无线传感器网络的安全节能路由协议①

A Secure and Energy Efficient Routing Protocol in Wireless Sensor Networks

李剑萍 徐晓明 （浙江省衢州职业技术学院 现代教育技术中心 浙江 衢州 324000）

摘 要: 本文提出了一种新的传感器网络安全节能路由协议,称之为 SEG。该协议基于梯度路由协议设计。由于传感器终端的资源限制，本协议使用了有效单向散列功能。分析表明安全协议能有效应对强劲的网络攻击或应对受损节点。

关键词: 路由协议 安全通信 无线传感器网络 单向散列功能 资源限制

1 引言

集成电路和 MEMS 的高速发展使得传感器、通信信号处理芯片集成在一块板上。这加快了无线传感器网络(WSN)的开发。无线传感器网络的应用正在增加,范围从室内环境布置到室外的军事和嵌入式环境布置。

无线传感器网络的应用中,因为我们的决定取决于来自散布的各个传感器节点的数据,所以安全性是关键,因此必须获得有安全保证的路由协议。我们称之为 SEG 的协议,能有效地打击各类攻击者在任何节点制造错误通信信息,甚至攻击者和受损节点就在网络中。

同时,由于这种传感器必须防止闯入者阻挠数据的传输或者防止他们输入伪造数据,因而安全 WSN 的设计和实施有一定的难度。SEG 的设计部分基于梯度路由协议[4]。考虑到传感器节点资源有限,并要防范 DOS 攻击,攻击者企图使其他节点过量占用网络带宽或处理时间,我们在协议中使用高效单向散列功能,而不使用不对称编码操作。

本文第二节讨论传感器网络的安全通信。第三节简单介绍梯度路由协议,并估计梯度路由协议遭受攻击的可能性。第四节提出有关网络和节点的假设。第五节对 SEG 作详细的描述。第六节提出议定的安全分析。第七节,总结和展望。

2 相关工作

传感器网络中安全路由是一个关键性的问题。无线传感器网络的最新进展,引起了许多特定协议的设计。这些协议中,能量是很重要的考虑因素。在文章[2]中,Kemal Akkaya 等人调查了大量路由协议后将它们分为三类:中央数据,层次性数据,基于位置的数据。然而,路由协议的设计很少以安全为目标。在文章[1]中,为保证无线传感器网络的通信并总结针对传感器网络的攻击,作者首次提出安全路由威胁模型和安全目标,提出了对传感器网络各主要路由协议详细的安全分析,并讨论传感器网络安全路由协议的对策和设计。但他们没有提出任何特定路由协议的完整的方案。

其他研究人员在专门的移动 ad hoc 网络的安全路由中结合了入侵检测技术。无线 ad hoc 网络的本质使得它们很容易遭受被动或主动攻击。因此,我们不能保证线路的自由通信,恶意终端不会遵从受聘协议,还会试图干涉网络的运行。受损节点,尤其是那些遇到通信瓶颈的节点的出现,限制了安全路由协议的效力。如何检测受损节点和减轻路由的不正常是另一个热点问题[5-7]。

Ad hoc 网络中的安全问题跟传感器网络中的安全问题相类似,但是为 ad hoc 网络而开发的防御机制不能直接适用于传感器网络。一些为了认证和保护安全路由协议的 ad hoc 网络机制是以公钥加密为基础

① 基金项目:浙江工业大学重中之重学科开放基金:基于 STEP 和 WEB 的产品数据共享与可视化技术研究

的,如 SAODV 路由、ARAN,等等。对传感器节点来说,公共密匙成本太高,因为传感器网络的安全协议必须完全依靠高效对称密匙。基于对称密匙的安全路由协议的 ad hoc 网络已经被提出,如 SEAD, Ariadne,SRP。这些协议是基于距离矢量协议或源路由,不适合传感器网络。在节点状态和信息包开销方面,它们太贵了,并且设计出来是为了寻找和建立任何两个节点之间的路由。

