来实现这一点。记负责生成并传送用户私钥的可信第三方为PKG。

节点被布置在特定的场景后，可以通过很多方式获得自己的位置信息，如GPRS[7]等。因此，节点在一系列的操作后可以获得与位置信息绑定后的密钥。以节点A为例，节点地理位置为l_A，产生$LK_A=sH(ID_A||l_A)$。本文假设网络中有一些节点具有自我定位的能力，其他不具有这种能力的节点通过与它们的交互获得位置信息并生成自己的节点信息。同样其它节点的LK也由节点自己计算得到。每个节点X通过随机预置的主密钥s计算出$LK_X=sH(ID_X||l_X)$。

在此基础上，将引入地理位置信息后的LK替代经典IBE算法中的ID，改进的算法如下：

1) Setup

Step 1 PKG选择k比特长的素数p，找一条满足BDH安全假设的超奇异椭圆曲线$E/GF(p)$，生成$E/GF(p)$上的q阶子群G和G的生成元P，以及双线性映射$\hat{e}:G\times G\rightarrow GF(p2)^*$。

Setp 2 PKG随机取$s\in Z_q^*$，计算$P_{pub}=sP$。

Step 3 选择散列函数$H_1:\{0,1\}^*\rightarrow E/GF(p)$，$H_2:GF(p^2)\rightarrow\{0,1\}^n$。明文空间$M=\{0,1\}^n$，密文空间$C=E/GF(p)\times\{0,1\}^n$，输出的系统公共参数$\pi=\{q,p,\hat{e},n,P,P_{pub},H_1,H_2\}$，$s\in Z_q^*$为主密钥（Master key）。

2) Extract：对给定的字符串$LK\in\{0,1\}^*$，生成密钥。

Step 4 计算$Q_{LK}=H_1(LK)\in E/GF(p)$。

Step 5 取密钥为$K_{LK}=(Q_{LK})^s$。

3) Encrypt：对原文$m\in M$和公钥LK，加密步骤如下。

Step 6 计算$Q_{LK}=H_1(LK)\in E/GF(p)$。

Step 7 随机取$r\in Z_q^*$，加密的密文为：

$c=\langle rP,m\oplus H_2(g_{LK}^r)\rangle$

式中，$g_{LK}=\hat{e}(QLK,P_{pub})\in GF(p^2)$

4) Decrypt：设$c=\langle U,V\rangle$为密文，解密步骤如下。

Step 8 应用密钥$K_{LK}\in E/GF(p)$，计算原文：

$m=V\oplus H_2(\hat{e}(K_{LK},U))$。

参数π和每个节点的K_{LK}在部署时就预置到节点中。需要说明的是，上述步骤的实现依赖于假设节点在布置后的一段时间内是安全的。在密钥生成后节点擦除保存的主密钥s。由于密钥的生成及分发等均在部署阶段完成，可以认为初始化过程并不消耗资源，能耗主要集中在加解密过程中。

2.2 基于LEACH的检测点选择

一种简单的方法是在源节点发送第一个事件包前，事先选择一个固定的检查点名单。这些被事先确定的中间节点在随后的事件包到来后，担当检查点的角色，一旦一定数量的检查点被俘获，敌方就能够轻易丢弃事件包，并通过编造ACK包的方法来避免其丢包行为被上游节点检测到。因此，需要实现一种随机的检查点选择方法，以降低中间节点共享成为俘获目标的风险，避免单点失败。

LEACH（Low Energy Adaptive Clustering Hierarchy）协议[5]是传感器网络中使用较多的一类路由协议。该协议以循环的方式随机选择簇首节点，将整个网络的能量负载平均分配到每个传感器节点中，从而达到降低网络能源消耗、提高网络整体生存时间的目的。

在本文提出的检测方案中可以应用LEACH协议中的簇头选择算法来解决检测点的随机选取问题。其优点主要包括：1）保证通信链路上的每个节点公平地享有成为检测点的几率，使系统的健壮性增强，避免了单点失败；2）由于检测点相比普通节点耗能多一些，采用随机公平的选取方法，使得各个节点耗能相当，从而增加了节点的平均生存时间；3）虽然随机点选取会增加能耗，但是相关研究表明能耗并不大，通过适量增加能耗来达到增加系统安全性的目的，理论上是可行的。

