无线传感器网络中的一种安全高效的路由协议

李少衡　张　琨　王翠荣
(东北大学秦皇岛分校, 河北 秦皇岛　066004)

摘　要: 针对无线传感器网络中部分路由协议在设计时对安全性考虑不够的问题,本文提出一种安全高效的路由协议 - STEEN 协议。该协议是在 TEEN(Threshold sensitive Energy Efficient sensor Network protocol)路由协议的基础上,以增强路由安全性同时兼顾网络的能量消耗为目标而设计的。该协议通过预置密钥和采用随机密钥对密钥管理的方法,解决了节点间的认证和安全通信的问题,增强了网络的安全性。通过安全性分析可以看到,该安全路由协议可防御多种针对网络层的攻击。

关键词: 无线传感器网络; 路由协议; 安全; 密钥管理
中图分类号: TP391

引　言

无线传感器网络是由部署在监测区域内大量的微型传感器节点组成,通过无线通信方式形成的一个多跳的自组织的网络系统。无线传感器网络应用十分广泛,包括军事监测、医疗护理、城市管理和空间探索等诸多方面,它被认为是 21 世纪最具影响力的技术之一。传感器网络、塑料电子学和仿生人体器官又被称为全球未来三大高科技产业[1]。

无线传感器网络路由协议负责监控网络拓扑结构变化、交换路由信息、定位目的节点、产生、维护和选择路由,根据选择的路由转发数据等。因此,无线传感器网络设计的成功与否,其路由协议的设计非常关键。现有的无线传感器网络路由协议主要分为以下几类:能量感知路由协议,包括能量路由、能量多路径路由[2]等;基于查询的路由协议,包括定向扩散路由[3](Directed Diffusion)、谣传路由[4](Rumor routing)等;基于地理位置的路由协议,包括 GEAR[5](Geographical and Energy Aware Routing)路由、GPSR[6](Greedy Perimeter Stateless Routing)路由等;基于层次式的路由协议,包括 LEACH[7](Low Energy Adaptive Clustering Hierarchy)路由、TEEN[8](Threshold sensitive Energy Efficient sensor Network protocol)路由等。

上述无线传感器网络路由协议,针对传感器网络有限的节点资源和特定的网络应用进行了优化设计,但都没有充分考虑网络的安全问题,这使得传感器网络在实际通信中容易受到针对网络层的各种攻击。本文研究无线传感器网络的路由安全问题,通过在 TEEN 协议基础上设计安全措施,提出了一种安全路由协议-STEEN 协议,并对该协议的安全性进行了分析。

1　路由协议的安全威胁

无线传感器网络路由协议的安全性对整个传感器网络而言至关重要,如果由于路由协议的不安全导致传送的消息被篡改,那么在应用层上讨论数据包的安全性是没有任何意义的。对无线传感器网络的网络层攻击模型[9]主要有以下几种。(1)伪造路由信息。恶意节点通过欺骗、更改和重发路由信息,在网络中形成路由环,吸引或者拒绝网络信息流通量,延长或者缩短路由路径,形成虚假的错误消息、分割网络、增加端到端的时延等,从而降低网络的可靠性,缩短网络的工作寿命,并且产生大量的拥塞和冲突。(2)选择转发攻击。恶意节点收到数据包后,丢弃部分或者全部数据分组,导致数据包不能完全或者根本无法到达目的地。当恶意节点处于节点消息传送路径上时,这种攻击最为有效。(3)陷洞(Sinkholes)攻击。攻击者通过一个恶意节点吸引某一特定区域的通信流量,形成以恶意节点为中心的

收稿日期: 2007-05-23
基金项目: 河北省科技厅博士基金(55470130-3);东北大学 985 信息化平台项目
第一作者: 男,1974 年生,硕士生
E-mail: lishaoh88@163.com

