

基于 LEACH 协议的 WSN 共享密钥管理方案的研究

范敏^{1,2}, 蒋珏³, 汤琳¹, 仇莫然¹, 李超¹

(1. 绵阳师范学院信息工程学院, 四川 绵阳 621006;
2. 北京邮电大学智能通信软件与多媒体北京市重点实验室, 北京 100876;
3. 绵阳师范学院图书馆, 四川 绵阳 621006)

摘要: 为了使层次式无线传感器网络传输更安全、节点寿命更长、网络运行效率更高, 提出了一种基于 LEACH 协议的 WSN 共享密钥管理方案。该方案具有很好的方案完整性与时效性、动态密钥安全性、节点安全独立性和密钥生存有效性, 也具备抗中间人攻击、DDoS 攻击等风险的能力, 而且分发共享密钥消耗的能量较低, 网络运行效率较高。

关键词: LEACH 协议; 无线传感器网络; 共享密钥; 路由协议; 密钥管理方案

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00084

Study on shared key management scheme for WSN based on LEACH protocol

FAN Min^{1,2}, JIANG Jue³, TANG Lin¹, QIU Mo-ran¹, LI Chao¹

(1. School of Information Engineering, Mianyang Normal University, Mianyang 621006, China;
2. Beijing Key Laboratory of Intelligent Telecommunications Software and Multimedia,
Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Library, Mianyang Normal University, Mianyang 621006, China)

Abstract: In order to achieve transmission safety, nodes longer life and higher operation efficiency for the hierarchical wireless sensor network, a shared secret key management scheme for WSN based on LEACH protocol was proposed. The scheme has good integrity and timeliness, dynamic key safety, node security independence and key survival, and also has the ability to resist the man-in-the-middle attack, DDoS attacks and so on. Furthermore, energy consumption is lower to distribute shared key, and efficiency is higher to operate network.

Key words: LEACH protocol, wireless sensor network, shared key, routing protocol, key management scheme

1 引言

近年来, 随着物联网 (IOT, Internet of things) 应用需求的快速增加, 无线传感器网络 (WSN, wireless sensor networks) 也得到了迅速的发展, 被广泛应用于环境监控、森林防火、国土安全、军事、航空管制、智能家居等诸多

领域^[1]。无线传感器网络不同于其他网络, 它由大量成本低廉、具有数据处理和传输以及一定存储和计算能力、并以 ad hoc 方式通信的无线传感器智能节点组成, 这些节点作为物联网感知层的感知设备, 往往被部署在无人值守、易于遭到攻击和破坏的恶劣环境中, 因而无线传感器网络的安全问题至关重要。由于无线传

收稿日期: 2016-06-17; 修回日期: 2016-07-09。通信作者: 范敏, afreefox@sina.com

基金项目: 四川省教育厅自然科学基金资助项目 (No.15ZB0284)

Foundation Item: The Natural Science Foundation of Sichuan Provincial Department of Education (No.15ZB0284)

感器本身具有计算能力、存储能力和能量受限、节点易失效的特点，无线传感器网络的安全面临与传统网络不同的挑战。无线传感器网络提供的安全性高度依赖于网络节点自身的物理安全性和节点相互之间通信的安全性，而通信的安全性体现在安全通信机制和密钥的安全性。可见，一旦通信机制确定，解决网络的密钥管理问题就是解决网络传输安全问题的关键所在^[2]。因此，研究无线传感器网络中的密钥管理问题具有非常重要的意义。

2 典型的无线传感器网络路由协议

无线传感器网络不同于有线网络，其节点分布广泛，且往往能量、计算能力和存储能力有限，路由情况需要随着节点状况的变化而变化。无线传感器网络节点之间的通信与其路由机制有关，路由协议决定其网络结构。针对不同应用的特点，人们研究了许多的路由协议。这些路由协议可以大致分为 5 类，即泛洪式路由协议、层次式路由协议、以数据为中心的路由协议、基于位置信息的路由协议、基于 QoS 的路由协议^[3]。各类无线传感器网络路由协议中常见的协议如表 1 所示。

表 1 常见的无线传感器网络路由协议

协议类别	协议名称
层次式路由协议	LEACH
	TEEN
	PEGASIS
以数据为中心的路由协议	SPIN
	DD (directed diffusion)
	Rumor
泛洪式路由协议	Flooding
	Gossiping
基于位置信息的路由协议	GPSR
	GEAR
基于 QoS 的路由协议	SAR
	SPEED