假设WSNs中某通信链路总节点数为N，期望的检测点个数为k，每个节点初始成为检测点的概率为$p=k/N$，每个节点本地有一函数H，每次转发时产生一随机值。LEACH是周期性执行的，系统一个周期的平均转发数$R=N/k=1/p$（其中N/k取整）。每次有源节点要发送信息就进行一次选举。为了简化，下面只讨论系统一个周期内的行为。因为检测点选取只在每次转发的开始，采用离散的整数r代表每一次转发（$r=0,1,2,\cdots,R$）。$x(r)$表示第r次检测点选取产生的检测点个数，$N(r)$表示第$r-1$次选择后还未成为检测点

的节点个数。可以将$\{x(r);r=0,1,2,\cdots,R\}$看作一个随机过程。

传感器节点由本地函数 H 随机地生成一个 0,1 之间的随机数,如果小于阈值 T,则该节点当选为检测点,T 按下列公式计算:

$$T=\begin{cases}\dfrac{p}{1-p*[r \bmod (1/p)]}, & \text{if } n\in G\\ 0, & \text{if } n\notin G\end{cases}$$

式中,P 为每轮节点成为检测点的百分数(可推知聚类的个数),r 为当前轮数。采用此计算公式可以保证每个节点在连续的 $1/p$ 次转发中的某一次成为检测点。

3 检测方案

3.1 方案防御总体规划

参考文献[3],针对选择转发攻击的总体防御步骤可以包括 3 个步骤:预备阶段、入侵检测阶段和响应阶段。

1)预备阶段

即整个传感器网络节点的部署阶段,网络进行节点间邻居发现、路由建立等初始化工作,同时进行 IBE 体系的初始化工作,产生用于加解密的公钥和私钥,在所有工作完成之后,还要将节点内存中的初置 s 擦除。

2)入侵检测阶段

入侵检测机制与网络常规路由协议协同运行,在数据采集传播的同时完成对网络异常丢包的检测。

3)响应阶段

当足够多的网络异常丢包信息被基站或者源节点收集后,决策模块可以根据预先规定的规则对各种入侵做出相应响应,如路由协议会减少通过可疑节点的流量。

本文提出的基于 IBE 的随机检查点多跳确认方案主要是针对第二阶段,检测选择转发攻击所导致的异常丢包。在这个方案中,能够随机地选取转发路径中的部分节点为检查点,负责包的确认。这种随机检查点的选择技术能够避免部分节点成为敌方俘获的目标,从而在保证检测能力的同时有效地提高系统的健壮性。

3.2 工作方式

方案采用 BO 和 BIN[3] 提出的检查点多跳确认方案框架,将 IBE 公钥加密和基于 LEACH 的随机节点选取算法引入,并直接引用 μTESLA[8] 安全多播协议帮助多节点间实现一对多的身份认证。通过该方案,不仅可以检测出转发过程中不正常的丢包,发现导致丢包的可疑节点,还可以提高整个系统的安全性和强健性。

图 1 中,称在一条从源节点到基站的转发路径上,靠近源节点的方向为上游,靠近基站的方向为下游,转发路径的部分节点会被随机选择成为检查点。称路径上两个连续的检查点之间的中间节点构成了一个中间节点段。这样,一条转发路径即由若干检查点和中间节点段组成。当源节点 S 检测到一个特定的事件时,源节点生成事件包并用接收方(这里取基站)的公钥 Q_R 由 IBE 体系加密,同时转发路径上的各节点由本地的函数 H 各生成一随机数,根据 LEACH 协议的簇头选举算法,随机选取出几个节点作为此次转发过程的检测点(此例中取 $u3$,$u5$,$u8$)。此后该事件包沿着路径,经过多跳转发向基站传递。

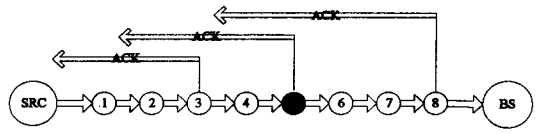

图 1 多跳确认方案示例

如果一个检查点从上游邻居节点收到了一个事件包,在继续转发前该检查点会为该事件包生成一个 ACK 包,并选择 μTESLA 密钥链上当前的密钥对整个 ACK 包内容签名并生成一个 MAC 码。之后该 ACK 包将沿着与先前事件包相同的路径但相反的方向向上游转发,并在穿过了若干中间节点段后,会被某个检查点或源节点抛弃。