“陷洞”,处于陷洞附近的攻击者就能相对容易的对数据进行篡改。(4) 女巫(Sybil) 攻击。一个恶意节点在网络中呈现多个号,那些实际上并不存在的节点称为 Sybil 节点。对于某些特殊的应用于无线传感器网络的路由协议,节点的位置信息是相当重要的,而 Sybil 攻击可以使一个节点呈现出多个位置,从而影响节点的正常路由。(5) 虫洞(Wormholes) 攻击。虫洞攻击通常是两个恶意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,这个节点声称自己和基站附近节点可以建立低时延高带宽的链路,以吸引其他节点的数据包。(6) HELLO 泛洪攻击。有足够强的信号的恶意节点可以使网络中的其它每个节点都将它当作邻居节点,其它节点会认为恶意节点是一条质量较高的传输路径而将信息发送给它,从而使网络不能正常运行。

2 安全路由算法 STEEN 协议

2.1 TEEN协议

TEEN 协议是在 LEACH 协议的基础上发展而来的,LEACH 协议是第一个提出簇的概念的层次路由协议。它的基本思想是:为平衡网络各节点的能耗,簇头节点周期性按轮随机选举,成为簇头的节点在无线信道中广播这一消息,其余节点选择加入信号最强的簇头。节点通过一跳通信将数据传送给簇头,簇头也通过一跳通信将经数据融合后的数据传送给汇聚节点。该协议采用随机选举簇头的方式避免簇头过分消耗能量,提高了网络生存时间。TEEN 协议也是一个层次路由协议,利用过滤方式来减少数据传输量。该协议采用与 LEACH 协议相同的聚簇方式,但簇头根据与汇聚节点距离的不同形成层次结构。聚簇完成后,汇聚节点通过簇头向全网节点通告两个门限值(分别称为硬门限和软门限) 来过滤数据发送。在节点第一次监测到数据超过硬门限时,节点向簇头上报数据,并将当前监测的数据保存为监测值(Sensed Value,简称 SV)。此后只有在监测到的数据比硬门限大且其与 SV 之差的绝对值不小于软门限时,节点才向簇头上报数据,并将当前监测数据保存为 SV。该协议通过利用软、硬门限进一步减少了数据传输量,且层次型簇头结构不要求节点具有大功率通信能力。

2.2 STEEN协议

TEEN 协议有很多优点,但是它在设计时并没有过多的考虑路由安全的问题,本文通过引入单向哈希函数和随机密钥对密钥管理[10] 等方法为 TEEN 协议添加安全外壳,提出了 STEEN 协议。

随机密钥对方案的基本思想是:在网络中为每个节点分配唯一的一个节点标识符(ID),每个节点在得到自己的节点标识符后,与另外 M 个随机选择的不同节点标识符匹配,并且为每对节点产生一个密钥对,存储在各自的密钥环中。然后每个节点向它的邻居节点广播自己的 ID,邻居节点在收到广 ID 播包后,在密钥环中查看是否有与这个节点共享的密钥对。如果有,则通过一次加密握手过程来进行身份认证。随机密钥对方案有较好的性能,主要表现在(1) 该方案在网络安全建立过程中,只需要广播节点的 ID,而不是很多的密钥或密钥的代号,因此节省了大量的通信能量。(2) 由于该方案中的两个节点之间有唯一的密钥对,因此方案可以提供两个节点之间的认证,而认证可以防止很多类型的路由攻击。(3) 该方案提供了很强的节点抗捕获能力,每个密钥对是唯一的,任何节点被俘都不向敌人透露除了其本身参与的直接通信以外的任何信息。

基于以上特点,本文采用随机密钥对方案为 STEEN 协议生成和管理密钥。STEEN 协议主要由以下 4 个阶段组成:

2.2.1 预配置阶段 在这个阶段,为每个节点分配一个唯一的 ID、一个初始密钥 K_0 和一个单向哈希函数 F,并为每个节点随机分配与 m 个节点的共享的密钥对。对于汇聚节点,需要装入所有节点的 ID 及整个网络的密钥池,这里假定汇聚节点有足够的能量、通信可以覆盖全网并且是物理安全的。

2.2.2 初始化阶段 在这个阶段,主要实现节点间的安全连接,并在汇聚节点与一跳节点之间建立通信密钥。

所有的传感器节点向其邻居节点广播自己的 ID,邻居节点收到 ID 后,首先和自己的密钥环进行比较,如果密钥环中有与收到的 ID 对应的密钥,则两个节点(如节点 A 和节点 B) 通过一次握手协议建立安全连接。典型的握手过程为