表 2 从生命周期、可扩展性、路径选择（单跳还是多跳）、能量感知、数据聚集、位置信息（是否需要节点的地理位置信息）、信息存储、可移动的节点、实时性、可靠性（容错能力）等方面给出了无线传感器网络路由协议性能和特点的比较结果^[3]。

从表 2 可以看出，不同路由协议各项指标表现不同，各有优劣。由于无线传感器网络路由协议的设计与应用密切相关，单一的路由协

表 2 无线传感器路由协议性能和特点的比较

协议	生命周期	可扩展性	路径选择	能量感知	数据聚集	位置信息	信息存储	可移动的节点	实时性	可靠性
Flooding	短	差	多跳	无	无	无需	无	传感节点 汇聚节点	差	较好
Gossiping	较长	差	多跳	无	无	无需	无	传感节点 汇聚节点	差	较好
LEACH	较长	差	单跳	有	有	无需	有	无	差	较好
TEEN	长	好	多跳	有	有	无需	有	无	好	差
PEGASIS	长	差	多跳	有	有	无需	有	无	差	差
SPIN	长	差	多跳	无	有	无需	无	传感节点 汇聚节点	差	差
DD	长	好	多跳	有	有	无需	有	无	好	差
Rumor	长	好	多跳	有	有	无需	有	汇聚节点	差	较好
GPSR	较长	好	多跳	无	无	需要	无	传感节点	差	较好
GEAR	长	好	多跳	有	无	需要	无	传感节点	差	较好
SAR	较长	差	多跳	有	无	无需	有	无	好	好
SPEED	长	差	多跳	有	无	需要	有	无	好	好

议不能满足各种应用需求^[3]。在实际应用中究竟选择哪一种路由协议更好, 必须根据具体应用和各路由协议的特点, 结合相应的安全协议进行综合考虑, 才能确保在各传感器节点和汇聚节点之间安全、可靠地传输数据。为了在保证层次式无线传感器网络传输数据的同时, 以适合无线传感器网络节点特点的方式提高数据传输的安全性, 本文提出了一种基于 LEACH (low-energy adaptive clustering hierarchy) 协议的 WSN 共享密钥管理方案。

3 LEACH 协议及其工作原理

LEACH 协议^[4]是一个在无线传感器网络中提出的层次式路由协议, 是一个低功耗、自适应集簇层次型协议。该协议将传感器节点分成簇, 每个传感器节点都将数据传给本簇内随机选出的簇头节点, 由簇头节点进行数据融合处理后再传给汇聚节点。由于均衡了网络中节点的能耗, 与一般的多跳路由协议和静态聚类算法相比, LEACH 路由协议可以将无线路由器的生命周期延长 15%^[5]。

随着无线传感器节点能量的变化, LEACH 在运行过程中按照一定周期不断地循环执行簇 (cluster) 的重构过程。一个簇重构过程称为一轮, 每轮分成 2 个阶段, 即簇的建立阶段和传输数据的稳定阶段。

簇的建立过程可分成 4 个阶段: 簇头 (cluster-head) 节点选择、簇头节点广播、簇头节点建立和调度机制的生成。簇头节点的选择, 要根据网络中所需要的簇头节点总数和迄今为止每个节点已成为簇头节点的次数来决定。具体的选择办法是每个传感器节点在 0~1 随机选择一个值, 如果选定的值小于某一个阈值, 那么这个节点就成为簇头节点。选定簇头节点后, 该簇头节点通过广播告知整个网络。网络中的其他节点根据接收信息的信号强度决定自己应该从属的簇, 并通知相应的簇头节点, 完成簇的建立。最后, 簇头节点采用 TDMA 方式为簇中每个节点分配向本簇头节点传递数据的时间点。通过 LEACH 路由协议建立的是一个层次式无线传感器网络, 结构如图 1 所示。

