第41卷 第12期 西 安 交 通 大 学 学 报 Vol.41 №12
2007年12月 JOURNAL OF XI'AN JIAOTONG UNIVERSITY Dec. 2007

基于随机密钥预分布模型的安全定向扩散协议

宋飞[1,2]，谷雨[1,2]，周颢[1,2]，赵保华[1,2]
（1.中国科学技术大学计算机科学与技术系，230027，合肥；2.安徽省计算与通讯软件重点实验室，230027，合肥）

摘要：为了解决无线传感器网络中定向扩散协议的安全问题，提出一种基于随机密钥预分布模型的安全定向扩散协议.通过建立安全梯度及应用累积报文鉴别码和多层加密，扩展了定向扩散协议的安全机制，使其能够提供点到点的安全数据通信.安全分析表明，基于随机密钥预分布模型的安全定向扩散协议能够保证定向扩散协议在兴趣扩散、数据传输、路由建立和路径加强阶段的安全性，有效抵御多种由泄密节点发起的攻击.

关键词：随机密钥预分布；定向扩散；无线传感器网络
中图分类号：TP393 **文献标识码**：A **文章编号**：0253-987X(2007)12-1423-04

Secure Directed Diffusion Protocol Based on Random Key Predistribution Model

Song Fei[1,2], Gu Yu[1,2], Zhou Hao[1,2], Zhao Baohua[1,2]
(1. Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China;
2. Anhui Province Key Laboratory of Software in Computing and Communication, Hefei 230027, China)

Abstract: For solving the security issues of directed diffusion in wireless sensor networks, a secure directed diffusion protocol based on random key predistribution model was proposed, which extends the security of directed diffusion protocol and provides node-to-node secure data communication by setting up secure gradients and applying cumulative message authentication code and multilayer encryption. Security analyses show that the proposed protocol can ensure the security in interest propagation, data propagation, routing setting and path reinforcement phases of directed diffusion, and defend against attacks launched by compromised nodes efficiently.

Keywords: random key predistribution; directed diffusion; wireless sensor network

在金融、军事等领域的应用中，无线传感器网络传输数据的安全性是首先要解决的问题，而传感器节点自身资源有限致使安全性问题难以解决.定向扩散协议[1](Directed Diffusion，DD)是一种以数据为中心的基于查询的路由协议，能够适应于大规模的无线传感器网络，并且能有效处理节点失效和拓扑变化的情况，但是该协议本身没有考虑安全性问题.

在系统布置之前，密钥预分布模型可完成大部分的密钥协商，因此它适用于传感器网络.随机密钥预分布模型是针对传感器网络的特点而提出的一种预分布模型，该模型的主要思想是，任意节点随机拥有一个大密钥池的部分密钥，只要节点之间拥有一对相同的密钥，它们就可以使用共享密钥进行安全通信[2].基本的随机密钥预分布模型等一系列的后续研究目前正在进行之中[3-4].

定向扩散协议的安全性研究主要有基于单向密钥链的安全定向扩散协议[5]，该机制对于点到点的数据验证需要使用洪泛的方法，其通信代价比较大，另外还有使用基于安全原语的节点间以及节点与基

收稿日期：2007-01-29. 作者简介：宋飞(1983～)，男，博士生；赵保华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60602016，60241004)；国家重点基础研究发展规划资助项目(2003CB14801)；国家高技术研究发展计划资助项目(2007AA01Z428)；华为基金资助项目(YJCB2006062WL，YJCB2007061WL)；信息产业部国家242信息安全计划资助项目(2005C56).

站间的通信密钥来达到安全路由的协议机制[6]，但该机制的安全特性过于依赖节点定位的准确性和安全性.

针对上述问题，本文提出了一种基于随机密钥预分布模型的安全定向扩散协议.

1 基于随机密钥预分布模型的定向扩散协议

基于随机密钥预分布模型的安全定向扩散协议包含如下阶段.

1.1 密钥预分布

对所有的随机密钥预分布方案，本文的安全定向扩散协议机制都易于扩充、实现，下面以基本的随机密钥预分布模型[2]为例加以说明.

