抗 DoS 攻击的多用户传感器网络广播认证方案

郭江鸿，马建峰
（西安电子科技大学 网络与信息安全教育部重点实验室，陕西 西安 710071）

摘 要：在 vBNN-IBS 签名基础上提出了一种抗 DoS 攻击的多用户传感器网络广播认证方案 DDA-MBAS，利用散列运算及用户信息进行虚假数据过滤。与现有的多用户传感器网络广播认证方案相比，DDA-MBAS 在抵抗节点妥协攻击、主动攻击的基础上，以较低的能耗过滤虚假消息并有效地限制了妥协用户发起的 DoS 攻击及共谋攻击的安全威胁。

关键词：多用户无线传感器网络；网络安全；广播认证；DoS 攻击
中图分类号：TP301 **文献标识码**：B **文章编号**：1000-436X(2011)04-0094-09

Multi-user broadcast authentication scheme in wireless sensor networks with defending against DoS attacks

GUO Jiang-hong, MA Jian-feng
(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)

Abstract: A multi-user broadcast authentication scheme was proposed in wireless sensor networks with defending against DoS attacks(DDA-MBAS) based on vBNN-IBS signature, the bogus messages could be filtered using hash operation and user information. Compared with existing multi-user broadcast authentication schemes, except defending against node compromise attack and active attack, the bogus messages can be filtered with low energy consumption and the threat of DoS attack and collusion attack launched by compromised user can be limited effectively.

Key words: multi-user wireless sensor network; network security; broadcasting authentication; DoS attack

1 引言

随着传感器技术的发展，无线传感器网络(WSN, wireless sensor network)的应用范围日益广泛。WSN 由大量资源传感器节点组成，彼此通过无线链路进行通信。由于无线链路的开放性，广播成为重要的通信手段。为保证广播消息的安全性，应当对其进行认证以抵御敌手广播的虚假消息。传感器网络广播认证方案有基于对称密钥及基于公钥系统 2 种。

基于对称密钥的认证方案主要是 μTESLA [1]及其改进方案。Perrig 等通过时间划分，将每个小的时隙与一个由密钥种子生成的反向散列链上的密钥对应，并通过延迟公布密钥的方法实现了认证的非对称性。同时，通过消息的接收时间与认证密钥对应的时隙提供消息安全性检查。Liu 提出了分层 μTESLA [2]，该方案采用预装参数的方法，通过建立多层密钥链减小了认证密钥计算量，提供了一定

收稿日期：2010-04-27；**修回日期**：2010-09-28
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2007AA01Z429, 2007AA01Z405）；国家自然科学重点基金资助项目（60633020, 60573036, 60702059, 60503012）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2007AA01Z429, 2007AA01Z405); The National Natural Science Foundation of China(60633020, 60573036, 60702059, 60503012)

的抗 DoS 攻击能力；沈玉龙等在多基站网络中对分层 μTESLA 进行扩展，提高了认证密钥种子的安全性[3]。但密钥与时隙对应及延迟公布认证密钥也带来以下问题：①由于密钥延迟发布，传感器节点必须缓冲未认证的消息，易受敌手发动的泛洪攻击。如敌手向网络中注入大量的伪造消息填满传感器节点的有限缓冲，导致基站发出的广播消息丢失。②由于密钥的延迟发布，敌手易发动虫洞攻击。

由于传感器节点资源有限，公钥方案一度被认为不适用于传感器网络，但研究表明[4]，即使是软件实现的公钥方案也可用于传感器网络，如在标准的 MICA2 传感器上进行 ECC-160 点乘运算需要 0.81s。由于 ECC 公钥系统为 160bit 的密钥提供了与 1024bit 密钥的 RSA 方案相同的安全性，且不需要延迟发布密钥，提供了比 μTESLA 等方案更好的安全性及灵活性，将是传感器网络安全方案的重要选择。但基于公钥的计算毕竟是 CPU 密集型计算，敌手易注入虚假数据使传感器节点进行大量公钥运算(如签名验证等)，以达到消耗节点能量的目的。因此，在基于签名的广播认证方案中以低能耗的方式对虚假数据进行过滤尤为重要。