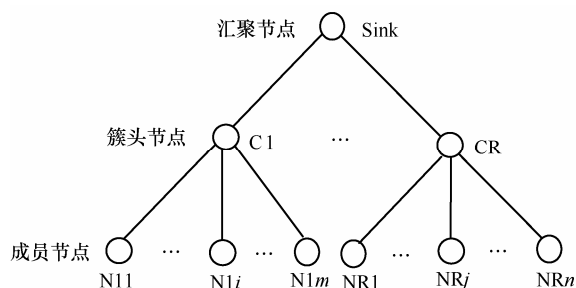


图 1 层次式无线传感器网络

簇建立后, 就进入传输数据的稳定阶段。在每个簇内, 簇头节点接收各成员节点采集、传输的数据, 并进行必要的融合; 各个簇头节点采用 CSMA 协议通信竞争通道, 获得通道的簇头节点将数据发送给汇聚节点 (Sink)。

每隔一定时间, 整个网络重新回到簇的建立阶段, 开始新一轮的选择簇头阶段。每个簇都使用不同的 CDMA 码进行通信, 以减少属于其他簇的节点对本簇节点通信的干扰^[6]。为了节省资源开销, 稳定阶段的持续时间要大于建立阶段的持续时间。

LEACH 协议在运行中有 3 个关键点: 1) 周期性地重建层次式路由结构, 各个节点在每轮中的作用不一定相同; 2) 节点建立簇的过程中, 当簇头节点选定后, 簇头节点将广播自己成为簇头节点的事实, 汇聚节点将监听到这个广播; 3) 簇的成员节点将按照接收到的广播信号强弱选择自己应加入的簇, 并向该簇的簇头节点通知自己成为该簇成员的事实。以上关键点正好为基于 LEACH 协议的 WSN 共享密钥管理方案的实施提供了必要条件, 也是该方案实施的主要过程。

4 密钥管理方案

鉴于无线传感器节点自身计算能力和存储能力低以及能量有限的特点, 节点通过对称密钥算法提供节点之间数据传输的安全性具有明显的现实意义。根据 LEACH 协议的工作原理, 在建立簇的同时, 可以实现簇成员节点与其簇头节点之间、簇头节点与汇聚节点之间共享密钥的分配。

4.1 系统模型

接下来以已经建立的由一个汇聚节点 Sink、一个簇头节点 C1 及其成员节点 {N11, ..., N1i, ..., N1m} 组成的层次式模型为例, 说明基于 LEACH

的 WSN 共享密钥管理方案的工作原理，模型见图 1 左支部分。

4.2 模型节点的说明

1) 每个节点都预置初始密钥 $mkey$ ，并得到了很好保护。

2) 每个节点都有一个 ID 号。

3) 每个节点都可以存储类似数据库表结构 $\{recID, nodeID, key, isHeader\}$ 的数据。其中， $recID$ 表示记录号，记录号随记录数的增多从 1 开始按自然数逐个增加； $nodeID$ 表示节点编号； key 表示传输数据时对数据进行加密和解密使用的共享密钥； $isHeader$ 表示是否为本节点与上一层通信的对应节点，取值为 0 或者 1，1 表示是，0 表示否。

4) 每个节点都有一个加密函数 $F(Plaintext, key)$ 和解密函数 $F^{-1}(Ciphertext, key)$ ，分别用于对传输的数据进行加密和解密。其中， $Plaintext$ 表示明文字符串， $Ciphertext$ 表示密文字符串， key 表示共享的加、解密密钥。

5) 每个节点都有一个数据融合函数 $P(datas[])$ ，用于对 $datas$ 数组元素中的数据进行融合。

6) 每个节点都可以进行异或运算（运算符为“ $\oplus$ ”）和散列函数运算（函数 $Hash()$ ）。

7) 每个节点都可以产生伪随机数 $r \in R\{0,1\}^{SL}$ ，其中， SL 为安全密钥长度。 r 作为节点对之间共享的会话密钥。

8) 本文方案的实施不改变原来 LEACH 协议过程，只是增加 LEACH 协议相应阶段中传输的内容。

4.3 符号定义

$\oplus$ ：异或运算符。

AND：与运算符。

||：连接运算符。

//：说明开始标志。

4.4 方案实现逻辑

1) Sink $\rightarrow$ all 过程：新一轮建立层次式结构网络开始，汇聚节点 Sink 广播信息。

Sink：处理逻辑

①产生伪随机数 r_0 // 作为汇聚节点与簇头节点之间的共享密钥。

②计算：START=11111111； $A=Hash(mkey||START)$ ； $B=Hash(mkey||r_0)$ ； $C=ID_0 \oplus mkey$ ； $D=$

