广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(3):164～166
Vol. 22,No. 3 August 2006

基于低能耗无线驱动装置和无线传感器网络安全性的管理方案

Management Project on Security for Wireless Actuator and Wireless Sensor Networks Based on Low Energy Consumed

归奕红,黄 力
GUI Yi-hong,HUANG Li

(柳州职业技术学院,广西柳州 545006)
(Liuzhou Vocational and Technical College,Liuzhou,Guangxi,545006,China)

摘要:针对无线驱动装置和传感器网络(WASNs)特殊的网络约束和数据传输要求,提出一种两层密钥更新/路由更新和多密钥管理方案,该方案具有可靠的安全性,可以抵御来自移动传感器网络的主动攻击;通过采用OPNET8.0进行网络仿真,证明该方案具备良好的节能性。

关键词:WASNs 本地安全 驱动装置 传感器 密钥 仿真
中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2006)03-0164-03

Abstract:Based on the special network constraint and data transmission requirements of Wireless Actuator and Wireless Sensor Networks, a scheme of two-level re-keying/re-routing and multiple-key management was presented. This scheme can protect from active attacks in mobile sensor network. In the simulation based on OPNET 8.0, the schemes has good security and efficiency.

Key words:WASNs,local security,actuator,sensor,key,simulation

无线驱动装置和传感器网络(WASNs)是在无线传感器网络(WSNs)基础上发展起来的一种带驱动装置的传感器网络,它能发现并对入侵和攻击作出反应,实现了一个由游离的计算(通过无线传感器网络协议)和巧妙的空间(通过传感器和驱动装置的调配)组成的体系结构[1]。WASNs相比较WSNs有一些独特的性质,如实时感测并采取行动、既是传感器又是执行者、驱动装置还具有变动性等[2],WASNs一般由大规模低能量微型传感器和少量随机分散在传感器中的资源丰富的驱动装置组成。为了实时控制[3],传感器一般向附近的驱动装置而不是遥远的接收端发送数据,WASNs主要关注传感器到传感器之间的相互连接。在WASNs中,有四种类型的调配需要考虑:驱动装置到驱动装置(A－A)、传感器到传感器(S－S)、驱动装置到传感器(A－S)(下行线路)和传感器到驱动装置(S－A)(上行线路)。与微型传感器相比,驱动装置通常有较高的能量、较大的存储空间和较强的计算能力,能完成较复杂的工作[1]。

在WASNs中存在许多有待解决的问题,如节能、安全性、实时A－S/S－A路由、A－A动态管理等等。针对无线驱动装置和传感器网络(WASNs)特殊的网络约束和数据传输安全性要求,本文提出一种两层密钥更新/路由更新和多密钥管理方案,旨在能量有效的前提下解决WASNs的安全问题,抵御网络中的各种攻击,如侦听和入侵,确保数据能在带驱动装置的传感器网络中安全地传送。

收稿日期:2006-03-06
修回日期:2006-07-28
作者简介:归奕红(1969-),女,广西钦州市人,讲师,主要从事计算机网络及信息安全研究。

1 两层密钥更新/路由更新和多密钥管理方案

1.1 密钥更新/路由更新方案

作为安全的重要条件,安全密钥管理需要一个低能量路由协议,设计一个分层的、高效能并适合WASNs特殊性的路由方案是非常重要的。面向安全的路由设计我们考虑以下方面:(1)适合独特的WASNs拓扑特征,利用少数资源丰富的驱动装置完成最多的计算机安全任务,使得多数资源受限的传感器完成较轻的任务;(2)实现路由开销条件下的能量有效;(3)有利于安全实行。

