文章编号：2095-4980(2021)01-0150-06

安全高效的无线传感器网络远程身份验证协议

张红军

(安阳学院 计算机学院，河南 安阳 455000)

摘　要：针对无线传感器网络节点资源受限及通信链路易出错的问题，给出一种安全高效的无线传感器网络远程身份验证协议。该协议采用集中式基于簇的分层无线传感器网络选出最优百分比的簇头，并对其与相邻节点的通信进行授权，再最小化节点能耗实现网络负载平衡，然后每个簇头作为服务器在每个传递消息的有效负载内保证数据认证与交换，对相邻节点进行身份验证后即可构成簇。由仿真分析结果可知：该协议的安全性、抗攻击鲁棒性、握手持续时间、平均能耗和网络平均吞吐量指标都优于已有改进的低功耗自适应集簇分层协议(imp-LEACH)与安全 LEACH 协议(sec-LEACH)。

关键词：无线传感器网络；远程身份验证；簇头选取；有效负载握手

中图分类号：TN915.08；TP393　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019434

A secure and efficient remote authentication protocol of Wireless Sensor Networks

ZHANG Hongjun

(School of Computer Science and Technology，Anyang University，Anyang Henan 455000，China)

Abstract：Aiming at the problems of the resource limitation of nodes and the error-prone communication chain in Wireless Sensor Networks(WSN), a secure and efficient remote authentication protocol based on WSN is presented. It adopts the centralized cluster-based hierarchical WSN to select the cluster head with the optimal percentage, and the cluster head is authorized to communicate with neighboring nodes; the network load balance is realized by minimizing the energy consumption of the nodes. Then each cluster head acts as a server, ensuring data authentication and exchange with each payload that delivers the message, and authenticating nearby nodes to form clusters. Simulation results indicate that the presented protocol is better than the existing protocols of improved Low Energy Adaptive Clustering Hierarchy(imp-LEACH) and secure LEACH(sec-LEACH) in the aspects of security, robustness, handshake duration, average energy consumption, and average network throughput.

Keywords：Wireless Sensor Network；remote authentication；cluster-head selection；active-load handshake

无线传感器网络(WSN)是用于监控、感知、捕捉和处理相关应用数据的微型传感器节点集合[1−2]。由于电池电量、存储空间、数据速率和可用带宽等限制，有必要对这些资源受限的节点进行高效利用，以提高无线传感器网络的整体性能[3]。此外，网络节点容易受到物理篡改以及各种远程攻击[4]。因此，良好的网络协议也是无线传感器网络的重要组成部分，而采用身份认证与加密技术可以在资源受限的情况下不仅能保障无线传感器网络的整体安全性，同时也能保证无线传感器网络的服务质量。所给协议使用了集中式基于簇的分层无线传感器网络——低功耗自适应集簇分层(LEACH)协议[5]，是基于有效负载握手 LEACH 的双向身份验证(active-load

收稿日期：2019-10-30；**修回日期：**2020-03-13

基金项目：河南省科技攻关项目资助(182102210208)；河南省高等学校重点科研项目资助(17B520002；18A520013)；河南省高等学校青年骨干教师培养计划资助项目(2018GGJS196)；河南省教育科学十三五规划课题资助项目(2018-JKGHYB-0407)；河南省教师教育课程改革研究项目资助(2019-JSJYZD-041)

作者简介：张红军(1979–)，男，硕士，副教授，主要研究方向为计算机网络、大数据技术。email:chunhuaw0801@163.com

handshake LEACH，ah-LEACH)协议。该协议通过选取最优百分比的簇头，最小化节点的能耗以实现网络负载平衡。每个被选取出的簇头使用四次握手消息来实现与基站的双向身份认证，其中握手消息是使用高级加密标准(Advanced Encryption Standard，AES)加密。所给协议与已有协议相比，在安全性、鲁棒性、抵御各种攻击、握手持续时间等方面具有较优性能。