$A \rightarrow B :\{ ID_A \}$

$B \rightarrow A :\{ ID_B \parallel K_{AB}[\text{RequestMessage}] \}$

$A \rightarrow B :\{ K_{AB}[\text{ACK and Challenge Message}] \}$

$B \rightarrow A :\{ K_{AB}[\text{Response for the Challenge}] \}$

对于两个没有共享密钥的邻居节点,可以向汇聚节点发送请求协商建立一个共享密钥对。假设 C 和 D 是邻居节点,但它们之间没有共享密钥对,则

分别向汇聚节点发送请求信息{ReqA, K_0(ID_C|ID_D|N_{C0})}和{ReqA, K_0(ID_D|ID_C|N_{D0})},其中ReqA表示该信息是请求协商密钥信息,N_{C0}和N_{D0}分别表示由C和D产生的随机数,表明信息的强新鲜性。汇聚节点收到请求信息后,为C和D分配密钥对,并回复{ReqR, ID_C, K_0(ID_D|K_{CD})}和{ReqR, ID_D, K_0(ID_C|K_{CD})},其中ReqR表示回复请求信息,C和D用K_0解密后获得共享密钥对K_{CD},再通过前面所述的握手协议建立安全连接。

对于可以直接与汇聚节点通信的节点(称为一跳节点),它们在TEEN协议的网络拓扑结构中担任最上层簇头节点,因此十分重要。汇聚节点需要为它们单独分配密钥,当汇聚节点侦听到一跳节点的广播的ID后,产生一个通信密钥,经K_0加密后发送给一跳节点;一跳节点收到信息后用K_0解密得到与汇聚节点的通信密钥并保存。同时,汇聚节点记录下所有一跳节点的ID和其所对应的密钥。

2.2.3　簇建立阶段　首先在一跳节点之间选取簇头节点,选取的原则是:所有一跳节点中能量最多的节点;前几轮没有成为簇头节点的节点。

在上述情况相同时,则随机选取节点做为簇头节点。对于其余的一跳节点和其它能够与簇头节点直接通信的节点,根据与簇头节点的通信能量消耗的多少加入到相应的簇中。以此类推,由上向下逐层建立簇,直到所有的节点加入到相应的簇中为止。其结果如图1所示。

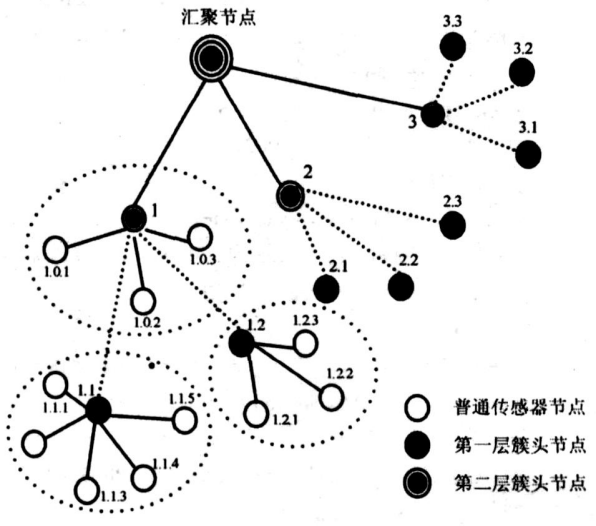

图1　簇形成过程示意图

Fig. 1　Process of cluster forming

簇建立完成后,簇头节点逐层上报簇内的组成和结构,汇聚节点据此描绘出整个网络拓扑结构。

2.2.4　数据传输阶段　TEEN协议是基于门限传输数据的,减少了数据传输量,节省了能量。但它也有缺点,主要是:如果数据达不到门限值,节点就不会传输数据,用户无法从网络中获得任何数据。另外还有一种可能就是:当网络中有重要数据传输时,新一轮簇建立周期来临,网络中所有节点重新组织,会造成大量重要数据的丢失。本文给出的一个解决方法是,每轮的发起由汇聚节点决定,当网络中有数据传输时,不发起新的一轮;当网络没有数据传输且超过一定的时限时,汇聚节点发起新的一轮,具体过程为当网络没有数据传输且超过一定时限时,汇聚节点向全网发出建立新一轮的通告{$Round_i$, ID_s, T_stamp, K_0(K_1)},其中$Round_i$代表当前轮次,ID_s代表汇聚节点T_stamp,是时间戳,K_1表示这一轮的密钥,用来检验消息的真实性。网络中的节点首先检查时间戳,如过期则直接丢弃该信息;如没有过期,则用K_0解密出K_1,计算$F(K_1)$,如果$F(K_1)=K_0$,则进行新一轮的簇建立过程,如果两者不相等,则丢弃该信息,并上报给汇聚节点。