在文章[8]中,A. Perrig 等人提出了一套最优化的传感器网络安全协议:SPINS。SPINS 有两个安全模块:SNEP 和 μTESLA。Ganesan 等人为传感器网络提出了冗余的"多路径"路由,以便提供可靠的容错功能和发布可靠数据。节点到节点可以有多重路径。我们研究了两种多路径:脱节路径和编织路径[9]。

在文章[10]中,Y. C. Hu 等人提出了四个保护路由协议路径向量和距离向量的新机制。在文章[11]中,J. Deng 等人提出了一种称为 INSENS 的新的传感器网络安全路由协议:无线传感器网络容忍入侵路由,它减少传感器节点的计算、通信、存储、带宽要求的同时却增加了接收发送器的计算、通信、存储、带宽要求。文章[12,13]中提供了在 WSNs 中处理信息的安全支持。由于能量限制,在数据发送之前先进行内网处理非常重要。这些机制对路由协议都具有重大作用。

3 梯度基础的协议和攻击

Schurger 等人[4]提出了梯度路由(GBR)协议,一种定向扩散协议的改进。

定向扩散是一种基于路由协议的查询。本协议的两个新词是兴趣和梯度。兴趣定义为一对属性-值,梯度以数据率、持续时间、溢出时间为特征。定向扩散可分为四个阶段。在第一阶段,将兴趣通过相邻的接受器广播到整个网络。每个节点接收并再创造兴趣,然后保存在缓存中。兴趣入口包含几个梯度场,指明数据率和数据传送方向。第二阶段是数据低速传输和路由设置阶段。探测目标或接收低速传输数据的传感器节点寻找与之相匹配的兴趣入口,当它找到后,节点低速广播数据。这样,数据沿着兴趣低速传输的反方向返回接收发送器。在第三阶段,接收发送器从多路低速通道中选择一条特殊通道。接收发送器通过选择的特殊通道用更短的间隙重新发送原始兴趣信息,强化了这条通道的源节点使之能更频繁发送数据。最后是资料传送阶段。数据沿着增强通道从源头传输到接收发送器。图 1 是从文章[3]中得来的,它概括了定向扩散协议。

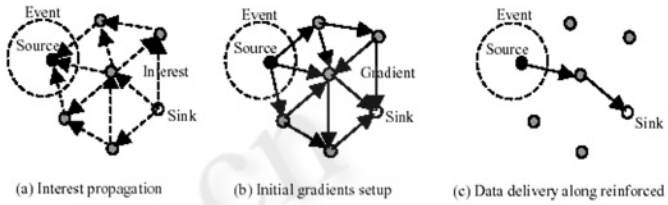

图 1　定向扩散协议

梯度路由(GBR)类似于定向扩散。GBR 的思想是当兴趣通过网络扩散时保持跳数。因此,每个节点都能发现接收发送器的最小跳数,称为节点高度。接收发送器相邻两节点的高度差称为梯度。当数据传送时,信息包跟最大梯度一起前进。在文章[4]中,Schurger 等人为了平衡网络中均一的通信,提出了一些辅助技术,如数据集合,与 GBR 一起进行数据传播,从而延长网络寿命。

然而,他们却没注意协议的安全性,这使得 GBR 饱受攻击。既然路由更新没有认证,从攻击者接收到一个从合法接收发送器发出的兴趣溢出后,攻击者可以简单重放它自己列出的兴趣。所有满足兴趣的事件都将会被同时送到非法入侵者和合法的接收发送器中。

既然高度没有校验,每个节点可以虚假地发布零高度或小高度。所以相邻节点将会传送数据给对手,因为接收发送器有最大梯度。当节点收到比以前认为的最低高度更低的假的高度时,上述的攻击可能会造成混乱。但如果有两个或更多的网络节点勾结,它能够引发上述攻击而不造成任何混乱。有一对攻击节点 A 和 B 通过私人网络相连,A 远离接收发送器而 B 靠近接收发送器。在这种情况下,A 比 B 更具有攻击性,然后将大部分的数据传送给 A 节点。A 可以结合其他攻击,如丢弃信息包,修改数据,以达到攻击目的。