1　相关工作研究

近些年，研究人员对网络协议的安全性进行了比较多的研究。文献[6]提出了一种基于状态信息的身份认证协议，在身份认证的同时可对节点的运行状态进行判断并发送异常报警，但该方法会增加数据传输延迟时间。文献[7]提出了一种基于区块链技术的身份验证机制，但该方法能耗较大且传感器节点大多并不具备生成区块记录的能力。在基于簇的分层路由协议中，LEACH 是一种具有开创性的协议，其将传感器场划分为簇的较小地理区域，但对簇头进行概率性选择存在潜在的风险，即后续轮次中低能量节点会被选为簇头。文献[8]提出一种新颖的基于非均匀分簇的无线传感器网络多跳路由协议，其核心是一个用于组织网络拓扑的能量高效的非均匀分簇算法。文献[9]提出一种考虑安全数据融合的安全 LEACH(sec-LEACH)协议，该协议使用 E-G 随机密钥预分配方法生成一个较大的密钥池，向每个节点分配这些密钥的子集，同时结合了分簇路由协议和数据汇聚协议，以提高基于簇的分层式无线传感器网络的安全性和效率。文献[10]提出了一种基于改进 LEACH(imp-LEACH)协议的簇间多跳路由算法，该协议引入能量因子和距离因子，以修正 LEACH 协议的阈值函数，在簇头与簇头之间形成一个优化路径。

2　基于令牌的簇头选举

所用网络模型由随机部署的异构传感器节点[11]组成，包括 100 个初始能量为 1 J 的普通节点和 5 个初始能量为 5 J 的高能量节点，所有节点均在 100 m×100 m 的地理区域中，每个普通节点均分配一个令牌和一个预共享密钥 λ_i，令牌用于基站和簇头间提名包与确认消息的安全交换，λ_i 用于网络内邻近节点与其可能簇头间的双向身份验证。网络部署模型如图 1 所示。

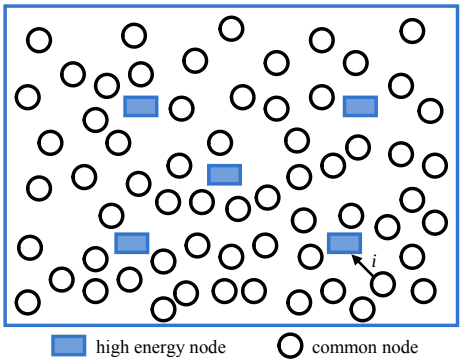

Fig.1 Schematic diagram of network deployment phase
图 1　网络部署阶段示意图

起始时，每个普通节点 i 创建一个控制包并发送至距离其最近的高能量节点。该数据包中包含节点 i 的剩余能量 E_i 与标识 ID_i。距离节点 i 最近的高能量节点的位置计算如式(1)：

$$d_{\mathrm{H}}=\sqrt{\left(x_{\mathrm{H}}-x_i\right)^2-\left(y_{\mathrm{H}}-y_i\right)^2} \tag{1}$$

每个高能量节点在其邻近节点中收集这些数据包，对 E_i 与 ID_i 进行检索，将包含了这些数值的控制包向基站广播，随后进入睡眠模式，在下一轮开始时再唤醒。基站接收数据后检索每个控制包的 E_i 与 ID_i。其中，平均能量阈值计算如式(2)：

$$\bar{E}=\sum_{i=1}^{N}\frac{E_i}{N} \tag{2}$$

式中：$\bar{E}$ 是所有 N 个正常节点的平均能量阈值；节点数 N 等于 100。任何普通节点 i 的 E_i 超过或等于 $\bar{E}$ 时，即有资格在某个特定轮中被选为簇头。网络部署后的启动初始轮次，所有节点拥有几乎相同的剩余能量，即此时 $E_i\approx\bar{E}$。所给协议能够基于极低 ΔE 数值选出簇头。在基于簇的分层路由协议 $E_i\geqslant\bar{E}$ 中，各轮次可能会有较多节点满足条件，这些节点都是簇头的提名节点，然后基站从这些提名节点中选出 k_{best} 个簇头。由于簇头能量会因资源密集型的任务迅速耗尽，k_{best} 过小会使基于簇的分层式网络的性能下降，k_{best} 过大则会因较低的数据融合率造成基于簇的分层式网络效率较低[12]。所给协议的 k_{best} 为 5%。

