WMSN的半依赖基站密钥管理方案

陈　昊[1]，王汝传[1,2]，黄海平[1,2]，孙力娟[1,2]，戴　庭[1]
（1. 南京邮电大学计算机学院，南京，210003；
2. 江苏省无线传感网高技术研究重点实验室，南京，210003）

摘　要：由于传统的WSN密钥管理方案，并没有考虑到无线多媒体节点的特殊性，文章提出半依赖基站密钥管理方案。该方案将密钥的产生和分发放在多媒体节点上，而sink节点采用延时认证方法负责所有节点的认证。通过分析后，该密钥管理方案符合安全性要求，并且具有较高的连通性，保证多媒体传感器网络安全高效运行。

关键词：无线多媒体传感器网络；密钥管理；网络安全
中图分类号：TP393.08

0　引言

无线多媒体传感器网络是建立在传统无线传感器基础上，引入一些具有多媒体信息感知功能的一种新型传感器网络。随着人们对检测需求的日益多样化，传统的传感器网络不能满足需求，因此，通过在装备低成本的摄像头和麦克风等环境数据采集功能传感器，就可以广泛用于战场可视化监控、环境检测、安全监控、交通监控、智能家居及医疗卫生等领域[1-2]。这些传感器分布在一些可控制的环境中，比如医院，家居，或者分布在无人值守的环境中，比如灾区或敌区。而在无人值守时，为了保证无线多媒体传感器在运行过程中的安全，则需要防止运行过程的窃听，提供虚假信息，冒充节点等非法行为的出现。所以必须对通信的内容进行加密，对加入的节点进行认证，因此，密钥的分配和管理就成为一个关键的问题。

收稿日期：2011-05-29。
基金项目：本课题得到国家自然科学基金（60973139、61170065、61171053、61003039、61003236）、江苏省科技支撑计划（工业）项目（BE2010197、BE2010198、BE2011844）、江苏省高校自然科学基础研究项目（10KJB520013、10KJB520014）、高校科研成果产业化推进工程项目（JH10-14）、江苏省六大高峰人才项目（2008118）、教育部高等学校博士学科点专项科研基金（20103223120007）和江苏省计算机信息处理技术重点实验室基金（KJS1022）资助。

1　相关工作

1.1　传统传感器网络密钥管理分析

由于无线传感器网络的特性：节点的计算存贮受限，网络的规模庞大，网络的拓扑未知，节点部署在无人值守区等，使得传感器的密钥管理和分配变得尤为困难。现有的传统传感器网络密钥管理的方案可分为以下3类：

（1）基于对称密钥体制的密钥管理方式，例如随机密钥预分配方案[3-4]。每个节点从密钥池中存储部分密钥，在节点布置好后，需找和自己有相同共享密钥的邻居节点。这种随机密钥预分配方案缺点在于，一旦攻击者俘获部分节点，网络中其余节点之间的共享密钥存在泄漏的危险[5]。

有些对称加密体制是基于可信任的第三方，例如SPINS，Kerberos[6]和Needham-Schroeder[7]，一个节点要与另外一个节点建立会话，都需要向密钥分发中心发送请求生成一个会话密钥。该协议具有很好的抗节点俘获能力，对部分节点的攻击不会影响到其他节点之间的安全通信，支持很大的网络规模；但是整个网络过分依赖密钥，造成通讯的负载太大。

另外文献[8-9]将对称加密技术与门限技术相结合，提出一种基于多元多项式的对称密钥管理方案，每个节点具有惟一的ID，并存储了相同的d元多项式。该方案可以具有较好的抗毁性，明显提高了安全性，然而存储空间的限制制约着网络规模的扩大。

（2）基于非对称加密体制的密钥管理方案。非对称加密体系不要求通信双发事先传递密钥或任何

约定就能完成保密通信,并且密钥管理方便,可以实现防止假冒和抵赖。由于传感器网络的资源受限,难以承受传统非对称加密的计算和存储复杂性。但是近期通过研究者对公钥密钥的研究、改进。文献[10-11]中,提出了轻量级椭圆曲线加密的密钥管理方案。通过性能仿真表明,相比于对称密钥体制,安全性有了显著提高;比其他的非对称密钥管理体制的密钥管理方案,节省了计算和存储开销。

(3) 基于 ID 或 Hash 函数的密钥管理,在基于 ID(身份)的密钥管理方案中,每个传感器节点都被赋予惟一的 ID 值,密钥管理方案将使用各个节点的 ID 号参与公钥运算,同时产生相应的私有密钥。文献[12]提出了适合于无线传感器网络环境的轻量级的、高效的密钥预分配方案,该方案融合了基于 CA 的公钥认证框架和基于身份的公钥认证框架二者的优点[12]。并基于二次剩余理论,对所设计的方案给出了高效的实现。