攻击者能轻易发动 DOS 类型的攻击,因为每一节点都能向外网播放信息。称为接收发送器的攻击性节点可以向整个网络广播兴趣。其它正常节点将会转播兴趣。如果攻击者经常广播兴趣,其他节点的能量将

被耗尽,因此网络寿命会缩短很多。

4 假想

一般来说,传感器网络可能部署在敌对的环境。因为单独的传感器资源有限,所以它容易受损,因而这些节点并不可靠。在另一方面,由于接收发送器是节点与外界沟通的网关,它的受损将损害整个传感器网络。因此接收发送器是我们作可靠处理的基本组成部分。我们信任的部分起反应后,所有的传感器节点也信任接收发送器。在创造时间里,每个节点都会得到只与接收发送器共享的预部署共享键。

我们假设所有的无线网络都是双向的,因为这对梯度路由协议来说是必要的。具体来说,A 节点可以发送信息到 B 节点,那么 B 发出的信息也能到达 A。无线连接通常是双向的,许多 MAC 层也需要双向通信以避免冲突。

我们还假设 WSNs 的网络大小有限。网络规模定义为节点和接收发送器的最大距离。当节点发送数据给接收发送器时,节点和接收发送器的距离是所需的最小跳。我们假定网络规模小于 1 米,那么就是说,一个节点可以传输的数据不到 1 米跳。

我们还假设 WSNs 中的节点资源严格受限。因此在我们的协议中,我们使用有效单向散列链,而不是依赖昂贵的不对称密码操作。单向散列链建立在一个单向散列功能上。就像一般散列函数(functions),单向散列函数,H, 描绘的是任意长度至固定长度的位串的输入数据。因此,$H:\{0,1\}^{*}\rightarrow\{0,1\}^{\rho}$,ρ 是散列函数输出的比特长度。函数 H 应可以简单处理,一般不可行颠倒处理。一系列函数已经被提出,包括 MD5 的和 SHA-1.

在本协议中,为了防止大量 DOS 类型的攻击,个人节点不得对整个网络广播。只允许接收发送器节点广播。为创造单向散列链,接收发送器节点随机选择 $X\in(0,1)$ 初始值和计算以下的值:

$h_n, h_{n-1}, h_{n-2}, h_{n-3}, \ldots, h_0$

$h_n = x, h_i = H(h_{i+1}), 0 \leqslant i < n$. 初始化的节点产生以上所示的散列链的基本元素,从“左向右”(为减少下标 i)。假定所有节点知道单向散列函数 H 和 h_0(它可通过预置 h_0 或用 SNEP 实现节点和接收发送器之间的通信来执行),那么当一个节点收到 h_i,它可以利用 $H^i(h_i) = h_0$ 这个等式来验证 h_i 是否是链的一部分。为简化下文描述,我们假定 n 能被 m 整除。

5 协议描述

5.1 设计原理

不同于查询驱动的梯度路由协议,REG 是一个事件驱动路由协议。本协议中,当节点发现一事件,它会传送一个信息包给接收发送器。靠近接收发送器的节点必须实现性能检测和数据传输。节点越接近接收发送器,数据转播得越多。这意味着将耗费更多的能量。所以为了延长 WSN 的寿命,节点要尽量密集在接收发送器附近。我们基于以下原则设计 REG:第一,防止大量 DOS 类型的攻击。个人节点不得广播给整个网络,只允许接收发送器广播。其次,针对资源限制,保证接收发送器和节点的安全性和认证,我们采用了对称密匙。第三,针对受损节点,建造了两条通道实现安全路由。第四,针对拓扑变化,采用序列号来更新路由信息。

第一条原则是为了防止 DOS 攻击。由于传感器网络节点受资源制约,更容易受 DOS 攻击。在本协议中,接收发送器通过单向散列链实现认证,个人节点不能欺骗接收发送器从而影响整个网络.