每轮中，基站向当选簇头广播提名包，包括簇头标识 ID_{cls} 和邻近节点标识 ID_{NB}，两种标识均在提名包的有效负载内传输，每个提名包的报头均有一个 16 位的令牌来确保 ID_{cls} 和 ID_{NB} 的安全传输，同时基站对每个当选簇头生成一个令牌。每个簇头接收提名包后检查其附加的令牌，若该令牌与簇头的令牌匹配，则簇头对其邻近节点的附加标识 ID_{add} 进行检索。每个簇头必须确认收到了一个提名包，这需要簇头创建一个附加其令牌的确认消息发送到基站。攻击者有可能会拦截到一个或多个提名包，但其无法重新生成检索附加标识所需的令牌。此

外，无线传感器网络的认证还包括消息认证码(挑战/应答机制)、添加生物因素(指纹)、临时证书、可信计算、第三方签名等方法。其中，消息认证码、添加生物因素的认证方法增加了单个传感器节点的资源消耗，将会缩短无线传感器网络寿命周期；而临时证书、可信计算、第三方签名的认证方法均需要一个网关或第三方可信任实体进行认证，客户端节点和服务器节点不能直接相互认证，不适用于所给基于有效负载握手协议。因此，所给协议较适宜采用基于令牌的认证方法。

3 所给协议设计

成功接收到广播消息后，每个邻近节点就发起簇的形成。所给协议采用 128 bit 的 AES 加密算法完成身份验证，该加密模式所需资源较少，对于节点生成的数据极为有利，同时可使节点在遭受攻击前拥有足够时间卸载数据，但需要复杂的软硬件平台。为此，所给协议使用基于有效负载的轻量级双向身份验证技术实现在每条信息的有效负载内进行身份验证，如图 2 所示。每个邻近节点与一个服务器节点在四条超轻量级的握手消息中完成身份验证。一旦得到认证，每个邻近节点被允许发送数据到相应簇头。所给协议的双向身份验证包括会话发起、服务器节点质询、客户端节点响应和质询、服务器节点响应四个阶段。

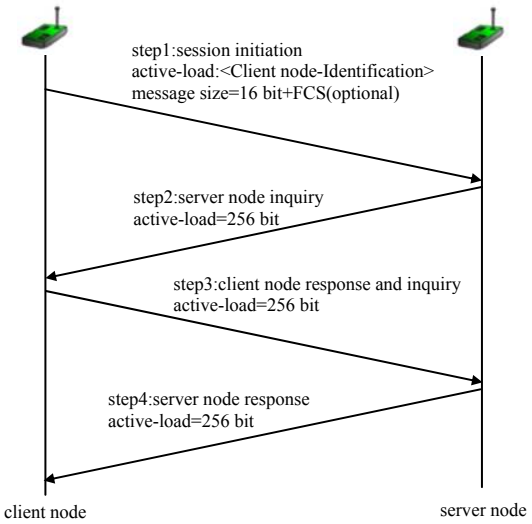

Fig.2 Two-way authentication of the proposed protocol
图 2 所给协议的双向身份验证

会话发起阶段，每个邻近节点 i 创建一个包含 ID_i (8 bit 源节点标识)与 ID_s (8 bit 簇头的目标节点标识)的加入请求消息。无论合法节点或恶意节点，每个邻近节点最多与服务器协商四次会话发起请求。其中 ID_i 在有效负载内传输，ID_s 在每个加入请求消息的报头内传输。有效负载之后是一个可选的帧校验序列[13]，作为尾部附加，用于错误检测和校正。