这是因为 ACK 包上的 MAC 码可认证其来源,所有 ACK 包所穿过的中间节点会相信先前的事件包已安全地到达了下游的检查点。如果这些中间节点没有收到 ACK 包(或者没有收到足够数量的 ACK 包),则很有可能先前的事件包已被某个被俘获节点恶意丢弃。这里假设 $u5$ 节点被俘获,并且丢弃了事件包,那么节点 $u4$,$u3$ 无法收到来自 $u8$ 的 ACK 包,这样节点 $u4$ 就会生成报警包指定其下游的直接邻居节点 $u5$ 为可疑节点,使用 MAC 码对报警包内容签名后转发给源节点。

源节点收集到足够报警包后,会采取相应响应措施应对上述的入侵行为。

4 模拟实验及结果分析

在 NS2 环境下对本方案进行了仿真,硬件配置情况为:CPU 为 Intel Pentium Dual E2140,内存 1G,操作系统为 Linux Ubuntu 8.10。实验场景假定 100 个节点随机分布在 100×100 的场地内,基站坐标为(50,150),距离其最近的节点也在 100m 以外,满足 LEACH 协议的基本假设。节点初始能量设为 3J,节点之间通信速率 19.2kbps。

4.1 检测点数目

在本文提出方案的背景之下,检测点的数目对于检测效率和能耗等具有重要作用,每轮平均能耗的大小决定了整个网络的生存周期,因此比较检测点数目不同时的耗能情况,选出最优检测点数目,具有重要的意义。

在前述实验环境中,设置每 10s 源节点发送一事件包,无其它事件发生,且信道误码率设为 0(即不考虑信道误码率对此次实验的影响),分别观察检测点为 $N(1\leqslant N\leqslant 10)$时,网络平均能耗的情况,结果见图 2。

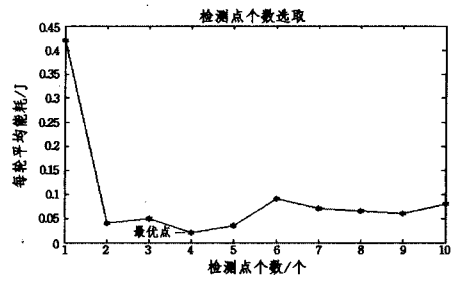

图 2 检测点个数选取

从图 2 中可以看出,当检测点数目为 4 时,平均能耗值最低,约为 0.02J,其它情况下除 N 为 1 外,耗能都在 0.1J 之内,这也表明通过适当选取检测点数目,可以将额外耗能降到一定水平,在提高安全性的同时具有一定的可操作性。在后面的实

验中均假定每轮通信中选取的随机检测点数目为4个。

4.2 计算速度与能耗

由于传统的非对称密码体制(如RSA)已被证明不适合无线传感器网络,因此这里只比较IBE和DES之间的计算速度。在DES算法中,采用的是固定56位密钥,以64位为单位对明文进行加解密;在IBE中以64位密钥对相同明文加解密,对比结果见表1。

表1 计算速度对比

	密钥长度(bit)	加密时间(s)	解密时间(s)
DES	56	0.00139	0.00112
IBE	64	4	3.2

从计算速度上来看DES比IBE快了许多,不过考虑到传感器节点的能耗主要在通信工作中(将1bit信息传输100m耗能相当于执行3000条加解密指令[9]),综合看来虽然IBE增加了计算时间,但是总的能耗比起DES并没有大太多,而且作为新型非对称体制的IBE在密钥分配及管理方面比起对称体制的DES具有无可比拟的先天优势[10],所以我们提出的方案具有一定的可实施性。

4.3 存储要求

对无线传感器网络中的节点,理想的内存需求是仅仅存储与相邻节点的密钥。在我们的方法中,每个节点需要保存的信息有在算法中用到的参数π,以及与相邻节点的密钥。与理想的内存开销相比,仅仅多了公共参数π,与所有的存储密钥内存开销相比,这一部分是相对小的。

因此在内存开销方面,我们的方法达到了一定的层次。而对于消息队列的存储,可以根据具体的场景和检测率进行相应的调整,尽量将节点存储的消息限定在一定的范围内,以达到一个最大限度的平衡。