第二条原则是关于安全网络的资源限制问题。因为节点的 CPU、存储器、带宽和能量等资源有限,我们不能使用公共加密技术。在其他方面,如果没有采取足够的警戒,入侵者可以提供虚假更新信息。另外,入侵者可以多次发出相同的路由更新信息或发送虚假信息来发动 DOS 攻击。REG 利用单向认证机制鉴别接收发送器发来的更新信息。

第三条原则是关于袭击者的问题。在敌对环境,节点受损是不可避免的。入侵侦测系统(IDS)虽然可以用来侦测恶意节点,但实行起来非常困难,而且要消耗时间和能量。入侵检测所需的常规用法和传播方式等重要参数在 WSNs 中通常事先并不知道。胜于 IDS,REG 采用两种以上的通信路径容忍入侵者。每个数据包被多次从源头送往目的地,每一次都沿重复路线。一名或多名入侵者沿着其中的一些路径只能危害一些副本的传输。不过,只要有至少一条路径不受侵扰,接收发送器将最终获得正确数据。接收发送器可使用 MAC(消息认证码)以确定是否已接获的信息是原件

或已被篡改。

第四原则是关于拓扑变化的问题。传感器网络的拓扑关系经常变化。由于网络节点会随时移动,也可能因为故障或电力耗尽而消失,或者可能配置新的传感器网络节点,所以路由协议还必须能够应对这些变化,学习新的路由信息来保持连通。序列号就是用于这一目的的。我们接下来将详细介绍序列号。

REG 分为路由更新和数据传输两个阶段,以下将详细说明。

5.2 路由更新

路由更新的目的是初始化梯度和搜集相关信息。当网络刚刚建立,或当网络节点可能因转移或能源消耗而改变时,接收发送器会广播一个被相邻节点接收的路由更新信息。下面会给出更新信息的详细格式。每个节点会保持当前的序列号,最小跳和相邻节点的设置(neighbor nodes set)。一个节点收到更新信息后会先核实是否来自接收发送器并鉴别序列号和跳。如果节点是首次接收信息,或序数号大于或等于当前值,或跳小于最小跳,它将更新当前序列号,最小跳和相邻节点的设置,并重播信息 否则,它只更新相邻节点的设置。

a)　路由更新信息格式

能量信息	序列号	跳	散列值

b)　相邻节点接受机(set)入口

节点 ID	能量信息	序列号	跳

图 2　路由更新信息格式和相邻节点设置入口

图 2(a)为路由更新信息的格式。能量信息领域显示发送器的残余能量,它在数据传输阶段是很有用的。序列号是一种时间标记。接收发送器节点保持一个当前的序列号。当网络节点因转移或能源消耗而彻底改变时,接收发送器会随着序列号的增加而广播路由更新信息。跳是接收发送器和发送器之间的距离。第四部分描述过的散列值用来鉴别发送器和校验序列号和跳。图 2(b) 为相邻节点接受机入口的格式。相邻节点接受机记录了其他节点的信息,包括节点的 ID,能量信息,当前序列号及最小跳。

正如第 4 部分所述,我们假定网络规模小于 1 米,因此节点的最小跳也小于米,散列链分割成 n/m 个部分,如下:

