文章编号:1001 - 9081(2007)08 - 1904 - 03

基于 Hash 函数的无线传感器网络密钥预分配方案

张建民, 刘贤德, 徐海峰
(华中科技大学 光电子工程系,武汉 430074)
(zjm1996@163.com)

摘 要:密钥分配是无线传感器网络通信安全的基础。在 Echenauer 和 Gligor 的随机密钥预分配方案的基础上,提出了一个基于 Hash 函数的密钥预分配方案。该方案利用 Hash 函数来计算出节点中部分的预置密钥,用 Hash 函数的单向运算特性来增强网络抵抗攻击的能力。分析表明,与现有的密钥预分配方案相比,该方案的计算负载小,安全性能高,更适合于无线传感器网络。

关键词:无线传感器网络;密钥分配;Hash 函数
中图分类号: TP309.7 **文献标志码**:A

Key pre-distribution scheme for wireless sensor networks based on Hash function

ZHANG Jian-min, LIU Xian-de, XU Hai-feng
(*Department of Optoelectronics Engineering, Huazhong University of Science and Technology, Wuhan Hubei* 430074, *China*)

Abstract: Key distribution plays a fundamental role in Wireless Sensor Networks (WSN). A key pre-distributing protocol based on Hash function was proposed, which extended the ideas of the probabilistic key pre-distribution scheme put forward by Echenaue and Gligor. In this scheme, some of the pre-distribution keys in the nodes were computed by Hash function. With the advantage of one-way Hash function, this scheme could enhance the ability of network to resist attacks. Compared with other schemes, this one has less computing overhead and higher security performance, which is more suitable for WSN.

Key words: Wireless Sensor Networks (WSN); key distribution; Hash function

0 引言

密钥分配是无线传感器网络(Wireless Sensor Networks, WSN)通信安全的基础。由于无线传感器网络具有节点资源受限、网络规模大、分布式等特点,许多传统的密钥分配方案,如基于公开密钥体系和可信任中心等的密钥分配方法不能直接应用于 WSN。目前在 WSN 中常用的密钥分配方法是采用密钥预分配技术,即在传感器节点部署之前,由离线服务器将密钥或者能产生密钥的信息预先配置在节点中,节点部署后通信双方可以通过这些信息计算出通信密钥。

Echenauer 和 Gligor 在文献[1]中首先提出了适用于无线传感器网络的随机密钥预分配方案(EG 方案),其主要思想是:在节点部署前,每个节点从同一密钥池中随机选取一定数量的密钥,使得任何两个节点之间以某一概率至少共享一个密钥。后来,文献[2]中对文献[1]中的方案进行了扩展,提出了 q-composite 密钥预分配方案。该方案要求两个节点间至少共享 q 个公共密钥才能建立安全链路,q-composite密钥预分配方案对小规模攻击具有很好的抵抗性能,但对大规模的攻击其安全性能将大大降低。在 EG 方案的基础上,文献[3]结合文献[4]的密钥预分配协议,文献[5]结合文献[6]的多项式的密钥预分配协议,分别提出了两种相似的多重空间密钥预分配协议。这两种协议都具有安全门限特点,只要被捕获的节点不超过门限值,则对节点捕获完全免疫,但是当被捕获的节点超过门限值时,所有安全链路会很快被破解。本文在 Echenauer 和 Gligor 的随机密钥分配方案的基础上,利用 Hash 函数提出了一个新的密钥预分配方案。

1 随机密钥预分配方案

EG 方案分为三个阶段:密钥预分配阶段、会话密钥直接发现阶段和会话密钥间接建立阶段。

在密钥预分配阶段,系统预先生成一个大的密钥池,密钥池中含有 ω 个互异的密钥(ω 很大),每个密钥有一个唯一的标识符。每个节点从密钥池中随机选取 τ 个密钥作为自己的预置密钥。节点部署后,进入会话密钥直接发现阶段。节点通过和相邻节点(节点在彼此的通信范围内)互相交换预分配的密钥标识符来寻找是否和某个相邻节点有公共密钥。如果两个相邻节点有公共密钥,则用其中一个作为二者之间的会话密钥。如果两个相邻节点之间不存在公共密钥,则需要通过间接方法建立会话密钥,这时可以通过与它们都有公共密钥的相邻节点作为中介,通过协商建立会话密钥。