4.4 健壮性

在对称密码体制中,节点之间使用相同的加解密密钥进行通信,因此如果一个节点被俘获,全网就变得不安全,通信无法得到保障[11]。

在我们的算法中,生成的每对对称密钥都不相同,只有进行通信的双方拥有这对密钥。即使交换的公共参数被攻击者获取,他也无法计算出密钥。另外,由于每对节点的密钥不同,当一个节点被破获后,牵涉不到其他节点的安全,更影响不到全网的安全。由此保证了网络的强健壮性。

结束语 本文在前人工作的基础上提出了一种简单有效的选择转发攻击检测方案。通过引入基于超奇异椭圆曲线的IBE算法,并采用无线传感器经典路由协议LEACH中的随机点选取机制,使得网络的安全性得到了很大的提升,理论证明及仿真结果表明我们的方案是可行的。

在未来的工作中,将对本文提出的方案进行更深入的复杂性研究,考虑将累积确认机制(cumulative acknowledge)引入到现有方案,从而解决节点间需要时间同步的问题;与此同时,考虑改进算法,仅利用邻居节点的信息来检测,以达到节省节点能量消耗的目的,从理论和应用角度,得到更优越的结果。

参考文献

[1] 李建中,高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展,2008,45(1):1-15

[2] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures [C]// Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications. 2003:113-127

[3] Yu B, Xiao B. Detecting selective forwarding attacks in wireless sensor networks [C] // Proceedings of the 2nd International Workshop on Security in Systems and Networks (IPDPS2006 Workshop). Greece, 2006

[4] Shamir A. Identity-based cryptography and signature schemes [C]// Advances in Cryptology - CRYPTO'84, Lecture Notes in Computer Science. 1985,196:47-53

[5] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks [C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. 2000

[6] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C] // Proceedings of Crypto 2001, Lecture Notes in Computer Science. 2001,2139:213-229

[7] Bulusu N, Heidemann J, Estrin D. GPS-less low-cost outdoor localization for very small devices[J]. IEEE Personal Communications, 2000,7(5):28-34

[8] Perrig A, Szewczyk R, Tygar J D, et al. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002,8(5): 521-534

[9] Wander A S, Gura N, Eberle H, et al. Energy analysis of public-key cryptography for wireless sensor networks [C] // Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications. 2005:324-328

[10] 杨庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报,2007,35(1):180-184

[11] 程宏兵,费国臻. 基于身份的无线传感器网络密钥系统[J]. 计算机科学,2007,34(10):116-119

(上接第48页)

[5] 赵冬梅,苏红顺,吴敬. 基于熵理论的无线网络安全模糊风险评估[J]. 计算机应用与软件,2006(8):24-26

[6] 陈鑫,王晓晗,黄河. 基于威胁分析的多属性信息安全风险评估办法研究[J]. 计算机工程与设计,2009,30(1):38-40

[7] 冯瑞,冯步云. 熵[M]. 北京:北京科学出版社,1992

[8] Kapur J N, Kesavan H K. Entropy Optimization Principle with Application[M]. San Diego: Academic Press, 1992

[9] ISO/IES TR 17799[R]. Information Security Management-Code of Practice for Information Security Management. 2000

[10] Risk Management Guide (DRAFT) [S]. National Institute of Standards and Technology. Special Publications 800-30. June 2001

[11] John M G. Fuzzy set computational Processes in risk analysis [J]. IEEE Transactions on Engineering Management, 1991, 38 (2):177-178

[12] Chiclana F, Herrera F, Herrear-Viedma. Integrating Three Representation Models in Fuzzy Multipurpose Decision Making Based on Fuzzy Preference Relations[J]. Fuzzy Sets and Systems, 1998,97:33-48

[13] Feng S, Xu L D. Decision Support for Fuzzy Comprehensive Evaluation of Urban Development[J]. Fuzzy Sets and Systems, 1999,105(1):1-12

[14] Masrhall D A. Coming to Acceptance of ways for Measuring and Ranking Security Properties[C]// First Workshop on Information Security System Rating and Ranking (ACSA). Williamsburg, Virginia, May 2001

[15] Dey P K. Decision Support System for Risk Management: a case study[J]. Management Decision, 2001,39(8):634-649