服务器节点质询阶段，每个服务器在接收的加入请求消息的报头中检索 ID_s，在该消息的有效负载中检索 ID_i。若 ID_s 与服务器的标识匹配，则表示该加入请求消息是传送给该服务器的，反之，该加入请求消息将被丢弃。为了进行会话协商，ID_i 必须与提供给该服务器标识池内的一个标识匹配，且仅在 $ID_i \in ID_{add}$ 的情况下才会出现匹配。每个服务器从有效负载中检索 ID_i，并搜索一个匹配的预共享密钥 λ_i。为实现身份验证，ID_{add} 的每个 ID_i 都与一个 λ_i 相关联。服务器若发现匹配就将使用 AES 算法发送加密后的有效负载作为回应。为创建一条质询消息，服务器创建一个 128 bit 的伪随机临时数 η_{serve} 和一个 128 bit 的潜在公共会话密钥 μ_{key}。临时数 nonce 是在整个加密通信过程中仅被客户端节点或服务器节点使用一次的一个临时数字。采用 μ_{key} 和 η_{serve} 生成一个加密的有效负载作为质询发送至客户端节点。首先用 λ_i 与 μ_{key} 执行异或运算得到 128 bit 的 ψ_{syn}，然后将其附加于 η_{serve}，并用 λ_i 加密，即可生成一个 256 bit 的有效负载 $\gamma_{ser-load}$，如式(3)所示：

$$\begin{cases}\psi_{syn}=\lambda_i \oplus \mu_{key}\\ \gamma_{ser-load}=\left\{\lambda_i,\left(\psi_{syn}|\eta_{serve}\right)\right\} AES128\end{cases} \tag{3}$$

客户端节点响应和质询阶段，客户端节点需要对加密的有效负载 $\gamma_{ser-load}$ 解密，以检索潜在的会话密钥 μ_{key}。若客户端节点成功完成解密，将得到正确的 η_{serve} 和 μ_{key}。根据互联网威胁模型[14]，入侵者只能窃听 η_{serve} 和 μ_{key}，但不能窃听 λ_i。客户端节点使用自己的 λ_i 对有效负载解码，成功解码后即完成了对自己的身份验证。因双向身份验证要求两方都要得到验证，所以服务器也需要对自己进行身份验证。与服务器相似，客户端节点生成一个新的加密有效负载作为一个质询发送到服务器节点。首先用 η_{serve} 和 λ_i 执行异或运算得到 128 bit 的 ψ_{syn}，然后将其附加于 η_{cli}，并用 μ_{key} 加密，即可生成一个 256 bit 的有效负载 $\gamma_{cli-load}$，如式(4)所示：

$$\begin{cases}\psi_{syn}=\eta_{serve} \oplus \lambda_i\\ \gamma_{cli-load}=\left\{\mu_{key},\left(\psi_{syn}|\eta_{cli}\right)\right\} AES128\end{cases} \tag{4}$$

服务器节点响应阶段，服务器节点对客户端节点的质询是通过解密有效负载 $\gamma_{cli-load}$ 找到 η_{serve}。若找到 η_{serve}，则对服务器节点来说，该客户端节点已成功完成了身份验证。如式(5)所示，服务器检索 η_{serve}，再将 η_{serve} 附加到 μ_{key} 上并以 λ_i 进行加密，以创建出一个自己的 256 bit 加密有效负载 $\gamma_{ser-load}$，然后将其作为对客户端节点质询的响应传送回客户端节点。

$$\gamma_{\text{ser-load}}=\left\{\lambda_i,\left(\eta_{\text{serve}}|\mu_{\text{key}}\right)\right\}AES128 \tag{5}$$

此时由于客户端节点 i 已成功通过身份验证，有资格将数据发送到服务器节点，但客户端节点还需要对服务器节点的真实性进行验证，所以正在进行的会话从会话协商阶段转变为对验证服务器节点阶段，通过解密服务器节点发送的有效负载 $\gamma_{\text{ser-load}}$ 找到 η_{cli}，最终客户端节点和服务器节点完成双向身份验证，并在一个公用会话密钥 μ_{key} 上进行数据包交换。在此阶段，服务器为其簇内每个成员节点 i 创建一个排程表，并向簇内每个成员节点分配时分多址时隙，这些时隙用于无争用通信，对每个节点的占空比进行排程。一旦客户端节点和服务器节点都通过身份验证，即完成了簇建立阶段，则启动稳态阶段。在稳态阶段，每个簇头从其成员节点中采集数据并聚合，然后发送给网络内部或外部的基站。所给协议的操作流程如图 3 所示。