目前提出的抗 DoS 攻击的传感器网络广播认证方案大多不适合多用户环境。如 Ning 等[5]提出了一种基于消息难题的抗 DoS 攻击方法，但该方法要求发送方有较强的能力且引入较大的发送延迟，因而不适合传感器网络；Dong[6]等在 ECDSA 基础上通过消息预认证提出了 KCFS(key chain based filter scheme)，有效地对大部分的虚假广播消息进行了过滤，但该方案主要针对基站广播且对共谋攻击抵抗能力差；Wang[7]等使用滑动窗口(DW, dynamic windows)进行虚假消息过滤，但该方案中敌手静止的假设及节点知道距离敌手跳数的要求对其应用造成较大限制，且该方案在存在多个敌手时效果不理想。

同时，目前的多用户传感器网络广播认证方案中未能提供低能耗的方式对虚假消息进行过滤。如 Ren 等[8]提出了 IDS(ID-based authentication scheme)多用户广播认证方案，利用双线对运算过滤虚假消息，能耗高且计算时间长；Cao 等[9]基于 BNN-IBS 的变形方案 vBNN-IBS 提出了多用户广播认证方案 IMBAS，通过 ECC 上点乘运算对消息签名进行验证，能耗低于基于双线对运算的认证方案，但对虚假消息的过滤仍然基于公钥运算。在多用户传感器网络中，妥协节点与妥协用户均可发起攻击。对于虚假消息，目前的多用户广播认证方案大多依靠高能耗的签名认证将其控制在一跳范围内；但妥协用户发出的消息可通过所有节点的签名认证，一个妥协用户就可严重威胁网络安全性，当妥协用户与妥协节点发动共谋攻击时，对网络能耗的影响更为严重，而目前的多用户传感器网络广播认证方案中均未有效抵抗妥协用户的攻击。

本文提出了一种抗 DoS 攻击的多用户传感器网络广播认证方案 DDA-MBAS，以 BNN-IBS 的变形方案 vBNN-IBS 为基础，利用预认证密钥与用户信息对虚假消息进行过滤，以较低的能耗将虚假消息控制在一跳范围内；对妥协用户发起的 DoS 攻击，通过速率控制使节点对该用户广播签名验证不会超过 1 次/β 秒，有效地降低了传感器节点能耗，延长了传感器网络生存期；对妥协用户与妥协节点进行共谋攻击， DDA-MBAS 有效地降低了妥协节点数目对网络安全的威胁，并提出了一个共谋攻击下妥协用户的简单检测方法。

第 2 节简介 BNN-IBS 及其变形方案 vBNN-IBS、网络模型及攻击者模型，第 3 节中给出 DDA-MBAS，第 4 节中分析了 DDA-MBAS 的开销及安全性，并与 IDS 及 IMBAS 等多用户传感器网络广播认证方案进行比较，第 5 节是结束语。

2　预备知识

2.1　vBNN-IBS 简介

Bellar 等于 2004 年提出了基于椭圆曲线的 IBS 方案 BNN-IBS，并对该方案的安全性做出了证明[10]。BNN-IBS 签名长度为 105byte[10]，为减少签名长度，Cao 等提出 BNN-IBS 的变形方案 vBNN-IBS，该方案与 BNN-IBS 具有相同的安全性及计算复杂度，但消息签名缩减为 83byte[9]，具体如下。

给定安全参数为 k；选择有限域 F_q 上的椭圆曲线 E/F_q，以 $E(F_q)$表示 E/F_q 上的点构成的群，$E(F_q)$阶为 n；$P \in E(F_q)$且 P 的阶为 p，p 为素数且 p^2 不整除 n；$<G>$为由 P 生成的群。