在布置传感器节点之前，应先为其设置一个全局惟一的标识符(ID)和一个与基站共享的主通信密钥，然后从一个大的密钥空间中为传感器网络选择一个密钥池 s，密钥池中的每个密钥对应一个惟一的序号. 对于每个传感器节点，从密钥池中随机选择 m 个密钥，并预分布到节点之中，这 m 个密钥构成节点的密钥环. 为了节省通信开销，增强通信安全性，可利用伪随机函数(PRF)选择、生成这 m 个密钥，节点标识符的哈希值作为随机函数的种子. 假设节点 P 在密钥环中的密钥为 $\{K_{I_1}, K_{I_2}, \cdots, K_{I_j}, \cdots, K_{I_m}\}$，则第 j 个密钥

$$I_j = f_{\mathrm{PRF}}(H^j(\mathrm{ID}_P)) \quad 1 \leqslant j \leqslant m$$

式中：H 表示哈希函数. 对节点的 ID_P，分别作用 j ($1 \leqslant j \leqslant m$)次 H 函数的结果作为 PRF 的种子，可生成节点密钥环中的密钥序号. 对于传感器网络中的另一节点，只要知道某节点的标识符，就可以计算出该节点在密钥环中的密钥序号，但不能获取相应的密钥.

1.2 安全的兴趣扩散

在兴趣扩散阶段，兴趣消息由基站向整个网络广播，在兴趣扩散的过程中各节点间建立起扩散梯度. 实现安全的兴趣扩散，需要保证兴趣消息在传播过程中不被修改，且各节点能验证兴趣消息是否来自基站，同时要保证扩散梯度的安全性. 本文使用了 μTESLA[7]协议，以防止修改兴趣消息和传播伪造的兴趣消息.

仅当 2 个邻居节点之间具有共享的预分布密钥时，才能建立扩散梯度关系，称之为安全梯度. 为了建立安全梯度，应对 μTESLA 协议进行调整，即当 P 转发兴趣消息时，在消息中加入自己的 ID_P. P 的邻居节点 Q 收到该兴趣消息时，应根据接收到的 ID_P 计算 P 在密钥环中的密钥序号，并与自己密钥环中的密钥进行比较. 如果存在共享密钥，Q 保存该兴趣消息中的信息，并与 P 建立梯度关系，且在兴趣消息中加入自己的 ID_Q，然后将该兴趣消息转发到其他邻居节点(除 P 以外的)，否则丢弃该兴趣消息.

经过一段时间，兴趣消息将扩散到整个网络，开始进入低速数据传输和路由建立阶段.

1.3 安全的低速数据传输和路由建立

若源节点感知到数据属于紧急数据，则使用与基站共享的主通信密钥对数据进行加密传输. 为了保证邻居节点间传输数据的安全性，应按照安全梯度进行数据传输，并根据共享的预分布密钥在邻居节点间建立通信密钥，过程如下.

(1)计算所有共享密钥的异或值，并将其作为协商通信密钥的加密密钥 K_e. 假设 P 和 Q 之间的共享密钥集合为 $\{K_{PQ}(1), K_{PQ}(2), \cdots, K_{PQ}(i), \cdots, K_{PQ}(l)\}$，$1 \leqslant l \leqslant m$，则加密密钥

$$K_e = K_{PQ}(1) \oplus K_{PQ}(2) \oplus \cdots \oplus K_{PQ}(i) \oplus \cdots \oplus K_{PQ}(l)$$

(2)设 P 要向 Q 传输数据，则 P 首先随机生成一个通信密钥 $K_C(P,Q)$并使用 K_e 进行加密，再将加密后的密钥传输给 Q. Q 在收到加密密钥后，使用过程(1)方法生成的密钥 K_e 进行解密，获得通信密钥 $K_C(P,Q)$，然后给 P 返回一个密钥确认消息，该消息中附加了一个使用密钥 $K_C(P,Q)$生成的报文鉴别码. P 在收到密钥确认消息之后，对附加的报文鉴别码进行验证. 如果验证通过，则完成通信密钥协商过程，否则拒绝向该邻居传输数据.