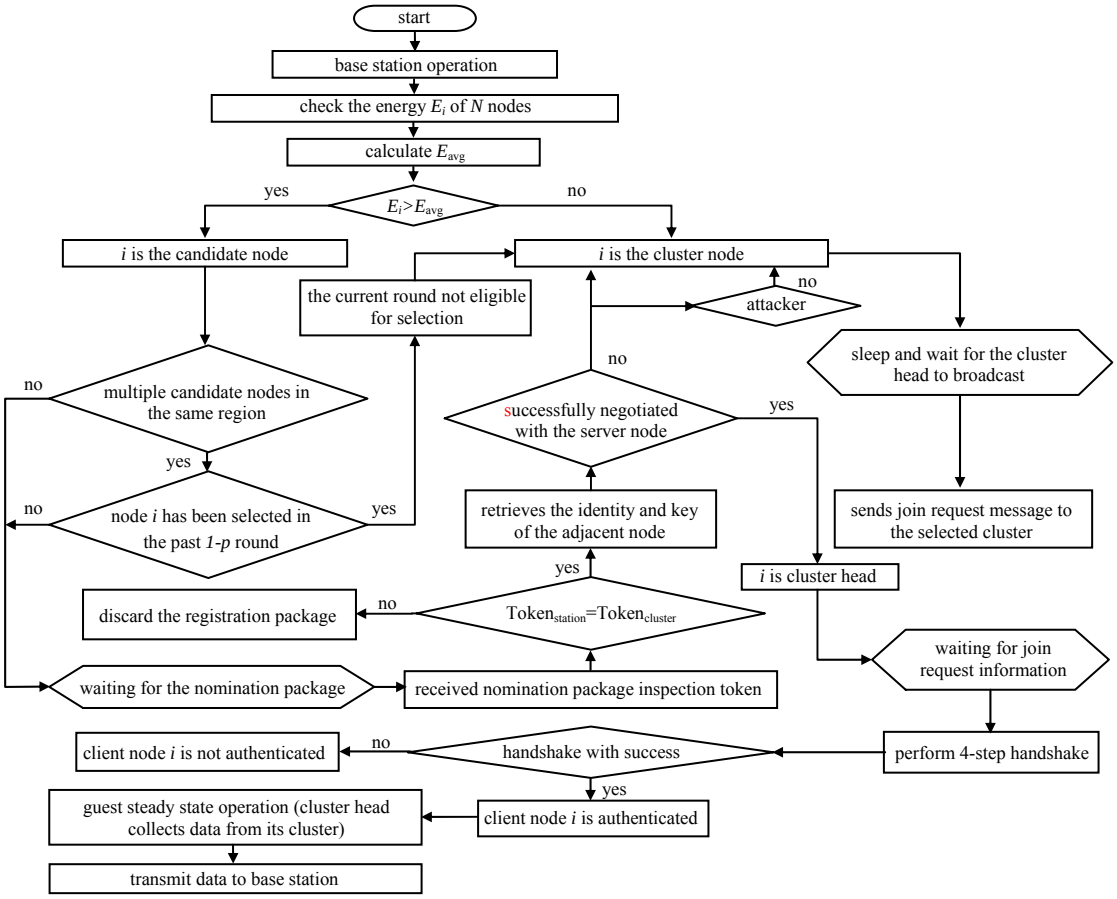

Fig.3 Flow of the proposed protocol
图 3 所给协议的流程图

4　仿真实验分析

采用 Matlab 2011a 平台对所给协议进行仿真实验分析，其中网络模型包括 100 个普通节点和 5 个高能量节点，部署在一个 100 m×100 m 的区域内。