系统参数设定：系统参数为 $<E/F_q,P,p,Q,H_1,H_2>$，其中 $x \in_R Z_p$ 为系统私钥；$Q=xP$ 为系统公钥。H_1，H_2 为 2 个加密散列函数。

$$H_1:\{0,1\}\times G_1^* \to Z_p, H_2:\{0,1\}^* \to Z_p$$

用户密钥生成：给定用户 ID 为 ID_u，$ID_u \in \{0,1\}^*$。

1) 选取 $r\in_R Z_p$，计算 $R=rP$。

2) 利用系统密钥 x 计算 $s=r+cx$，$c=H_1(ID_u\|R)$。

用户 ID_u 的私钥 $SK_u=(R, s)$。

签名：用户 ID_u 对消息 m 的签名如下。

1)选取 $y\in_R Z_p$，计算 $Y=yP$；

2)计算 $z=y+hs$，其中 $h=H_2(ID_u, m, R, Y)$。

用户 ID_u 对消息 m 的签名为$<R, h, z>$。

签名验证：给定用户 ID_u、系统参数、消息 m 及签名$<R,h,z>$，验证如下内容。

1) 计算 $c=H_1(ID_u\|R)$;

2) 检查 $h=H_2(ID_u, m, R, zP-h(R+cQ))$是否成立。

2.2 网络模型

DDA-MBAS 主要用于多用户静态无线传感器网络，并做如下假设。

1) 只有基站与用户可以对消息进行签名，以节点身份进行的广播通过先将该消息发给基站，由基站进行广播。

2) 假设部署后有一小段安全时间，节点可根据一定的定位算法获得位置信息(如通过一组配备 GPS 的移动锚点进行定位[12])，并通过基站广播得到基站的位置信息。

3) 用户可通过 PDA 或其他设备访问网络，用户入网后位置固定，可自行完成定位并将位置信息上报基站，用户、传感器节点及基站保持松散的时间同步。

4) 为简化分析，设基站、用户、传感器节点具有相同的通信半径。

2.3 攻击者模型

敌手可以在网络中移动，妥协传感器节点，修改并注入虚假数据，发动以下攻击。

妥协攻击：一般来说，传感器节点妥协难以避免，敌手可以在物理上俘虏节点，获取其秘密信息，使节点完成敌手要求的操作。另外，设敌手可对用户进行妥协攻击。

主动攻击：敌手可以重放以前的合法消息，使网络中的传感器节点提供数据或执行其他操作；敌手也可以伪造消息发动攻击。

DoS 攻击：敌手可以向网络中注入大量的虚假数据，以达到 2 个目的：① 由于传感器节点资源有限，大量的虚假数据容易填满接收方的缓冲，从而导致节点无法接收正确的广播消息；② 在基于公钥加密的传感器网络广播认证方案中，为验证所接收的消息，传感器节点不得不进行大量的公钥运算，消耗大量能量，缩短了传感器网络的生命期。

3 DDA-MBAS 简介

DDA-MBAS 主要由系统初始化、消息广播、消息认证、用户注册与撤销、预认证密钥更新等部分组成。

3.1 系统初始化

部署前，部署服务器(相当于可信第三方)按 2.1 节所述选取合适的 E/F_q 及系统参数，基站选取一随机密钥种子生成反向预认证密钥链，将系统参数与基站预认证密钥承诺预装入传感器节点。同时，为每个节点 A 选取一个随机密钥种子 K_A^n，按以下方法生成 2 级密钥链预装入节点。

1 级：$K_A^i=H_l^1(K_A^{i+1})$，$0\leqslant i<n-1$；

2 级：$K_A^i=K_A^{i,0}$，$K_A^{i,j}=H_l^2(K_A^{i,j-1})$，$1\leqslant j<n$。

$H^1(\,)$、$H^2(\,)$为单向函数，$H^1(\,)\neq H^2(\,)$; $H_l(\,)$表示取单向函数输出的前 l bit。

由于传感器节点资源有限，可先计算并使用$\{K_A^{0,j}\}$，当前节点的密钥承诺为 $K_A^{0,n}$；该密钥链消耗完后动态计算$\{K_A^{1,j}\}$，并通知邻居节点更新密钥承诺为 $K_A^{1,n}$，同时更新对应的标号。