由于 τ 小于 ω,所以任意两个相邻节点间只能以某个概率存在公共密钥,该概率即为节点间的安全连通概率。根据随机图论,有 N 个节点的随机图,如果要达到给定的全局连通概率 Pc,则节点的平均度数 d 至少要满足:

$$d = \frac{(N-1)}{N}[\ln(N) - \ln(-\ln(P_c))]$$

假设传感器网络中每个节点平均有 D 个邻居节点,如果要达到要求的全局连通 Pc,则节点与相邻节点之间的本地连通概率 P_{local} 至少要满足:

$$P_{local} = \frac{d}{D} = \frac{1}{D}\frac{(N-1)}{N}[\ln(N) - \ln(-\ln(P_c))]$$

相关的数学已经证明,在一般传感器网络的节点部署密

收稿日期:2007 - 02 - 02;**修回日期**:2007 - 03 - 30。

作者简介:张建民(1970 -),男,河南新郑人,博士研究生,主要研究方向:智能家庭、无线传感器网络; 刘贤德(1938 -),男,湖北武汉人,教授,博士生导师,主要研究方向:智能空间、高速信息网络; 徐海峰(1965 -),男,江苏南京人,副教授,博士,主要研究方向:红外光电网络、数字家庭。

度下,安全连通概率 P_{local} 只要达到 0.33,两相邻节点至多需要 3 跳即可建立共享的会话密钥[2]。

另外,由于所有节点都从同一个密钥池中抽取密钥,所以攻击者可以从捕获的节点中得到未被捕获节点的密钥信息,一个被捕获节点泄漏的密钥信息越少,网络抵抗攻击的能力就越强。减少 τ 值或增加 ω 值可以提高网络抵抗攻击的能力,但会降低节点间的连通概率;增加 τ 值或减少 ω 值都可以增大节点间的连通概率,但会降低网络抵抗攻击的能力。

2　基于 Hash 函数的密钥管理方案

2.1　方案的基本思想

本方案的基本思想把每个节点上预置的密钥分为两类,一类密钥与 EG 方案中预置的密钥类似,相邻节点间可用共享的此类密钥作为节点间的会话密钥,但是当节点被捕获时也会泄漏其他节点上的密钥信息。另一类密钥只有与前一类密钥结合起来才能建立节点间的会话密钥,而相邻的节点无法只利用这类密钥来建立节点间的会话密钥,但是这类密钥对节点捕获的攻击是完全免疫的,攻击者无法从中获取其他节点上的任何密钥信息。

本文提出的方案以 EG 方案为基础,分为三个阶段:密钥预分配阶段、会话密钥直接建立阶段和会话密钥间接建立阶段。

2.2　密钥预分配阶段

系统首先生成包括 w 个密钥的密钥池,每个节点从中随机选取 t 个密钥,然后再从这 t 个密钥中随机选取 tp 个密钥作为节点的原始密钥,其余 tm 个密钥作为节点的主密钥。系统把节点选取的 tp 个原始密钥直接分配给节点保存,然后根据节点的标识符和主密钥按下列方法生成子密钥:假设节点 u 的标识符是 id_u,主密钥为 $Km_i(1 \leqslant i \leqslant tm)$,$H(id, Key)$ 为一哈希运算函数,则主密钥 Km_i 在节点 u 上的子密钥为 $Ks_i = H(id_u, Km_i)$。最后,系统把生成的子密钥和其标识符(生成子密钥的主密钥标识符)也分给对应的节点保存。