我们将使用"波密钥"完成异步广播证明,并提出用一个基于波-区(Ripple-Zone,简称RZ)的运算法则去组织传感器到不同的波中。

基于RZ的WASNs路由方案如下:设计一个可扩展的能量有效的路由方案,建立一个成员认可协议(Member Recognition Protocol,简称MRP),允许驱动装置和传感器自组织成分开的"域",每一个驱动装置作为域的中心,其周围形成一个RZ。运行了MRP之后,每一个驱动装置将知道它域中的成员,传感器基于它们与驱动装置之间的距离和一定数量的跳数被分配到不同的波。为了减少数据冗余,我们选择一些传感器作为"主人",每一个"主人"从它区内的传感器中聚合数据,然后使用多跳通信(即:波-波)向邻近波的"主人"转发,最后到达驱动装置,即用一个较小的跳数到达驱动装置,基于RZ的路由如图1所示。

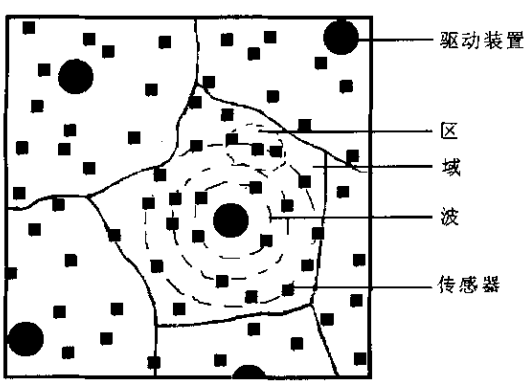

图1 基于波-区的路由

1.2 密钥方案

WASNs路由协议自组织整个网络分成两层:(1)高层驱动装置;(2)属于某一个驱动装置的域并自组织到一个波结构的低层传感器。本文讨论安全协议用于高层节点的情况,即若干驱动装置和一个接收端。一个接收端可以执行所有主要的传感器网络任务,如向每一个驱动装置/传感器分配密钥和收集来自传感器的感测数据,在高层体系结构中,存在两种类型的密钥:(1)会话密钥(Session-Key,简称SK),用于数据包的加密;(2)主密钥(Backbone Key,简称BK),用于包的安全管理,包括SK更新的密钥信息。SK需要定期地更新以抵御主动的攻击,然而BK要通过一个触发事件才能激活,典型的事件包括新驱动装置的插入、节点的删除或节点受到破坏等。接收端能使用任意已知的群组广播协议[4]去更新BK。

在WASNs安全方面,共享密钥方案的选择应该考虑网络内部处理的影响,例如对冗长的感测数据进行数据聚合对于减轻通信开销是必要的。如果一个节点只是接受一种类型的密钥,也就是仅仅在两个节点之间共享的成对密钥,内存的限制将阻止一个来自维护所有需要从它的成员节点中聚合数据的密钥的集合。在每一个传感器和接收端之间简单地构筑一个端到端的安全通道是失策的,因为中间的传感器/驱动装置需要解密和证明从各种传感器收集到的数据。在传感器节点中交换不同类型的消息有不同的安全要求,单一的密钥结构不可能适合所有情况,因此,在低层传感器中需要引入多种密钥。此外,还需要一种密钥,它能把由区和波组成的路由体系结构与密钥管理结合起来。

为适应不同安全目的,我们设置多种类型的密钥如下:(1)主人-驱动装置密钥(MAK):一个MAK在每一个主人和它的域驱动装置之间共享,它用于直接的主人-驱动装置安全通信,MAK基于SK产生;(2)中间-主人成对密钥(MPK):偶尔安全通道必须在两个属于不同驱动装置的域的"主人"之间确立;(3)传感器-主人成对密钥(SPK):一个SPK在一个主人和它区中的每一个传感器之间共享;(4)区密钥(ZK):ZK用于数据聚合,也用于向整个区广播一条询问信息,每一个ZK被同一个区中的所有节点共享;(5)波密钥(RK):一个RK用于一个驱动装置域内的广播证明。RK由驱动装置决定,驱动装置通过控制为包加密向不同的波发送不同的RK,一个驱动装置将发出一条需要被多次证明的广播消息,每一次驱动装置用一个不同的RK加密消息,因此,只有这个波中的主人能对它解密。

安全实行。流密码RC4用于加密/解密运算,因为这种流密码相比较块密码来说有一个较低复杂度的可靠运算,为了解决流密钥重用问题,发送者把自己的sensor-ID放入产生的密钥中,每发送一条消