设节点已经通过定位算法获取了自己的位置信息，并通过密钥协商方案与邻居节点建立了配对密钥，节点间可通过配对密钥交换彼此的密钥承诺。则每个节点维护一张邻居节点表及用户表，邻居节点表格式如下：

ID_B	K_B^i	i
ID_C	K_C^j	j
…	…	…

其中，第 1 列为邻居节点 ID，第 2 列为该邻居节点的密钥承诺，第 3 列为与当前密钥承诺对应的标号。

同时，节点维护一张网络中的用户表格式如下：

ID_{U1}	K_{U1}^i	i	t_{U1}
ID_{U2}	0	j	t_{U2}
ID_{U3}	0	k	t_{U3}
…	…	…	…

其中，各项分别表示用户 ID、用户位置信息、用户预认证密钥承诺、标号、最近已认证广播消息的时间。除了预认证密钥为 16byte 外，其他各项均为 2byte。若节点通过位置信息判断在用户 U 通信范

围内，则在用户表中添加 U 的全部信息；若用户 U 不是邻居，则添加除了用户预认证密钥承诺外的其他信息。

3.2　消息广播

设用户的广播频率受限，对于任一用户，其发出的 2 个连续广播消息的时间间隔 $\Delta T \geqslant \beta$s。消息格式 1 如下：

$$<ID_{\mathrm{A}}, i_{\mathrm{A}}, K_{\mathrm{A}}^{\,i_{\mathrm{A}}}, M,\ t,\ Sig_{SK_{\mathrm{A}}}\{ID_{\mathrm{A}}, M, i_{\mathrm{A}}, t\}>$$

其中，ID_{A} 为广播源，i_{A} 为消息标号，$K_{\mathrm{A}}^{\,i_{\mathrm{A}}}$ 为与 i_{A} 对应的预认证密钥，t 为广播源的消息发送时间，M 为广播消息，$Sig_{SK_{\mathrm{A}}}\{ID_{\mathrm{A}}, M, t\}$ 为消息签名，SK_{A} 为 ID_{A} 私钥。

广播源节点的邻居节点 ID_{B}(即 1 跳节点)收到广播消息后进行验证(如 3.3 节)，如正确则用自己预认证密钥承诺取代消息中广播源的预认证密钥，同时添加自身 ID 及预认证密钥标号，对消息进行转发。转发的消息格式 2 如下：

$$<ID_{\mathrm{B}}, i_{\mathrm{B}}, K_{\mathrm{B}}^{\,i_{\mathrm{B}}}, ID_{\mathrm{A}}, i_{\mathrm{A}}, M,\ t, Sig_{SK_{\mathrm{A}}}\{ID_{\mathrm{A}}, M,\ i_{\mathrm{A}}, t\}>$$

3.3　广播认证

设 ID_{C} 接收到了广播消息，进行如下验证。

1) 消息源检查：检查 $ID_{\mathrm{A}} \in UList$ 且 $ID_{\mathrm{B}} \in NList$，通过则转 2)，否则丢弃(若 ID_{C} 为用户 ID_{A} 的一跳节点，则仅检查 $ID_{\mathrm{A}} \in UList$)。

2) 预认证：若 ID_{C} 为 ID_{A} 的一跳节点，设存储的 ID_{A} 密钥承诺与标号为 $K_{\mathrm{A}}^{\,j}$ 与 j，当前消息中的预认证密钥与标号为 $K_{\mathrm{A}}^{\,i_{\mathrm{A}}}$ 与 i^{A}，验证：$K_{\mathrm{A}}^{\,j} = H_l^{\,i_{\mathrm{A}}-j}(K_{\mathrm{A}}^{\,i_{\mathrm{A}}})$，$1 \leqslant i^{\mathrm{A}} - j < T$。