4.1 安全性分析

为了进行安全性分析，首先确保节点到节点的通信数据真实、保密和新鲜[15]。表 1 给出了各方法在安全性上的比较。ah-LEACH 使用两步程序进行双向身份验证，imp-LEACH 仅将网络划分为簇但没有进行任何身份验证，sec-LEACH 使用消息验证码(Message Authentication Code，MAC)进行身份验证，通过利用密钥池对每条消息使用的密钥进行加密，接收方在成功解密该消息后才可知其是否来自传感器网络的合法节点。ah-LEACH 采用有效负载的方法确保消息的保密性，imp-LEACH 未提供数据的保密性，sec-LEACH 同样采用 MAC 进行数据的保密。ah-LEACH 和 sec-LEACH 方案都使用临时数 nonce 来确保数据的新鲜性，而 imp-LEACH 不能确保数据的新鲜性。比较可以看出，所给 ah-LEACH 协议安全性能更优。

表 1 安全性分析
Table1 Safety analysis

security services	imp-LEACH	sec-LEACH	ah-LEACH
authentication	no	MAC	verified by 2 steps
confidentiality	no	MAC	active-load
freshness	no	random number	random number

4.2 抵御各种攻击的鲁棒性

表 2 给出了 ah-LEACH 协议抵御各种攻击和恶意活动的鲁棒性。ah-LEACH 通过伪随机数 R_i 生成 η_{cli} 和 η_{serve}，并附加到一个定时器 T_i 上。T_i 和 R_i 的结合确保了攻击者难以对过期的数据包进行重放。R_i 的伪随机性质确保了 η_{cli} 和 η_{serve} 是不可重现的，定时器 T_i 则确保了 η_{cli} 和 η_{serve} 的不可预测性。sec-LEACH 使用散列函数 H 和密钥环 k_r 来抵御重放攻击，而 imp-LEACH 难以提供任何攻击的防御手段。除可较好地防御重放攻击外，ah-LEACH 在抵御资源耗竭攻击和拒绝服务攻击时也具备较好的鲁棒性。ah-LEACH 使用 λ_i 对来自任何一个邻近节点的会话发起请求进行认证，λ_i 不存在于服务器表中，这确保了任何未验证的邻近节点不能与某个已知服务器节点建立一个或多个连接，所以服务器的资源不会受到损耗，节点具有防篡改性。而 sec-LEACH 和 imp-LEACH 没有提供任何应对资源耗竭攻击和 Sybil 攻击的防御手段。

表 2 抵御网络攻击的鲁棒性

Table2 Robustness against network attacks

attack methods	imp-LEACH	sec-LEACH	ah-LEACH
replay	no	yes	yes
resource depletion	no	no	yes
Sybil	no	no	yes

4.3 握手持续时间

表 3 给出了各协议在不同簇规模下的平均握手持续时间比较。可以看出，sec-LEACH 的平均握手时间远高于 ah-LEACH，这是由于 sec-LEACH 使用 LEACH 协议的随机分布式底层簇分层方法，使用概率阈值进行簇头选举，但簇头因没有邻近节点的局部知识，则需耗费更长的时间对邻近节点进行身份验证。在 ah-LEACH 中，簇头则使用其邻近节点的局部知识来完成身份验证，每个簇头只需在自己的表中查找，即能验证一个会话发起请求是否有效，λ_i 的存在使得每个簇头均能通过 4 步握手协商实现双向身份验证。

表 3 握手持续时间

Table3 Handshake duration

cluster size	for sec-LEACH/ms	for ah-LEACH/ms
15	4 332.46	2 071.28
20	4 992.09	2 166.19
25	5 321.07	2 389.13

4.4 能量消耗

ah-LEACH 协议使用的簇形成的集中式方法与 imp-LEACH 协议的有些类似。但 imp-LEACH 没有提供安全的数据传输方法，易受很多恶意攻击。图 4 给出了 ah-LEACH 与 imp-LEACH 的平均能耗比较。可以看出，ah-LEACH 在大部分轮次中的平均能耗略高于 imp-LEACH。但 ah-LEACH 在能耗方面的增加是可以忽略的，这是因为其提供了进行身份验证和数据保护的一整套操作。而 imp-LEACH 则没有提供安全特性，且簇头的选取过于复杂。imp-LEACH 使用模拟退火算法进行簇头选取并形成簇，这个簇形成和簇头选取方法会造成过长的延时和较多的能耗。ah-LEACH 则使用一个简单的方法进行簇头选取，其消耗的能量较少，同时能够抵御各种恶意攻击。