通信密钥的协商过程为

$$\begin{aligned} P \Rightarrow D:&\quad \mathrm{ID}_P, \{K_C(P,Q)\}_{K_e} \\ Q \Rightarrow P:&\quad \mathrm{ID}_Q, \{\mathrm{KeyAckMsg}\}, \\ &\quad \mathrm{MAC}_{K_C(P,Q)}(\mathrm{KeyAckMsg}) \end{aligned}$$

相应的梯度节点间的数据均采用该通信密钥传输数据. 对于相同的邻居节点，如果存在多个梯度，则需要建立各自的通信密钥并对数据进行加密传输.

在传输过程中，数据依次记录下所经节点的标识符. 当数据到达基站 B 时，B 便获得了多条到达源节点路由上的节点标识符列表. 为了保证数据的新鲜性，在传输过程中应加入现时(Nonce，一次交互的惟一标识符，为防止冒充使用随机数发生器生成现时)来抵御重放攻击. 基站为了验证路由信息并降低通信开销，可采用累计报文鉴别码来验证节点

列表，每个节点以收到的报文鉴别码与其节点标识符的连接作为源报文，使用与基站共享的主通信密钥来生成报文鉴别码，然后将报文鉴别码附加到报文之中. 当数据到达 B 时，节点根据节点列表和 Nonce 重新计算报文鉴别码并进行验证.

假设数据从节点 S 开始沿路径$\{S,A,E,B\}$传输，则 S 以生成的 Nonce 与 ID_S 的连接作为源报文，使用密钥 $K_b(S)$生成初始报文鉴别码 Mac(S). 节点 A 收到该报文后，以 Mac(S)与 ID_A 的连接作为源报文，使用 $K_b(A)$生成新的报文鉴别码，依次进行. 节点间的加密数据传输内容如下.

$$S\Rightarrow A:\mathrm{Mac}(S)=\mathrm{Mac}_{K_b(S)}(\mathrm{Nonce}|\mathrm{ID_S})\{\mathrm{Data}|\mathrm{Nonce}|\{\mathrm{ID_S}\}|\mathrm{Mac}(S)\}_{K_C(S,A)}$$

$$A\Rightarrow E:\mathrm{Mac}(A)=\mathrm{Mac}_{K_b(A)}(\mathrm{Mac}(S)|\mathrm{ID}_A)\{\mathrm{Data}|\mathrm{Nonce}|\{\mathrm{ID_S},\mathrm{ID}_A\}|\mathrm{Mac}(A)\}_{K_C(A,E)}$$

$$E\Rightarrow B:\mathrm{Mac}(E)=\mathrm{Mac}_{K_b(E)}(\mathrm{Mac}(A)|\mathrm{ID}_E)\{\mathrm{Data}|\mathrm{Nonce}|\{S,A,E\}|\mathrm{Mac}(E)\}_{K_C(E,B)}$$

在基站处，应检查如下等式是否成立，即

$$\mathrm{Mac}(E)=\mathrm{Mac}_{K_b(E)}(\mathrm{Mac}_{K_b(A)}(\mathrm{Mac}_{K_b(S)}(\mathrm{Nonce}\mid\mathrm{ID_S})\mid\mathrm{ID}_A)\mid\mathrm{ID}_E)$$

1.4　安全的路径加强

路径加强是定向扩散协议的重要特征之一，各节点应根据设定的规则加强特定的路径以提高传输速率，加强路径也是攻击者的首要目标. 为了保证路径加强信息的安全性，所有路径加强信息的传播都要经过基站来进行，基站根据预先设定的规则，概率性地选择路经进行加强. 基站使用与各节点共享的主通信密钥进行多层加密路径加强信息，节点收到路径加强信息后，只能获得加强路径上该节点的下一跳信息，却无法获得加强路径上的完整信息.