1.2 WMSN 与 WSN 密钥管理特征比较[2]

两种网络都具有自组织、多跳路由、超大规模、资源受限、无人值守的特点,而且对于能耗都很敏感。但是相比于传统的 WSN,多媒体传感器网络还需要对图像、视频、音频等多媒体信息进行采集、处理和发送,因此使得 WMSN 与 WSN 有以下几点不同:

(1) 能耗更为敏感。多媒体传感器处理数据时,所进行的计算不是简单的标量运算,而是对多媒体数据进行压缩编码、分布式视频处理、信息融合等。需要更多的能量,所以应该尽可能的节省能耗,使用的密钥管理方案不能过于复杂。

(2) 存储空间消耗大。多媒体传感器节点在运行时,由于多媒体数据量要比标量数据大的多,需要很大的存储空间,主要用于数据采集,数据处理,数据转发等。因此设计密钥管理协议时,应该尽可能使用少量的空间。

(3) 数据冗余。多媒体数据存在多种冗余:空间冗余、视觉冗余、结构冗余及时间冗余。因此可以利用这一特性,在多媒体数据中嵌入水印信息。

(4) 较高的网络吞吐量。多媒体传感器网络中的数据量大,所以需要网络能够有较高的通信吞吐量。因此,需要能够保证节点快速的连通,密钥管理协议不能过于复杂,减少通信能量消耗。

本文主要是根据 WMSN 的特点,结合传统无线传感器网络密钥管理的方法,提出适用于 WMSN 的半依赖于基站密钥管理方案。

2 WMSN 的半依赖于基站密钥管理方案

2.1 模型假设

(1) 所有的节点通信半径相同;

(2) 敌人对于节点的攻击目的是为了获取更多的节点密钥信息;

(3) 窃听者对截获的加密数据包不能立即破解其中的密钥;

(4) 在多媒体传感器网络中,假设没有丢包的发生,所有的数据包都顺利到达指定目标。

2.2 密钥预分配阶段

在多媒体网络中将所有节点分为:sink 节点、多媒体数据采集节点、数据传输节点。

sink 节点:数据的主要汇聚点,sink 节点可以向全网络广播信息,检测或控制网络的运行。

多媒体数据采集节点:这些节点上装有诸如廉价的麦克风、摄像头等的多媒体数据采集设备,用于感知周围环境信息,这些节点需要对原始的多媒体数据进行复杂的加工(图像压缩,视频编码等),因此需要在这个节点上配备较强的处理器和容量较大的存储器。

数据传输节点:相比于多媒体数据采集节点,其构造比较简单,主要目的能够成功转发多媒体数据。

在节点部署到实际的区域之前,需要对节点做以下工作:

(1) 对于所有的节点都分配惟一的 ID 号,而为了能够将多媒体节点和传输节点能够以示区别,将多媒体节点和 sink 节点的排在之前,表示为 ID^M,而传输节点编号表示成 ID^T。

(2) 所有节点都存贮一个特定的通信密钥 E_C,用于初始的临时通信。

(3) 所有节点需要存储与 sink 节点约定通信密钥 S_i,以及认证码 en_i 和初始随机数 $Nounce_i$,随机数发生函数 N。

(4) 多媒体节点由于需要进行图像处理,以及发送图像的缓冲区,所以需要较大的存储空间。为了能够节约存储,所以在多媒体节点上只存储一部分多媒体节点的通信密钥,以及多媒体节点间的约定水印信息。

(5) 所有的多媒体节点在部署到实际区域前,设定定时开始向网络发送 hello 包。

所有节点通过以上的步骤后,可以进入部署阶段。实际中,多媒体节点一般会部署在远离 sink 节点的检测区域。在部署的时候,可以考虑存有相同

密钥的多媒体节点尽量部署在一起。

2.3　网络的初始化

当所有的节点部署在特定的区域后,将多媒体节点作为簇头节点,根据传输节点到簇头的跳数,将各个网络进行分簇。多媒体网络被部署在指定区域后,多媒体节点按指定的时间向整个网络发送 hello 包,而且初始阶段,整个网络使用初始密钥 E_C 进行通信。数据包的形式如下: $E_C(\mathrm{ID}_1,\mathrm{ID}_2,n)$,其中 ID_1 为多媒体节点号,ID_2 为数据包的来源,n 是已经过的跳数,如图 1 所示。