显然当每个节点选取的密钥都作为主密钥,即 $tp = t$ 时,本方案就与 EG 方案相同。

2.3　会话密钥的直接建立阶段

节点部署后,相邻节点相互交换密钥的标识符(包括原始密钥和子密钥的标识符)和节点的标识符。如果两个相邻节点有公共的原始密钥,就选择其中一个作为会话密钥;如果两个节点中一个原始密钥的标识符与另一个节点的子密钥的标识符相同,这表明一个节点的原始密钥与另一个节点子密钥的主密钥相同,这个子密钥可以作为二者之间的会话密钥。另一个节点可按下述方法生成会话密钥:假设节点 u 上的原始密钥 Kp_u 与节点 v 上的子密钥 Ks_v 的标识符相同,即 Kp_u 与 Ks_v 的主密钥 Km_v 相等,则节点 u 可以根据节点 v 的标识符 id_v 生成二者之间的会话密钥 $SK = H(id_v, Kp_u)$,显然 SK 与节点 v 上的子密钥 Ks_v 相等。

2.4　会话密钥的间接建立阶段

如果两个相邻节点间没有相同密钥标识符(包括原始密钥和子密钥的标识符),或者只有子密钥的标识符相同,则可以寻找与它们都可以建立会话密钥的第三方节点来构建它们之间的会话密钥。

3　性能分析

3.1　安全连通概率

根据密钥预分配方案可知,两个相邻节点间只有在两种情况下不能直接建立会话密钥,即这两个相邻节点间的密钥标识符(包括原始密钥和子密钥的标识符)都不相同,或这两个相邻节点之间只有子密钥的标识符相同。假设两个相邻节点没有相同密钥标识符的概率为 P_1,两个节点只有子密钥标识符相同的概率为 P_2,经推导可知:

$$P_1 = \frac{\binom{w}{2t}\binom{2t}{t}}{\binom{w}{t}\binom{w}{t}}$$

$$P_2 = \sum_{i=1}^{t_m} \frac{\binom{w}{i}\binom{t_m}{i}\binom{t_m}{i}\binom{w-i}{2(t-i)}\binom{2(t-i)}{i}}{\binom{w}{t}\binom{t}{i}\binom{w}{t}\binom{t}{i}}$$

则任意两个相邻节点间的安全连通概率 P 为:

$$P = 1 - P_1 - P_2 = 1 - \frac{\binom{w}{2t}\binom{2t}{t}}{\binom{w}{t}\binom{w}{t}} - \sum_{i=1}^{t_m} \frac{\binom{w}{i}\binom{t_m}{i}\binom{t_m}{i}\binom{w-i}{2(t-i)}\binom{2(t-i)}{i}}{\binom{w}{t}\binom{t}{i}\binom{w}{t}\binom{t}{i}} = 1 - \sum_{i=1}^{t_m} \frac{\binom{w}{i}\binom{t_m}{i}\binom{t_m}{i}\binom{w-i}{2(t-i)}\binom{2(t-i)}{i}}{\binom{w}{t}\binom{t}{i}\binom{w}{t}\binom{t}{i}}$$

图 1 是当节点上保存密钥数 $t = 200$,子密钥数 tm 取不同值时,相邻节点间的连通概率随密钥池大小 w 的变化曲线。从图 1 中可以看出,当 w 和 t 一定时,网络中相邻节点间的连通概率随 tm 值的增加而减少,因为当 tm 的取值增加时,每个节点的子密钥数增加,而即使节点间的子密钥具有相同的主密钥,二者之间也不能直接建立会话密钥。显然,当 tm 增加到 200 时,节点上只有子密钥而没有原始密钥,这时任何两个节点间都不能建立会话密钥。图 1 中 $tm = 0$ 的曲线为 EG 方案的安全连通概率曲线,可以看出,在相同的条件下,本方案节点间的连通概率低于 EG 方案,因为本方案中两个节点间不是所有共同的密钥(包括原始密钥和主密钥)都可以用来直接建立会话密钥。