3　安全性分析

3.1　伪造路由信息攻击

TEEN协议能够抵御这种攻击,因为TEEN协议从汇聚节点到簇头节点、簇头节点到簇内节点的每一层数据传输都是在一跳内完成,在聚簇完成后,信息沿着簇内节点→簇头节点→汇聚节点的方向传输,恶意节点伪造路由信息是毫无意义的。

3.2　选择转发攻击

TEEN协议有可能受到此类攻击,选择转发攻击经常与HELLO泛洪攻击结合使用,一个或多个恶意节点通过广播大功率信号,吸引网络中的节点的通信流量,并把这些信息全部或部分丢弃,造成网络工作的异常。如果恶意节点成为簇头节点可能会带来选择转发攻击,在STEEN协议中,簇头节点需要与簇中所有节点建立共享密钥,恶意节点需要攻陷网络中的很多节点才能达到这个目的,这需要很高的代价。

3.3　陷洞(sinkholes)攻击

TEEN协议对单纯的陷洞攻击有较强的抵抗能力,因为TEEN协议中的簇内节点只向簇头节点转发数据,且不需要经过中间节点,因此簇内节点不会形成陷洞;簇头节点采用轮换制,不会长时间的受陷

洞攻击的影响。

3.4 女巫(Sybil)攻击

TEEN 协议可能会受到女巫(Sybil)攻击。根据 TEEN 协议中簇头节点的产生机制,恶意节点可以采用 Sybil 攻击,一个恶意节点在网络中的其它节点面前具有多个不同的身份,在每一轮簇头选取过程中以不同的身份出现,同时宣布有很多的能量,以此来增加自己被选择为簇头的机会。STEEN 协议采用了随机密钥对管理方案,通过使用节点的和对应的密钥对,实现点到点的认证,对于伪造的身份无法进行认证;同时由于汇聚节点知道整个网络的拓扑结构,当一个节点出现多个身份时,很容易被汇聚节点感知到,因此 STEEN 协议能够抵抗女巫攻击。

3.5 虫洞(Wormholes)攻击

虫洞攻击是通过建立一个具有很小延迟的链路,吸引网络中的部分通信流量。前文已经提到 TEEN 协议中的信息是沿着簇内节点 →簇头节点 → 汇聚节点的方向传输的,且每层的传输都是在一跳内完成的,节点对具有很小延迟的链路并不感“兴趣”,因此,TEEN 协议能够抵御用这种攻击。

3.6 HELLO 泛洪攻击

由于在 TEEN 协议中,节点根据聚簇信号的强弱来加入相应的簇,因此恶意节点可以轻易的采用 HELLO 泛洪攻击,恶意节点以大功率进行广播,使得大量的节点都想加入到该簇中,然后恶意节点可以采用其他的攻击方法,例如选择转发,修改数据包等,来达到攻击的目的。在 STEEN 协议中,首先节点间的通信需要进行认证,如果通不过认证,则其能量再大,也不能成为网络中的节点;其次如果内部节点被攻陷,泄露的也只是与被攻陷节点有关的信息,网络的其它部分不会受到影响。

4 结束语

本文以提高网络安全性为首要设计目标,通过引入密钥管理方案和认证机制,为传感器网络路由协议 - TEEN 协议添加安全外壳,提出一种安全路由算法 - STEEN 协议。通过分析可以看出,STEEN 协议对几种主要的针对无线传感器网络路由协议的攻击方式均有一定的抵抗能力,网络安全性较高。

相对于 TEEN 协议,本文在建立安全外壳时增加了网络的能量消耗,但由于采用了随机密钥对方法,其增加能耗很小,且只在网络初始化阶段进行一次。下一步拟在理论分析的基础上,利用 NS2 仿真工具对本文方案的安全性能及网络性能进行定量分析和仿真实验。

参考文献:

[1] KERMAL A, MOHAMED Y. A survey on routing protocols for wireless sensor networks[J]. Communications Magazines, 2002, 40(8):102 - 114.