若 ID_{C} 不是 ID_{A} 的一跳节点且存储 ID_{B} 密钥承诺与标号为 $K_{\mathrm{B}}^{\,p}$ 与 p，消息中的预认证密钥与标号为 $K_{\mathrm{B}}^{\,i_{\mathrm{B}}}$ 与 i^{B}，则验证：$1 \leqslant i^{\mathrm{A}} - j < T$，$1 \leqslant i^{\mathrm{B}} - p < P$，且 $K_{\mathrm{B}}^{\,p} = H_l^{\,i_{\mathrm{B}}-p}(K_{\mathrm{B}}^{\,i_{\mathrm{B}}})$，$P$、$T$ 为阈值。检查通过则转 3)，否则丢弃。

3) 新鲜性检查：根据广播源 ID 及消息时戳与用户信息表中的相应内容对比，检查消息的新鲜性，不新鲜则丢弃。若当前广播消息中的消息发送时间为 t，用户信息表中该用户上次发送合法消息的时间为 t_1，则检查：$t - t_1 \geqslant \Delta T$ 且 $0 \leqslant t_s - t \leqslant \Delta T_1$，$t_s$ 为节点时钟，ΔT_1 为阈值。第 1 项表示该用户发布的 2 个连续广播消息时间间隔合法，第 2 项表示该消息未经过较长的时延。

4) 进行签名验证(如 3.4 节)，验证通过则接受并转发消息，同时更新用户表及邻居表中相应内容；否则丢弃消息，从邻居表中删除转发节点对应信息，上报基站。

3.4　用户注册与撤销

用户注册：入网前，由基站为其分配 ID、预认证密钥链$\{K_U^{\,i}\}$、BNN-IBS 系统参数。入网后通过某定位方法(如 GPS 定位)获取自己的位置信息并通过一定的密钥协商协议及路由协议将位置信息发给基站。基站向网络广播用户注册信息。消息格式如消息格式 1，其中 M 为$\{ID_{\mathrm{U}}、LOC_{\mathrm{U}}、K_{\mathrm{U}}^{\,i}\}$。网络中各节点根据位置信息计算判断是否为用户的一跳节点，并对用户信息表进行相应更新。

用户完成任务离开网络时，基站向网络广播要撤销的用户 ID，节点更新用户信息表。

3.5　预认证密钥更新

由于节点资源限制，其预装的预认证密钥链长度有限(设长度为 n)。当该密钥链用完，则需由节点生成新密钥链，并将新的密钥承诺通过配对密钥发送给其邻居节点，各邻居节点解密消息并完成更新。

4　方案分析

DDA-MBAS 方案主要针对多用户传感器网络的广播认证提供安全性，除了抵抗节点妥协攻击与主动攻击，还以较低的能耗对大部分的虚假广播进行过滤。

为与 IMBAS 及 IDS 进行比较，先对 2 种方案的广播消息格式做简介[8,9]。

IMBAS: $<M, t, ID, Sig(M, t, ID)>$。$M$ 为消息，t 为时间，ID 为用户身份，$Sig(\ )$为签名。IMBAS 采用 vBNN-IBS 进行签名，签名长度为 83byte。

IDS:$<U_{id}, t, M, \delta_{x,y}, h(M, t, \theta)>$。$U_{id}$ 为用户身份，t 为时间，$\{\delta_{x,y},\ h(M,\ t,\ \theta)\}$ 为消息签名，其中 $\theta = e(P,P)^a$。IDS 采用 Hass 的签名方案[14]，签名长度为 60byte。