序列号 = n/m : h_n, h_{n-1}, …… h_{n-m+1}……

序列号 = k : h_{km}, h_{km-1}, …… h_{km-m+1}……

序列号 = 1 : h_m, h_{m-1}, …… h_1h_0

假定序列号 = k、跳 = j,它具有对应的单一的散列值,即 h_{km-j}。所以我们可以利用散列值验证序列号及跳。

刚开始,所有节点的当前序列号重置为 0,最小跳为米,相邻节点接受机为空。需要时,接收发送器广播更新信息。如果接收发送器目前的序列号是 k -1,它将发出最新信息(能量信息、k、0、h_{km}),然后调整序列号为 k。当节点收到更新信息(能量信息、k、j、h_{km-j}),它首先检验是否 H^{km-j}(h_{km-j})等不等于 h_0,如果它们相等,我们会将序列号、跳与当前的序列号、最小跳作比较。如果序列号小于当前值,那这就是一个过时的信息,就丢弃它。如果序号大于当前值,它会更新当前的序列号为 k,最小跳为 j +1。此外,它还会清空相邻节点的接受机,并添加新的入口(发送器身分,发送器能量信息,k, j +1),并重播信息(能量信息、k、j +1、H(h_{km-j})),这里的能量信息是指节点的能量信息。如果当前的序列号是 k,最小跳小于等于 j +1,它只会更新相邻节点接受机。如果相邻接收机没有入口,它会新开一个入口(发送器身份、发送器能量信息、k、j + 1)。如果已经有入口了,那只有当入口跳大于 j +1 时才需要更新更新相邻接受器。

由于单向散列链的性质,利用对应于序列号和跳的散列值可以防止任何节点宣告一个更大的序列号。因为只有接收发送器熟悉整个散列链,所以只有接收发送器才能与更大的序列号一起广播更新信息。同样,没有节点可以广播一个比收到的跳数小的跳数,因为跳不能减少。

5.3 数据前进

利用数据更新阶段收集的信息,数据可很容易的从源头转发到接收发送器。更新的路由信息广播至整个网络后,每一个节点都会有以下的信息 :当前序列号,最小跳,相邻节点设置。每一个节点都知道相邻节点的能量信息和相邻节点与接收发送器的距离。依靠这些信息和适度的局部化运算法则(既要考虑相邻节点的距离及其残余能量),每个节点都能决定哪些是最

好的相邻路由器(转接数据包的中间节点),哪些是次好的相邻路由器。

下个相邻路由器	资源	数据	MAC(资源|数据,键)

图 3 数据包格式

图 3 为数据包格式的资料。下个相邻路由器是中间转接节点 ID。资源领域包括资源节点 ID。键是接收发送器和节点共享的唯一的键。当节点需要发送数据给接收发送器时,它发出的数据包给最好的相邻路由器和次好的相邻路由器。节点必须确定是否是首次接受数据包。如果是,它将选择最佳的相邻路由器作为下一个转接节点。如果不是,则选择次佳的。

在这一阶段,采用两种机制反击攻击。第一,加密的 MAC 运算法则被用来阻止恶意节点修改数据包。每个节点独立配置一个只与接收发送器共享的密匙。节点的密匙用来生成以下的方面:MAC(资源|数据,键)"|"表示相连。数据包包含 MAC 域,如图 3。它用来检查数据包的完整性。第二,采用了多路路由增加数据传输的可靠性。本协议中,两份资料的副本沿不同途径发送,以使恶意节点复原。

6 安全分析

SEG 的耗能相对较小。为了保持当前序列号,最小跳,相邻节点设置,接收发送器需要定期广播更新信息。如果不频繁改变网络拓扑关系,我们可以长时间间隔地广播更新信息。所以通信成本并不高。与此同时,每个节点需要存储的所有资料包括当前序列号,跳和相邻节点设置,所以存储成本也有限。在 SEG,我们使用对称密匙,因此计算成本也不大。

既然只有接收发送器熟悉整个单向散列链,恶意节点不能冒充接收发送器广播更新信息。在 SEG,假设有一个序列号为 k 和跳为 j 的更新消息,恶意节点能伴随序列号 k 让跳大于等于 j 时产生更新信息路由,或小于序列号 k 的任意长度产生更新信息路由。也就是说,恶意节点不能在序列号大于等于 k 或跳小于 j 时产生更新信息。恶意节点可以和跳 j 产生更新信息,因为它只需简单地重发一次它已收到的单向散列链元素。合法节点可以和跳 j+1 广播更新信息并依靠散列接收到的散列值生成认证。因为序列号和单向散列链的概念,没有节点可以发起相同的攻击和 DOS 类型的攻击。如果节点收到更新信息时的序列号小于当前序列号时,就会丢弃信息。