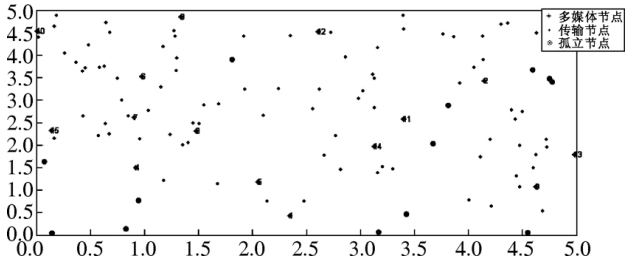

图 1　多媒体传感器网络部署情况

图 1 中模拟 5* 5 的区域,其中传输节点为 100 个,多媒体节点为 15 个,并设定所有节点的通信半径为 0.7。当传输节点收到了跳数更高的 hello 包,则扔掉。若是收到的数据包小于或等于已收到数据包的跳数,则转发数据包,并且选择跳数较近的多媒体节点作为该传输节点的簇头。

在确定了簇头后,向簇头发送数据包,向簇头汇报自己的 ID 号,而簇头则定期地为簇内传输节点分配密钥。为了保证簇内传输节点的合法性,需要对其进行认证。然而多媒体节点并没有认证能力,如果全部提交 sink 节点必定会造成网络的拥挤。因此该方案中,当传输节点被使用时,多媒体节点向 sink 节点发送认证信息: $S_i(en_i,\mathrm{Nounce}_i)$。sink 节点收到后,对信息进行验证,并将验证结果发送给多媒体节点。

2.4　节点密钥对建立过程

由于多媒体节点需要的内存空间较大,而传输节点的计算能力和存储空间小,这成为了密钥管理中的挑战。若两个节点相互通信,则两个节点相互密钥建立的过程可以分为以下 3 类:

(1) 假设多媒体节点 A,B 之间相互通信,由于多媒体节点存储部分其他多媒体节点的通信密钥,以及一些水印信息。若 A 在存储空间有多媒体节点 B 的通信密钥 E_{AB} 以及水印认证信息 en_{AB},则可以通过已有的通信密钥进行通信。其通信的过程如下:

$$A-B:(\mathrm{ID}_A,E_{AB}(n_A,\mathrm{ID}_A,0,S_A(\mathrm{Nounce},en_{AB})))$$

当 B 收到数据包后,若 B 同意与 A 进行通信,则向 A 发送同意数据包。

$$B-A:(\mathrm{ID}_B,E_{AB}(n_{AB},\mathrm{ID}_B,N(n_A)))$$

在 B 同意与 A 通信的同时,向 sink 节点发送日志数据包,并且转发节点 A 与 sink 节点约定的密钥 S_A 和认证码 en_A。使得 sink 节点能够验证 A,B 的合法性,若发现有非法的密钥,则能够及时的停止通信。

若多媒体节点 A 中不存在 B 的通信密钥,则多媒体节点 A 向已存储密钥的所有多媒体节点发出询问数据包,被查询的节点收到查询数据包后,若发现节点 C 有多媒体节点 B 的通信密钥时,多媒体节点 C 为 A,B 产生通信密钥 TE_{AB},以及临时的水印信息。如果多个节点都有节点 B 的密钥,将这些临时密钥,以及水印方式进行简单的位操作后,向 A 发送通信请求数据包。为了保证节点的合法性,A 向 B 首先发送与 sink 约定的认证数据包。数据包格式:

$$A-B:TE_{AB}(\mathrm{ID}_A,n_A,S_A(en_A,\mathrm{Nouce}_A))$$

B 收到这样的数据包后,可以向 sink 节点报告这次通信的细节,以便 sink 节点对通信的合法性做出判断。

(2) 若是多媒体节点 A 向传输节点 B 之间相互通信,首先 A 向簇内以及存有密钥的多媒体节点查询是否有节点 B。如发现 B 在簇内,如果 B 没有认证过,则需要向 sink 节点发送认证信息,则无条件的同意与簇头进行通信,但仍然需要向 sink 节点发送 A 和 B 的认证数据包等信息。而相互的通信密钥采用簇内的密钥。

如果 B 在另一个多媒体节点 C 内的传输节点,多媒体节点 C 分别为 A,B 分配临时的通信密钥,以及水印等信息。之后 A 需要向 B 发送认证数据包,以及通信细节。而 A,B 相互转发与 sink 节点的预先约定的信息,认证 A,B 的合法性。