基站如果加强了路径$\{S,A,E\}$，则向节点 E 发送报文，即

$$B\Rightarrow E:\{\mathrm{Reinforcement}\mid\mathrm{Nonce}\mid\{\{\{\mathrm{Nonce}\mid\mathrm{ID_S}\}_{K_b(S)}\mid\mathrm{ID_S}\}_{K_b(A)}\mid\mathrm{ID}_A\}K_{b(E)}\}_{K_C(B,E)}$$

E 在收到路径加强消息之后，使用密钥 $K_b(E)$解密加强路径，得知下一跳为 A，并将剩余的路径信息发送给 A，即

$$E\Rightarrow A:\{\mathrm{Reinforcement}\mid\mathrm{Nonce}\mid\{\{\mathrm{Nonce}\mid\mathrm{ID_S}\}_{K_b(S)},\mathrm{ID_S}\}_{K_b(A)}\}_{K_C(E,A)}$$

A 在收到路径加强消息之后，使用密钥 $K_b(A)$解密加强路径，得知下一跳为 S，并将剩余的路径信息发送给 S，即

$$A\Rightarrow S:\{\mathrm{Reinforcement}\mid\mathrm{Nonce}\mid\{\mathrm{Nonce}\mid\mathrm{ID_S}\}_{K_b(S)}\}_{K_C(A,S)}$$

S 在收到消息之后，使用密钥 $K_b(S)$进行解密，发现自己是目的节点，并检查 Nonce 是否一致，如果 Nonce 是一致的，则更新兴趣信息，否则拒绝更新兴趣信息. 至此，路径加强过程结束.

2　安全分析

2.1　安全连通

由于对兴趣扩散过程进行了调整，当两邻居节点具有共享的预分布密钥时，才能建立安全的梯度关系和转发兴趣消息，因此兴趣扩散过程受到了抑制. 为了保证兴趣消息能从基站扩散到任意节点，必须保证网络是安全连通的.

可用每个节点拥有的密钥占整个密钥池中密钥的比例表示节点安全责任度 $r_{ns}=m/|s|$，那么节点的安全责任度越大，节点泄密后泄露的密钥信息越大，整个网络的安全性就越低，此时 2 个节点间共享密钥的概率越大，网络的安全连通度越高.

令 2 个相邻传感器节点能够建立安全梯度的概率[2]为 p_s，对于未扩展安全性的定向扩散协议，如果在数据源和基站间存在一条 h 跳的路径，那么引入本文安全特性后的路径安全连通概率为 p_h，则 $p_h=p_s^h$，其中

$$p_s=1-\frac{((|s|-m)!)^2}{(|s|-2m)!(|s|)!}=1-\frac{(1-m/|s|)^{2(|s|-k+1/2)}}{(1-2m/|s|)^{(|s|-2m+1/2)}}\qquad(1)$$

传感器节点存储密钥的空间一般是有限的，因此密钥环 m 的大小往往是固定的. 给定 $m=100$，不同安全责任度下的 p_h 与 h 的关系如图 1 所示. 实际应用时，可根据需要并通过调整预分布参数 r_{ns}来平衡安全性和连通性.

2.2　攻击抵御分析

下面分析本文安全定向扩散协议机制在协议各阶段抵御攻击的能力.

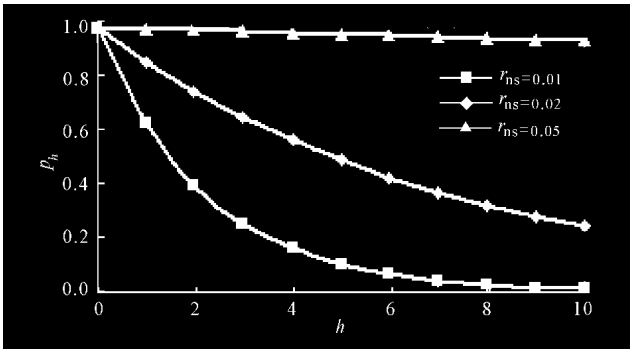

图 1　路径安全连通概率(m=100)

2.2.1 针对兴趣扩散的攻击 由于采用了μTESLA协议对广播报文进行认证,因此攻击者伪造和修改过的兴趣消息将被节点丢弃,详细分析参见文献[7].