$r_0 \oplus mkey||START=11111111$ 作为新一轮网络构建开始的标志

③Sink 广播信息 (A, B, C, D)。

2) 所有非汇聚节点处理 Sink 的信息。

all nodes：处理逻辑

①计算： $key=D \oplus mkey$ ；

IF ($A=Hash(mkey||11111111)$) AND ($B=Hash(mkey||key)$) // A, B 来自合法节点广播，且是新一轮网络构建开始

②计算： $ID=C \oplus mkey$ ； $isHeader=0$ 。

③存入 Sink 有关信息： $[nodeID, key, isHeader]=[ID, key, isHeader]$ 。

IF 本节点 C_i 为簇头节点

④调用 $C_i \rightarrow all$ 过程 // 以下以 $C_1 \rightarrow all$ 过程为例
ENDIF

ENDIF

3) $C_1 \rightarrow all$ 过程： C_1 节点成为簇头节点后，广播自己成为簇头节点的事实。

C_1 ：处理逻辑

①产生伪随机数 r_1 。

②修改表的第一条记录的 key 字段值为 r_1 、 $isHeader$ 字段值为 1 // 该记录对应节点为上一层节点

③计算： $E=Hash(mkey||key)$ ； $F=Hash(mkey||r_1)$ ； $G=r_1 \oplus key$ ； $H=ID_1 \oplus r_1$ 。

④ C_1 广播信息 (E, F, G, H)。

4) Sink 节点处理 C_1 的信息

Sink：处理逻辑

IF $E=Hash(mkey||r_0)$ // E 来自于簇头节点

①计算：START=00000000； $k_tmp=G \oplus r_0$ ； $ID=H \oplus k_tmp$ ； $isHeader=0$ 。

②存入簇头节点 C_1 有关信息： $[nodeID, key, isHeader]=[ID, k_tmp, isHeader]$ 。

ENDIF

5) $N_{1i} \rightarrow C_1$ 过程：节点成为某簇成员后，向簇头节点 C_1 通告自己加入簇的事实。

N_{1i} ：处理逻辑

①计算： $k_tmp=G \oplus key$ 。

IF ($E=Hash(mkey||key)$) AND ($F=Hash(mkey||k_tmp)$) // E 来自本轮合法的簇头节点广播

②产生伪随机数 r_{1i_1} // 作为簇成员节点

$N1i$ 与簇头节点 $C1$ 的共享密钥。

③计算: $ID=H \oplus k_tmp$; $isHeader=1$ 。

④存入簇头节点 $C1$ 有关信息: $[nodeID, key, isHeader]=[ID, r1i_1, isHeader]$ 。

⑤计算: $I=Hash(mkey||k_tmp)$; $J=Hash(mkey||r1i_1)$; $K=ID1i \oplus k_tmp$; $L=r1i_1 \oplus k_tmp$ 。

⑥ $N1i$ 向簇头节点 $C1$ 通告信息 (I, J, K, L) 。

ENDIF

6) $C1$ 处理 $N1i$ 的信息。

$C1$: 处理逻辑

①计算: $k_tmp=L \oplus r1$ 。

IF $(I=Hash(mkey||r1))$ AND $(J=Hash(mkey||k_tmp))$ //本轮簇成员加入本簇的通告

②计算: $ID=K \oplus k_tmp$; $isHeader=0$ 。

③存入本簇成员节点 $N1i$ 有关信息: $[nodeID, key, isHeader]=[ID, k_tmp, isHeader]$ 。

ENDIF

经过以上过程后, 层次式无线传感器网络就被建立起来, 各节点中存储的共享密钥情况如表 3 所示。

表 3 节点存储的共享密钥情况

节点名/ ID	$recID$	$nodeID$	key	$isHeader$
Sink/ $ID0$	1	$ID1$	$r1$	0
	...	...	...	...
	R	IDR	rR	0
$C1/ID1$	1	$ID0$	$r1$	1
	2	$ID11$	$r11_1$	0
	...	...	...	...
	m	$ID1m$	$r1m_1$	0
$N11/ID11$	1	$ID0$	$r0$	0
	2	$ID1$	$r11_1$	1
$N12/ID12$	1	$ID0$	$r0$	0
	2	$ID1$	$r12_1$	1
...	...	...	...	...
$N1m/ID1m$	1	$ID0$	$r0$	0
	2	$ID1$	$r1m_1$	1