息，发送者将为发送包的初始向量（IV）递增计数值，因此确保了密钥的唯一性。具体加密过程如图2所示。伪随机函数（PRF）$\{f\}$ 被用作产生新的密钥，该密钥基于当前会话密钥 SK_{now} 和随机数 x 产生：$KEY_{new} = f(SK_{now}, x)$。

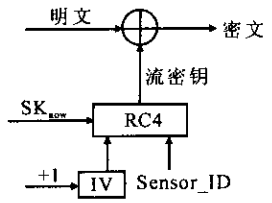

图2 加密过程

2 性能分析

系统仿真采用 OPNET8.0，根据文献[5,6]中提出的仿真方法，给定网络150个节点，分成5个子网，网络覆盖面积 300 m×300 m，子网重组间隔周期为20 s。各节点起始能量相同，考虑到节点移动带来的影响，在网络中取30个节点以 10 m/min 的速度在网络区域内沿水平方向往复移动。图3给出了常规方案和基于RZ方案的仿真结果，该结果表明，基于RZ的方案由于使用波-波中继，具有较低的能量开销，是一种节能的方案。

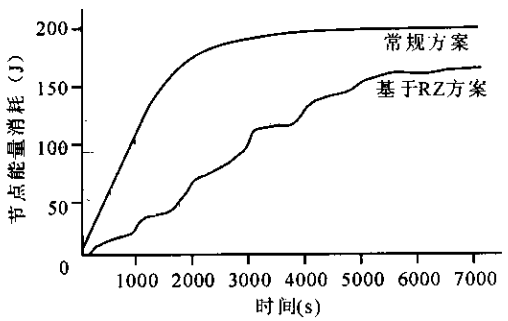

图3 网络节点能量时域

3 结束语

本文提出的一种两层密钥更新/路由更新和多密钥管理方案，该方案可以将 WASNs 安全性与一个可扩展的能量有效的路由体系结构无缝结合，可以防御来自移动传感器网络的主动攻击，两层更新的密钥/更新的路由方案不仅能适应动态的网络拓扑，还能安全地为每一个会话数据传输更新密钥，大大提高网络处理数据的安全性，仿真分析也显示，该方案是一种有效的节能方案。

参考文献：

[1] JAMES F KUROSE, KEITH W ROSS. Computer networking, a top-down approach featuring the Internet [M]. California: Addison-wesley Publishing, 2003: 74-75.

[2] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. A Survey on sensor networks [J], IEEE Communications Magazine, 2002, 40(8): 102-114.

[3] STANKOVIC J A, ABDELZAHER T F, LU C Y, et al. Real-time communication and coordination in embedded sensor networks[J]. Proceeding of the IEEE, 2003, 91: 1002-1022.

[4] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks: proceedings of the IEEE Computer Society Symposium on Security and Privacy[C]. Piscataway, USA: IEEE, 2003: 197-213.

[5] 陈敏. OPNET 网络仿真[M]. 北京：清华大学出版社，2004.

[6] 伍俊洪，杨洋，李惠杰，等. 网络仿真方法和 OPNET 仿真技术[J]. 计算机工程，2004(3): 106-108.

（责任编辑：韦廷宗）

日本研制出月球探测车样车

日本宇宙航空研究开发机构最近研制出了月球探测车样车，可爬20度的斜坡，并能在沙地上畅行无阻。

月球表面布满了因天体碰撞和自然演化而留下的凹坑和岩石，表层土壤则由于含有大量细沙相对松软，当年美国“阿波罗计划”中使用的探测车就曾出现过陷车和爬坡困难等问题。为解决这些问题，日本新研制出的样车使用了4条密封履带，每条履带包裹5只车轮。在类似月球表面的沙地上进行的测试表明，这辆 70 cm 长、60 cm 宽、40 cm 高的样车每秒可行驶几厘米，爬20度的斜坡不会滑落。利用履带间的速度差，可改变其行驶方向。

据《科学网》