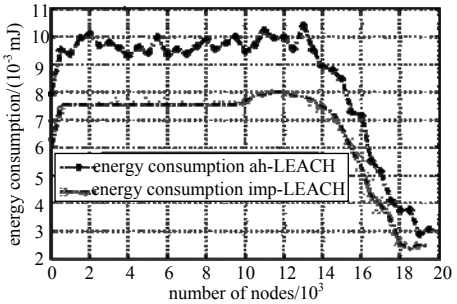

Fig.4 Average energy consumption
图 4 平均能量消耗

4.5 网络平均吞吐量

网络平均吞吐量是指在基站成功接收的数据包总数与发送数据包总数的比率。图 5 给出了 ah-LEACH 的网络平均吞吐量。ah-LEACH 在簇头选取阶段和簇形成的过程中都提供了身份验证。但即使 ah-LEACH 进行两级身份验证，数据包成功接收的百分比在大多数轮中依然高得多。在不存在身份验证的情况下，传送到基站的数据包数量会高得更多。虽然 ah-LEACH 提供了一个具有鲁棒性和防御性的底层网络解决方法，但是部署区域的性质和通信链路的质量也在很大程度上会导致数据包处理延迟、数据包丢失和排队延迟，增加重传尝试的次数，从而降低服务质量。

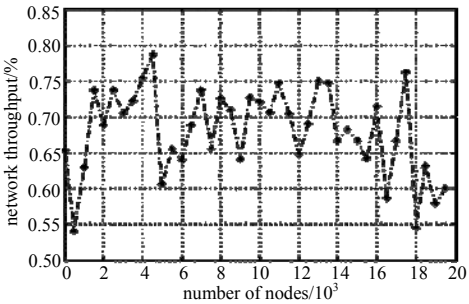

Fig.5 Average network throughput
图 5 平均网络吞吐量

5 结论

通过基于簇的分层式无线传感器网络给出了一个轻量级的双向身份验证协议，所给协议利用基于簇的分层式体系结构的高能效性实现能耗最小化，并利用双向身份验证方案的轻量级特性确保了安全性。所给协议在抵

御攻击的鲁棒性、握手持续时间、平均能耗和网络平均吞吐量等多个性能指标上对 ah-LEACH 和现有其他协议进行了比较。结果表明 ah-LEACH 能够很好地抵御重放、拒绝服务、Sybil 和资源耗竭等多种攻击，且平均握手持续时间比 sec-LEACH 短得多，能以 sec-LEACH 所需时间的大约一半建立身份验证会话。所给 ah-LEACH 使用令牌来完成对基站和簇头的身份验证，但在一些任务中可使用其他替代方法来达到这个目的，以进一步最小化能耗。下一步将测试使用随机分布式基于簇的分层式结构(类似于 LEACH)。

参考文献：

[1] 徐晶晶,张欣慧,许必宵,等. 无线传感器网络分簇算法综述[J]. 计算机科学, 2017,44(2):31-37. (XU Jingjing,ZHANG Xinhui,XU Bixiao,et al. Survey of clustering algorithms for wireless sensor networks[J]. Computer Science, 2017,44(2):31-37.)

[2] 刘春刚,刘松林,杨文超,等. 无线传感器网络中基于 APIT 与 DV-HOP 的混合定位算法[J]. 太赫兹科学与电子信息学报, 2017,15(3):432-437. (LIU Chungang,LIU Shonglin,YANG Wenchao,et al. Hybrid localization algorithm based on APIT and DV-HOP in wireless sensor networks[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(3):432-437.)

[3] 姜彬彬,于寒. 综合负载均衡与能量消耗的无线传感器网络分簇算法[J]. 吉林大学学报(理学版), 2017,55(6):1552-1556. (JIANG Binbin,YU Han. Clustering algorithm for wireless sensor networks with integrated load balancing and energy consumption[J]. Journal of Jilin University(Science Edition), 2017,55(6):1552-1556.)