4.5 利用方案进行数据传输 (以数据从传感节点到汇聚节点为例)

1) $N11 \rightarrow C1$ 过程: 簇成员节点 $N11$ 上传感知

到的数据 $Data11$

$N11$: 处理逻辑

①查询数据表 $isHeader$ 字段值为 1 的记录, 得到上传对象节点 $ID=ID1$ 、密钥 $key=r11_1$ 。

②计算: $A=F(Data11, key) \oplus key$; $B=Hash(ID)$ 。

③向簇头节点 $C1$ 发送 (A, B) 。

2) 簇头节点 $C1$ 处理簇成员节点 $N11$ 的数据

$C1$: 处理逻辑。

数据表中逐条记录地检查字段 $nodeID$ 的值

IF $B=Hash(nodeIDi)$

①得到与传输对象节点 $ID=nodeIDi$ 共享的

密钥 $key=keyi$ 。

②计算: $Data11=F^{-1}(A \oplus key, key)$ 。

ENDIF

③同样, 可以得到簇的其他成员节点的数据,

比如 $Data12, \dots, Data1m$ 。

④各个数据存入数组 $datas[]$ 。

⑤采用融合函数得到该簇各个成员节点数据的融合结果 $C=P(datas)$ 。

⑥查询数据表 $isHeader$ 字段值为 1 的记录, 得到传输对象节点 $ID=ID0$ 、密钥 $key=r1$ 。

⑦计算: $D=F(C, key) \oplus key$; $E=Hash(ID1)$ 。

⑧向汇聚节点 Sink 发送 (D, E) 。

3) 汇聚节点 Sink 处理簇头节点 $C1$ 的数据

Sink: 处理逻辑

数据表中逐条记录地检查字段 $nodeID$ 的值

IF $E=Hash(nodeIDi)$

①得到与传输对象节点 $ID=nodeIDi$ 共享的密钥 $key=keyi$ 。

②计算: $Data=F^{-1}(D \oplus key, key)$ 。

③对最终得到的数据 $Data$ 做其他的操作。

④来自无线传感器节点数据的传输和处理结束。

ENDIF

5 密钥管理方案的性能分析

5.1 方案的安全性分析

1) 方案完整性

方案以 LEACH 无线路由协议为基础, 没有破坏原有协议的工作机制; 同时, 方案确保了随着每轮网络结构的重新建立而完成新一轮共享密钥的重新生成和分配, 做到了 LEACH 协议运行与本方

案分配密钥两不误。

2) 方案时效性

方案实施的目标是在每对交互节点之间传输数据的会话过程中都采用节能、省时、占用运行空间少的对称密码体制，由于是在层次式网络结构产生的同时完成共享密钥发布的，所以，保证了方案在每轮所构建网络中的时效性。

3) 动态密钥安全性

方案实施过程中，密钥发布时对节点之间交换的内容都进行了加密处理，并且密钥都是随机生成的，这大大增加了敌手通过分析截获到的信息来得到密钥的难度，保证了密钥的动态安全性。

4) 节点安全独立性

层次式网络结构建立后，任何两对会话节点所采用的会话密钥都互不相同。任何一个会话密钥丢失，都不会影响其他节点之间的安全会话，保证了节点安全独立性。

5) 密钥生存有效性

除了无线传感器节点自身的初始密钥 $mkey$ 外，其余所有密钥都是在每一轮簇重构过程中随机产生的，不同轮、不同节点间会话以及不同加、解密过程中使用的任何密钥都不相同，且同一个密钥的生存期不超过层次式网络结构的生存期，保证了密钥在生存期内的有效性。

6) 抗攻击性

由于每对节点的会话密钥不同，且都是随机生成的。所以，可以抵抗中间人攻击、DDoS 攻击等攻击。但是，由于 $mkey$ 等密钥存在于无线传感器节点中，密钥的静态安全性存在一定风险。