(3) 若两个节点 A,B 都是传输节点,假设其所在的簇头分别为 C,D,节点 A 向所在的簇头节点 C 发出询问 B 请求,簇头节点 C 向簇内和存储密钥的多媒体节点查询传输节点 B。同样,如果 A,B 在同一簇内,则由 C 约定两个节点的通信细节。如果节点 C 存有 D 的密钥,则能找到传输节点 B,并由 C 和 D 共同决定 A,B 的通信方式。当 A,B 确定了通信密钥、

水印等细节后，由 B 向 sink 节点发送验证信息。

2.5　节点的加入和退出

由于传感器节点常常被部署在恶劣的环境中，以及网络协议的问题，会出现某些节点停止工作，或是某个节点重新开始工作。为了新加入的节点，能够安全获得网络的密钥，而节点的退出不影响网络的运行，所以需要合理的管理加入或退出节点的密钥。

若是传输节点退出时，并不影响到其他节点，所以只需要向簇头汇报这一行为。而当传输节点加入时，只需要把邻居节点的簇头当做自己的簇头，并告诉簇头，传输节点的存在。尽管这种加入方式，并不一定能够找到距离最近的簇头，但是可以有效减少通信消耗。

如果是多媒体节点退出时，则会使得簇内的传输节点没有了簇头，因此在退出前，告诉簇内的传输节点，让传输节点作为新加入的传输节点一样，寻找新的簇头。而当多媒体节点需要加入时，只需要向周围的节点发送 hello 包，让周围的传输节点根据跳数重新选择簇头节点。

3　密钥管理方案分析

通过以上对方案的详细描述，可以明确密钥管理的过程。

3.1　连通性分析

通过以上对该密钥管理协议的详述，可以看到，多媒体节点作为簇头，负责产生和分发传输节点密钥，而 sink 节点则负责通信双方的认证，这可以有效减少节点所存储的密钥信息，尤其是对于存储空间较小的传输节点，便于多媒体数据的处理和传输。因此整个网络的连通，主要依赖于多媒体节点所存储的密钥，而连通性的程度与所存储密钥的数量有关。假设多媒体节点所存储密钥数占整个多媒体节点的百分比为 P，多媒体节点的数量为 n，并假设所有的节点均匀的部署在区域内，则节点间相互连通的可能性为 $1-(1-P)^{np}$。

图 2 中表示为当多媒体节点数分别为 50，100，200 时，不同的密钥存储率下的连通性情况。可以看到使用这样的密钥管理方案可以达到很高的连通性，这是由于在密钥管理中，允许间接的连通，并且允许簇内的传输节点进行通信，只要发往 sink 节点的认证信息无误。所有节点的连通性都可归结于多媒体节点的连通性。并且在图中可以看到，当多媒体节点越多时，存有相同的百分比的密钥，连通性越

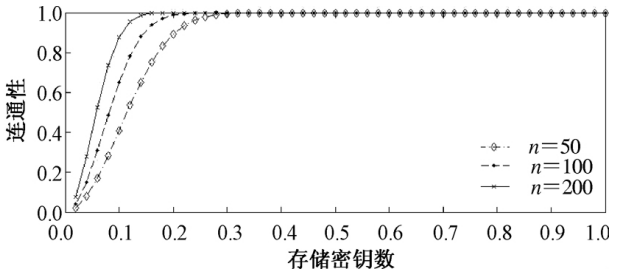

图 2　网络连通性

高，但是实际存储的密钥数也越多。然而在实际的部署中，由于存储密钥的多媒体节点距离比较远，以及丢包等原因，网络的连通性要稍微差点。

3.2　安全性分析

由于传感器网络中的节点很容易被俘获，所以密钥管理协议需要保证，即使节点被俘获后，尽可能保证不会泄露其他节点密钥信息。而对手利用被俘获的节点，通过以下两种方式对其余节点进行攻击。

直接获取：从俘获节点的存储空间内直接获取其他节点间的通信密钥。当传输节点被俘获后，由于其内部只存储与 sink 节点约定的认证信息和通信密钥以外，没有关于其他节点间密钥的任何信息，所以对手无法从俘获传输节点中获取其他节点的密钥信息。而多媒体节点被俘获，其存储了与其他多媒体节点的通信密钥，对手可以很容易获取与其他多媒体节点的通信密钥。通过图 2 的连通性可以看到，网络可以获得较高的连通性，所以多媒体节点间的密钥可以保证较高的独立性，减少了泄密的可能性。即使泄密了之后，对手无法确定具体哪两个具体两个节点之间的通信密钥，并且采用了随机数增加了密钥的安全性。