SEG 并不检测入侵,而是绕过恶意入侵节点容忍入侵。本协议中是用多路径来对付受损节点。由于敌对的环境和资源及成本的限制,节点受损是必然的。即使在一个节点路径受损,数据仍可以通过其他路径传输到接收发送器。此外,本协议中的 MAC 算法用来防止恶意节点修改数据包。在发送数据之前,发送器产生 MAC(发送器|数据,键),发送器是指发送器的 ID,键是只与接收发送器共享的重新装配的键。因而,接收发送器可以检查数据包的完整性。

7 总结和展望

在本文中,我们制定了一项新的无线传感器网络安全路由协议,称为 SEG。它分为两个阶段,路由更新阶段和数据传输阶段。在第一阶段,用单向散列链来鉴别序列号和跳。第二阶段,用两个机制(加密的 MAC 运算法则和多路路由)来对付入侵者。加密的 MAC 运算法则是用来防止数据被篡改,冗余的多路路由通过绕开恶意节点防止入侵。不管在网络中有强劲的攻击者还是有受损节点,分析显示本安全协议能应对强劲的多重攻击。

在今后的工作中,我们计划考虑开发能检查不传送数据包节点的机制,并让 SEG 与查询驱动路由协议相结合。另外,有些基于 NS2 的仿真将用来分析协议的成本和承受恶意攻击的能力。

参考文献

1 C. Karlof, D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

2 Kemal Akkaya, Mohamed Younis. A Survey on Routing Protocols for Wireless Sensor Networks.

3 C. Intanagonwiwat, R. Govindan, D. Estrin. Directed diffusion: A scalable and robust communication paradigm for sensor networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile

Computing and Networking (MobiCom'00), Boston, MA, August 2000.

4 C. Schurgers, M. B. Srivastava. Energy efficient routing in wireless sensor networks. MILCOM Proceedings on Communications for Network - Centric Operations: Creating the Information Force, McLean, VA, 2001.

5 Wensheng Zhang, R. Rao, Guohong Cao, George Kesidis. Secure routing in ad hoc networks and a related intrusion detection problem. Department of Computer Science & Engineering The Pennsylvania State University.

6 Yongguang Zhang, Wenke Lee. Intrusion detection in wireless ad - hoc networks. Mobile Computing and Networking, 2000. 275 - 283.

7 Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker. Mitigating Routing Misbehavior in Mobile Ad hoc Networks. Mobile Computing and Networking, 2000: 255 - 265.

8 A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks. Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.

9 D. Ganesan, R. Govindan, S. Shenker, D. Estrin. Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks. Mobile Computing and Communication Review (MC2R), 2002,1(2).

10 Y. C. Hu, A. Perrig, D. B. Johnson. Efficient security mechanisms for routing protocols. Proc. of the Tenth Annual Network and Distributed System Security Symposium, NDSS' 03, San Diego, CA, February 2003.

11 J. Deng, R. Han, S. Mishra. INSENS: Intrusion - Tolerant Routing in Wireless Sensor Networks. In the 23rd IEEE International Conference on Distributed Computing Systems (ICDCS 2003), Providence, RI, May 2003.

12 B. Przydatek, D. Song, A. Perrig. SIA: secure information aggregation in sensor network. ACM sensys' 03, Los Angeles, CA, Nov, 2003.

13 Jing Deng, Richard Han, Shivakant Mishra. Security Support For In - Network Processing in Wireless Sensor Networks. First ACM Workshop on the Security of Ad Hoc and Sensor Networks (SASN) 2003.