[4] 李健. 基于无线传感器网络的安全网络运行环境构建[J]. 计算机工程与应用, 2017,53(22):66-70. (LI Jian. Secure network running environment construction scheme for wireless sensor network[J]. Computer Engineering and Applications, 2017,53(22):66-70.)

[5] 池涛,严浩伟,陈明. 无线传感器网络 LEACH 算法的研究与改进[J]. 小型微型计算机系统, 2018,39(10):2222-2225. (CHI Tao,YAN Haowei,CHEN Ming. Research and improvement on LEACH algorithm for wireless sensor networks[J]. Journal of Chinese Computer Systems, 2018,39(10):2222-2225.)

[6] 刘静,赖英旭,杨胜志,等. 一种面向 WSN 的双向身份认证协议及串空间模型[J]. 计算机科学, 2019,46(9):169-175. (LIU Jing,LAI Yingxu,YANG Shengzhi,et al. Bilateral authentication protocol for WSN and certification by strand space model[J]. Computer Science, 2019,46(9):169-175.)

[7] TAI Weiliang,CHANG Yafen,LI Weihan. An IoT notion-based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks[J]. Journal of Information Security and Applications, 2017, 34(2):133-141.

[8] 黄廷辉,伊凯,崔更申,等. 基于非均匀分簇的无线传感器网络分层路由协议[J]. 计算机应用, 2016,36(1):66-71. (HUANG Tinghui,YI Kai,CUI Gengshen,et al. Hierarchical routing protocol based on non-uniform clustering for wireless sensor network[J]. Journal of Computer Applications, 2016,36(1):66-71.)

[9] RAHAYU T M,LEE S G,LEE H J. A secure routing protocol for wireless sensor networks considering secure data aggregation[J]. Sensors, 2015,15(7):127-138.

[10] 陈炳才,么华卓,杨明川,等. 一种基于 LEACH 协议改进的簇间多跳路由协议[J]. 传感技术学报, 2014,27(3):373-377. (CHEN Bingcai,YAO Huazhuo,YANG Mingchuan,et al. A inter-cluster multi-hop routing protocol improved based on LEACH protocol[J]. Chinese Journal of Sensors and Actuators, 2014,27(3):373-377.)

[11] 闫丽丽,昌燕,张仕斌. 异构传感器网络的用户认证和密钥协商协议研究[J]. 电子科技大学学报, 2017,46(1):55-60. (YAN Lili,CHANG Yan,ZHANG Shibin. Authentication and key agreement scheme for heterogeneous wireless sensor networks[J]. Journal of University of Electronic Science and Technology of China, 2017,46(1):55-60.)

[12] 甄岩,李兴,王汝言. 带有群体智能的能量感知分层数据转发机制[J]. 系统工程与电子技术, 2017,39(9):2109-2118. (ZHEN Yan,LI Xing,WANG Ruyan. Swarm intelligence based energy-aware hierarchical packet forwarding mechanism[J]. Systems Engineering and Electronics, 2017,39 (9):2109-2118.)

[13] 袁征,冶晓隆,郭超. 基于 FPGA 的 10G 以太网并行 CRC 设计[J]. 计算机工程与设计, 2014,35(5):1510-1515. (YUAN Zheng,YE Xiaolong,GUO Chao. Implementation of parallel CRC for 10 gigabit Ethernet based on FPGA[J]. Computer Engineering and Design, 2014,35(5):1510-1515.)

[14] XING Jie,BI Hongjun,LIU Yun. Research on security threat assessment method based on the attack tree model of the Internet of Things[J]. Journal of Convergence Information Technology, 2013,8(3):653-658.

[15] CHENG Shuhong,WANG Yi,ZHANG Wenke. Research on the cooperative game model of Internet of Things based on mobile node-to-mobile node communication[J]. Journal of Computational and Theoretical Nanoscience, 2016,13(12): 9607-9611.