协议漏洞：利用已被俘获的节点，通过协议的漏洞俘获其余节点的密钥。而该密钥协议可以有效的避免漏洞，主要原因：1）任何节点都无法请求其他两点间的通信密钥；2）与没有存储密钥的节点进行通信时，中间节点只分配临时密钥，与其他密钥相互独立；3）被请求的节点都会向 sink 节点转发认证数据包，可以使 sink 节点有效的监督网络的运行，阻止非法节点的通信请求。这使得对手难以获取其他节点的密钥。

4　结束语

本文针对多媒体传感器网络，较为详细地分析了该网络的特征，提出了较为安全适用的密钥管理

方案,在方案中减少了存储空间和计算的消耗。然而由于网络存储计算要求较高,在认证方面并没有采用非对称方式,所以在认证方面的安全性还有待提高。

参 考 文 献

[1] Chung-Kuo Chang, Huang J. Video surveillance for hazardous conditions using sensor networks [C] //Proceedings of the 2004 IEEE Inter Conf on Networking, Sensing & Control. New York: IEEE, 2004: 1008-1013.

[2] 罗武胜,翟永平,鲁琴. 无线多媒体传感器网络研究 [J]. 电子与信息学报, 2008, 30(6): 1511-1516.

[3] Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks [C] //Proceeding of IEEE Symposium on Security and Privacy. Berkeley, California, USA, 2003: 197-213.

[4] Wenliang Du, Jing Deng, Yunghsiang SHan, et al. A pair-wise key pre-distribution scheme for wireless sensor networks [C] // The 10th ACM Conference on Computer and Communication Security, 2003 (CCS'03). Washington DC, USA: ACM Press, 2003: 12-21.

[5] 周琴,李腊元,程真. 一种基于分簇的无线传感器网络动态密钥分发协议 [J]. 传感器技术学报, 2009, 7(22): 1002-1006.

[6] Neuman B C, Ts'o T. Kerberos: an authentication service for computer networks [J]. IEEE Communications, 1994, 32(9): 33-38.

[7] Needham R M, Schroeder M D. Using encryption for authentication in large networks of computers [J]. Communications of the ACM, 1978, 21(12): 993-999.

[8] Delgosha, Ayday, Fekri. MKPS: A multivariate polynomial scheme for symmetric Key-establishment in distributed sensor networks [C] //IWCMC'07. Honolulu, Hawaii, USA: ACM Press, 2007: 236-241.

[9] Lu Kejie, Qian Yi, Hu Jiankun. A framework for distributed key management schemes in heterogeneous wireless sensor networks [C] //Performance, Computing, and Communications Conference (IPCCC 2006. 25th IEEE International) [S. l.]: IEEE, 2006: 513-519.

[10] Arazi Ortal, Qi Hairong. Self-certified group key generation for ad hoc clusters in wireless sensor networks [C] //The 14th International Conference on Computer Communications and Networks, 2005 (ICCCN 2005). San Diego, USA: [s. n], 2005: 359-364.

[11] Reza Azarderakhsh, Arash Reyhani-Masoleh, Zine-Eddine Abid. A key management scheme for cluster basedwireless sensor networks [C] //2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. Shanghai, China: IEEE Computer Society, 2008: 222-227.

[12] 潘耘,王励成,曹珍富,等. 基于轻量级 CA 的无线传感器网络密钥预分配方案 [J]. 通信学报, 2009, 30(3): 130-134.

陈昊(1985-),男,硕士研究生,主要研究方向是无线传感器网络、计算机软件在通信中的应用。

Semi-dependent Base Station Key Management Scheme for Wireless Multimedia Sensor Networks

CHEN Hao[1], WANG Ru-chuan[1,2], HUANG Hai-ping[1,2], SUN Li-juan[1,2], DAI Ting[1]

(1. School of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu Key Research Laboratory of High Technology for Wireless Sensor Networks, Nanjing 210003, China)

Abstract: As traditional WSN key management scheme didn't take into account the special nature of wireless multimedia nodes, this paper proposes a semi-dependent base station key management scheme. In this scheme, multimedia is in charge of generation and distribution of key, and the sink node is responsible for the certifications of all nodes based on delay-certifications. This can reduce the storage space of the whole network and improve the network throughput. After analysis, the key management in compliance with security requirements and with high connectivity ensures safe and efficient operation of the networks.

Key words: Wireless multimedia sensor networks (WMSN); key management; network security