5.2 方案的效率分析

在 LEACH 路由协议工作期间，各个无线传感器节点都必须发送相关信息才能保证层次网络的建立，同时也才能保证基于 LEACH 协议的 WSN 共享密钥管理方案的实施。为了使各个密钥能安全地分配到各个相关节点，各个节点必须付出通信和计算代价，具体的通信量和计算开销情况分别如表 4 和表 5 所示。其中， h 表示散列函数运算代价， c 表示连接运算代价， p 表示异或运算代价， a 表示与运算， L 表示密钥长度。

表 4 本文方案各节点的通信代价

节点	通信量
簇成员节点	$4L$
簇头节点	$4L$
汇聚节点	$4L$

表 5 本文方案各节点的计算代价

节点	计算开销
簇成员节点	$6h+6c+6p+2a$
簇头节点	$6h+6c+6p+2a$
汇聚节点	$3h+3c+4p$

从表 4 可知，各个节点产生的通信量一样。从表 5 可知，在将簇成员节点感知的数据传输到汇聚节点的过程中，各个簇头节点和簇成员节点的计算量一样，汇聚节点的计算量更小，说明簇头节点和簇成员节点在方案实施过程中消耗的能量基本相同。除了散列函数运算外，连接运算、异或运算和与运算都是占用时间和空间很少的运算，说明方案实施中占用的能量较少。

另外，各节点中必须存储相关节点的编号 ID 和密钥，每个相关节点的信息量最多为 $2L$ 。因此，如果一个节点（如簇头节点）存储与之相关信息的节点数为 n ，那么该节点为此需要的存储空间大小为 $2nL$ 。

6 结束语

随着物联网应用的迅速发展，对无线传感器网络安全的得到了学者们的重视。延长无线传感器寿命、提高无线传感器网络的效率、保证网络的安全是无线传感器网络研究的重要目标。基于 LEACH 协议的 WSN 共享密钥管理方案的实施，没有改变原有路由协议的运行机制，同时该方案具有很好的方案完整性、方案时效性、动态密钥安全性、节点安全独立性、密钥生存有效性，具有抵抗中间人攻击、DDoS 攻击等风险的能力，而且分发共享密钥消耗的能量较低，网络运行效率较高，这对提高无线传感器网络性能很有意义。

参考文献:

- [1] AKYILDIZ F, SC W, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.
- [2] 袁艳祥, 游林. 基于身份加密的可认证密钥协商协议[J]. 信息网络安全, 2014(3): 1-6.
- YUAN Y X, YOU L. Identity-based encryption authenticated key agreement protocol[J]. Netinfo Security, 2014(3):1-6.
- [3] 赵强利, 蒋艳凰, 徐明. 无线传感器网络路由协议的分析与比较[J]. 计算机科学, 2009, 36(2): 35-41.
- ZHAO Q L, JIANG Y H, XU M. Analysis and comparison of routing protocols for wireless sensor networks[J]. Computer Science, 2009, 36(2):35-41
- [4] [EB/OL]. <http://network.51cto.com/art/201006/207523.htm>.
- [5] 汪祥莉, 李腊元, 王文波. 无线传感器网络中的路由协议研究[J]. 计算机科学, 2008, 38(7): 50-52, 60.
- WANG X L, LI L Y, WANG W B. Research on routing protocols for wireless sensor networks[J]. Computer Science, 2008, 35(7): 50-52, 60
- [6] 吴征, 朱军, 等. 一种新的基于 LEACH 的 WSN 分簇协议[J]. 计算机技术与发展, 2010, 20(5): 29-33.
- WU Z, ZHU J, et al. A new LEACH-based clustering protocol for wireless sensor networks[J]. Computer Technology and Development, 2010, 20(5):29-33.

作者简介:



范敏 (1967-), 男, 四川中江人, 硕士, 绵阳师范学院副教授, 主要研究方向为物联网、信息安全、计算机网络与应用。



蒋珏 (1971-), 女, 贵州盘县人, 绵阳师范学院助理馆员, 主要研究方向为计算机应用。



汤琳 (1982-), 女, 四川中江人, 绵阳师范学院讲师, 主要研究方向为计算机应用、网络通信。



仇莫然 (1995-), 男, 四川绵阳人, 绵阳师范学院硕士生, 主要研究方向为物联网应用。



李超 (1993-), 男, 四川峨眉山人, 绵阳师范学院硕士生, 主要研究方向为计算机应用。