[2] SHAH R C, RABAEY J M. Energy aware routing for low energy ad hoc sensor networks[C]//Proc IEEE Wireless Communications and Networking Conference. IEEE, 2002, 1:17 - 21.

[3] INTANAGONWIWAT C, GOVINDAN R, ESTRIN D, et al. Directed diffusion for wireless sensor networking[J]. IEEE/ACM Trans on Networking, 2003, 11(1):2 - 16.

[4] BRAGINSKY D, ESTRIN D. Rumor routing algorithm for sensor networks[C]//Proc of the 1st workshop on sensor networks and applications. Atlanta: ACM Press, 2002: 22 - 31.

[5] YU Y, ESTRIN D, GOVINDAN R. Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks[M]. Los Angeles: University of California, 2001.

[6] KARP B, KUNG H. GPSR: Greedy perimeter stateless routing for wireless networks[C]//Proc of the 6th Annual Int'l Conf on Mobile Computing and Networking. Boston: ACM Press, 2000: 243 - 254.

[7] HEINZELMAN W, CHANDRAKASAN A, BALAKRISHNAN H. Energy-efficient communication protocol for wireless micro-sensor networks[C]//Proc of the 33rd Annual Hawaii Int'l Conf on System Sciences. Maui: IEEE Computer Society, 2000: 3005 - 3014.

[8] MANJESHWAR A, AGRAWAL DP. TEEN: A protocol for enhanced efficiency in wireless sensor networks[C]//Int'l Proc of the 15th Parallel and Distributed Processing Symp. San Francisco: IEEE Computer Society, 2001: 2009 - 2015.

[9] KARLOF C, WANNER D. Secure routing in wireless sensor networks: Attacks and countermeasures[C]//The 1st IEEE Int'l Workshop on Sensor Network Protocols and Applications. Anchorane: [s. n.], 2003: 113 - 127.

[10] PERRIG A, Song D, TYGAR J D. A new protocol for efficient large-group key distribution[C]//Proceedings of the IEEE Symp on Security and Privacy, 2001: 247.

(下转第 123 页)

取之前,先对参数表进行约简以去除无意义的参数组合。

本文所述的基于模型的测试系统能够很好的应对这种变化,从而提升测试效率。

参考文献:

[1] APFELBAUM L, DOYLE J. Model-based testing[C] // Software Quality Week Conference in May, 1997.

[2] GURARI E. An introduction to the theory of computation[M]. Jones and Barlett Publishers, Inc, 2001.

[3] DALAL S R, KARUNANITHI J N, LEATON J M, et al. Model-based testing in practise[M]. ACM Press, 1999.

Dynamic software testing method based on fintie state machine model

ZHU YuWen　LIU Li　YANG JiaNing　LIU WanChun

(College of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

Abstract: In this paper, model-based testing approach is introduced. By abstracting a finite state machine(FSM) from the System under Testing(SUT), this approch can increase the test coverage by developing test cases for each states and transition, making the implementation of test tool and cases easier. When the SUT changes, only the test tool need to be rebuilt while the previous test cases can still be used without modification.

Key words: model-based testing; FSM; auto testing

(上接第 118 页)

A secure routing protocol of wireless sensor networks

LI ShaoHeng　ZHANG Kun　WANG CuiRong

(Northeast University at Qinhuangdao, Qinhuangdao Hebei 066004, China)

Abstract: A TEEN protocol-based security-efficient protocol STEEN is presented. This protocol addresses the problems of inadequate consideration for security in some of existed routing protocols for wireless sensor networks. The protocol, which takes saving of energy consumption and improving of routing security as its design targets, solves the problems of authentication and secure communication between nodes through pre-distribution of key and the random key pair-wise management. Analysis on security indicates that this protocol can be used to defend many attacks at network layer.

Key words: wireless sensor network; routing protocol; security; key management