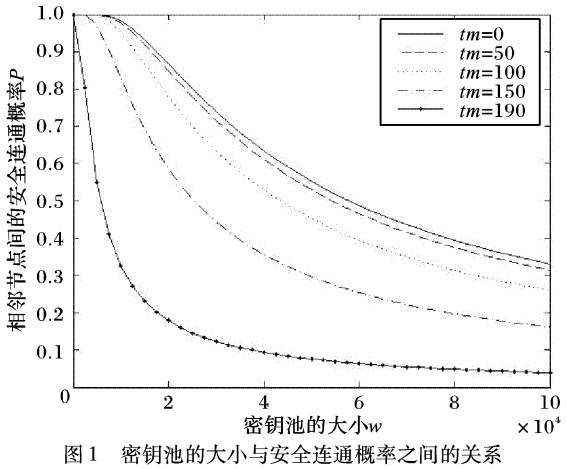


图 1　密钥池的大小与安全连通概率之间的关系

3.2　抵抗攻击的能力

当传感器节点部署后,攻击者可以物理捕获节点,获得被捕节点的所有密钥信息,并通过这些信息来攻击网络中其他安全节点间的链路。

在本方案中,每个节点上的子密钥都是不同的,而且 Hash 函数具有单向运行性质,攻击者从捕获节点中的子密钥无法推算出其对应的主密钥,所以攻击者只能从捕获的节点

中获得其他节点的原始密钥信息。根据文献[1]可知，当 x 个节点被捕获时，网络中未被捕获节点间安全链路被破解的比例 P_{broken} 为：

$$P_{broken} = 1 - \left(1 - \frac{t_p}{w}\right)^x = 1 - \left(1 - \frac{t - t_m}{w}\right)^x$$

当节点上保存密钥数 $t = 200$ 时，方案在不同的连通概率 P 和不同子密钥数 tm 情况下，网络抵抗攻击的能力如图2所示。可以看出，在其他条件相同时，随着 tm 值的增加安全链路被破解的比例减少，因为随着 tm 值的增加，每个被捕获节点能够泄漏其他节点的密钥信息也随之减少。

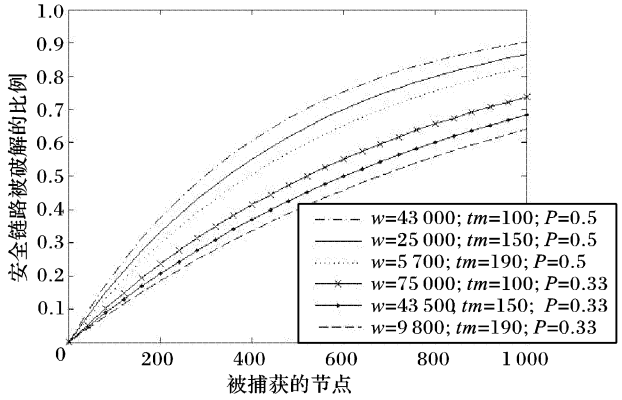
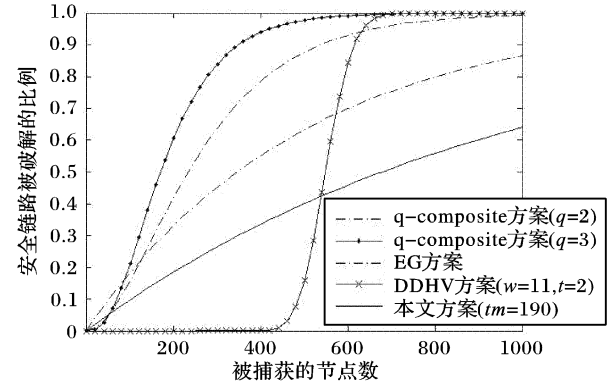


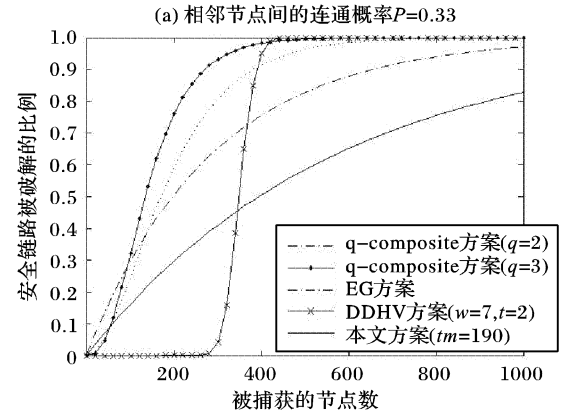
图2 被捕获的节点数与安全链被破解比例之间的关系

3.3 方案的性能比较

首先比较在相同的条件下本方案与 EG 方案、q-composite 方案（$q = 2,3$）以及基于多空间密钥随机预分配方案（DDHV 方案）[3]的安全性能。假设节点有相同的密钥存储空间限制，这里都用每个节点保存的密钥数 t 表示，而且节点间都以相同的概率 P 建立安全链路。以 $t = 200$，$P = 0.33$ 和 $t = 200$，$P = 0.5$ 为例，方案间安全性能比较分别如图3(a、b)所示。