2.2.2 针对数据传输的攻击 攻击者在俘获了部分节点之后,将获得密钥池的部分密钥信息,从而窃取网络中其他节点传输的数据.由于未采用节点密钥环内的密钥作为节点间的通信密钥,因此攻击者无法破解已建立通信密钥的节点传输的数据信息.又因每个节点与基站之间共享一个主通信密钥,所以攻击者也无法获取该密钥来破解通过泄密节点传输给基站的数据信息.在文献[5-6]中,数据采用明文传输,因此泄密节点可轻松获得经过该节点的数据信息.

2.2.3 针对路由建立的攻击 在路由建立阶段,攻击者可通过删除或修改节点列表的节点标识符来破坏路由建立过程.对于路由$\{S,A,E,B\}$,假设E是泄密节点,且攻击者想在节点列表中删除A,则必须获得Mac(S).根据报文鉴别函数的特性,从Mac(A)获取Mac(S)在计算上是不可行的.如果想在A后增加B,则必须获得B与基站共享的主通信密钥,这样才可计算正确的报文鉴别码.因此,攻击者无法修改路由建立阶段的路由信息.文献[6]在路由建立过程中未进行加密保护,而是通过灵活的路由加强策略来避开不安全路由,所以需要较长的收敛时间.

2.2.4 针对路由加强的攻击 攻击者通过截获路径加强信息获知当前兴趣的数据源位置,进而可在数据源附近发起拥塞攻击来破坏数据的传输,或者直接破坏数据源附近的节点以干扰网络的正常工作.本文的安全定向扩散协议的路径加强信息是通过基站进行传播的,且采用点到点的安全信道传播.这样,即使加强路径上的部分节点被泄密,加强路径以外的节点将无法获得路径加强信息.由于本文在路径加强信息上采用了多层加密法,所以每个节点在解密加强路径信息之后,只能获得下一跳信息,而不能通过获得整个路径信息来确定数据源节点,从而保护了数据源的位置.文献[5-6]对路径加强信息未作加密保护,而是在路径加强报文中采用明文传输,因此任何节点都可获得数据源位置.

泄密节点一般是利用提高数据发送速率等手段,通过基站加强其所在的路径来破坏数据传输,对于这种情况,本文则通过设定规则概率选择加强路径,从而抵御攻击,同时在路径加强信息中加入现时,这样数据源可以检验路径加强信息的新鲜性,从而拒绝接受重放的路径加强信息.

3 结 论

本文基于随机密钥预分布模型,提出了一种安全定向扩散协议机制,并对定向扩散协议的安全性进行了扩展.节点间通过预分布的密钥建立了安全的梯度关系,路由建立的过程则通过累积报文鉴别码和多层加密对路由信息进行验证和加密.安全分析表明,根据不同的应用需求,可通过调整配置参数来平衡安全性和连通性,该机制能有效保证定向扩散协议在各个阶段的安全性,并提供点到点的安全数据通信.

参考文献:

[1] Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion for wireless sensor networking[J]. IEEE/ACM Transactions on Networking, 2003,11(1):2-16.

[2] 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. New York: ACM, 2002: 41-47.

[3] Chan Haowen, Perrig A, Song D. Random key predistribution schemes for sensor networks[C]//Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. Los Alamitors, USA: IEEE Computer Society, 2003:197-213.

[4] 王换招,罗东玮,陈菲菲,等. 基于密钥池的簇状传感器网络动态密钥分配协议[J].西安交通大学学报,2006,40(8):911-914.
Wang Huanzhao, Luo Dongwei, Chen Feifei, et al. Dynamic keys distribution protocol based on key-pool in clustered sensor networks [J]. Journal of Xi'an Jiaotong University, 2006,40(8):911-914.

[5] Wang Xiaoyun, Yang Lizhen, Chen Kefei. SDD: secure directed diffusion protocol for sensor networks [C]//1st European Workshop on Security in Ad-Hoc and Sensor Networks. Heidelberg, Germany: Springer-Verlag, 2004:205-214.

[6] Yang Hao, Wong S H Y, Lu Songwu, et al. Secure diffusion for wireless sensor networks [EB/OL]. [2007-01-01]. http: www. cs. ucla. edu/~ hyang/paper/BROANETS06. pdf.

[7] Perrig A, Szewczyk V, Wen V, et al. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5):521-534.

(编辑 苗凌)