(a) 相邻节点间的连通概率P=0.33



(b) 相邻节点间的连通概率P=0.5

图3 网络抵抗攻击能力的比较

从图3可以看出，本方案安全性能明显好于 EG 方案，如在相邻节点间连通概率为 0.33 情况下，当 600 个节点被捕获时，本方案中只有 45% 的安全链路被破解，而在 EG 方案中已有 70% 的安全链路被攻击者控制。这主要是因为本方案中节点的子密钥虽然对节点间的安全连通概率只有部分贡献，但是对攻击者利用捕获节点进行的攻击是完全免疫的。与 q-composite 方案相比，只有当被捕获节点数较少时，其抵抗攻击的能力才比本方案强。如在图3中，当被捕获的节点数超过 60 时，本方案的安全性能就好于 q-composite 方案，而对于一个有几千个节点的无线传感器网络来说，攻击者很容易捕获 60 个节点。从图3可以看出，文献[3]中的 DDHV 密钥预分配方案具有安全门限，当被捕获的节点数低于安全门限值时被捕获节点对安全链路的影响几乎为零，但是当被捕获的节点数超过安全门限时，网络中的所有安全链路会被很快地破解，如当连通概率 $P = 0.5$ 时，攻击者只需捕获 400 个节点就基本上可以控制整个网络。

对方案计算负载进行比较，由于文献[3]的密钥预分配方案需要大素数的模余运算，计算负载较大，因此只需与 EG 方案和 q-composite 方案的计算负载进行比较。这里假设每个节点要预置 200 个密钥，由于本方案中每个密钥除了标识符外，每个密钥还要有 1 bit 来标示密钥的类别（原始密钥或子密钥），因此本文方案每个节点多需 25 Byte 的内存空间，同样在生成密钥时每个报文也多需 25 Byte。在本方案中，密钥预分配阶段中节点上子密钥的产生由系统的离线服务器完成，所以这里只分析在密钥生成时所需运算量。根据密钥生成方案，节点间在直接生成会话密钥时最多只需要一次 Hash 运算，而且也只需在其中一个节点上进行，所以相对于 EG 方案，本方案所引起的额外计算量是很小的。由于 q-composite 方案密钥生成时也需要 Hash 运算，所以本方案的运算量与之相差不大。

4 结语

密钥管理是无线传感器网络安全的热点研究问题。本文利用 Hash 函数提出了一个新的无线传感器网络密钥管理方案。该方案利用 Hash 函数的单向运算性质来提高网络的安全性能。分析表明，该方案只需要少量的 Hash 运算，计算负载小，非常适合于节点能量十分有限的无线传感网络。另外，与其他方案相比，该方案具有较高的网络抵抗攻击能力，可以满足无线传感器网络的安全要求。

参考文献：

[1] ESCHENAUER L, GLIGOR V D. A key management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. Washington: ACM Press, 2002: 41-47.

[2] CHAN H, PERRIG A, SONG D. Random key pre-distribution schemes for sensor networks[C]// IEEE Symposium in Security and Privacy. Berkeley, California: IEEE Computer Society, 2003: 197-205.

[3] DU W, DENG J, HAN Y. *et al.* A pairwise key pre-distribution scheme for wireless sensor networks[J]. ACM transaction on Information and System Security, 2005, 8(2): 228-258.

[4] BLOM R. An optimal class of symmetric key generation systems [C]// Advance in Cryptography. London: Springer-Verlag, 1984: 335-338.

[5] LIU D, NING P, LI R. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security, 2005, 8(2): 41-77.

[6] BLUNDO C, SANTIS AD, HERZBERG A, *et al.* Perfectly secure key distribution for dynamic conference[J]. Information and Computation, 1995, 146(1): 1-23.