4.1　开销分析

本节主要对 DDAMBS 方案的开销做分析，包括存储开销、计算开销、通信开销。由于基站与用户有较丰富的资源，因此主要对传感器节点做开销分析。

1) 存储开销

除了预装的 BNN-IBS 系统参数、基站预认证密钥承诺、节点 ID、基站 ID 外，节点还需保存 2 级密钥链、邻居表及用户表。设预认证密钥为

128bit，由于 BNN-IBS 采用 SHA-1，为了不使节点再存储其他的单向函数代码，采用 3.1 节的方法产生长为 128bit 的密钥链，安全性等同于 AES-128。若 1 级密钥链长为 L，2 级密钥链长 M，则共有 $L\times M$ 个预认证密钥，约需$(L+M)\times 16$ byte 的空间；设网络中共有 k 个用户，节点通信范围内有 n 个邻居节点及 m 个邻居用户，设 L=50，M=50，n=50，则一个节点需 $2\,600+22m+6(k-m)$byte，对于本文方案，网络中同时存在的用户数目受节点内存的限制。

实际上，在网络中同时存在的用户数目不宜过多，否则很可能引起严重的信道竞争甚至通信阻塞，降低网络性能。当网络中同时存在的用户数目受限时，多个用户访问网络可通过一定的调度方法进行协调，如按照用户任务的紧急程度或按照其完成时间等为用户指定优先级，用户按优先级对网络进行访问。这部分内容超出本文范围，不予过多讨论。

2) 通信开销

通信开销主要取决于消息长度。对比 ECDSA 及 vBNN-IBS 签名方案中各种不同类型的消息长度，一般来说，消息类型有以下几种：用户注册消息(M1)、节点转发的注册消息(M2)、用户注销消息(M3)、节点转发的注销消息(M4)、广播消息(M5)、节点转发的广播消息(M6)。

设本文方案、IMBAS、IDS 的消息中 M 最大为 20byte，签名长度分别为 83byte、83byte、60byte，其他各项长均为 2byte，不同类型广播消息的长度如表 1 所示。

表 1　不同类型消息长度

消息类型	DDA-MBAS	IMBAS	IDS
M1	125	0	0
M2	129	0	0
M3	107	89	66
M4	109	89	66
M5	125	107	84
M6	129	107	84

注：vBNN-IBS 与 IDS 中，用户入网不需身份以外的信息，无需注册，但用户离网需进行基站广播

设对于 3 种方案均采用 802.15.4 标准对消息进行封装，该标准允许最多 102 byte 的可变载荷，总长度最大为 128byte。则 3 种方案在 802.15.4 标准封装下不同消息数据长度如表 2 所示。

表 2　802.15.4 标准封装下不同类型消息长度

消息类型	DDA-MBAS	IMBAS	IDS
M1	177	0	0
M2	181	0	0
M3	159	115	92
M4	163	115	92
M5	177	162	110
M6	181	162	110

据 Gura 等的研究[4]，在 MICA2 传感器上(8bit，ATmega128L，8MHz，电压 3V，活动电流 8mAh)[12]，SHA-1 的能耗约 5.9μJ×L，L 为输入长度；ECC 点乘需 0.81s，能耗约 0.81s×3V×8mAh=19.44mJ；MICA2 节点发送与接收一个字节的能耗分别为 59.2μJ、28.6μJ；根据 Bertoni 等的研究[13]，在 32bit，33MHz 的 ST22 智能卡处理器上，进行一次双线对运算约为 0.752s，则可估算在 MICA2 传感器上进行双线对运算时间为：0.752×33/8=3.102s，能耗为 3.102s×3V×8mAh=74.45mJ。

设一个广播消息数据长度为 $d$byte，则发送能耗 $E_{tr}=d\times 59.2\mu J$，接收能耗 $E_{re}=d\times 28.6\mu J$。3 种方案下不同消息的发送与接收能耗对比如图 1 所示。

由图 1 可看出，IDS 发送/接收消息所需能耗最少，原因在于其签名长度最短，为 60byte；IMBAS 次之，高出的能耗主要来自 83byte 的签名及封装后的包头数据；DAA-MBAS 能耗最多，主要原因是 83byte 的签名以及消息中包含的 16byte 的预认证密钥。

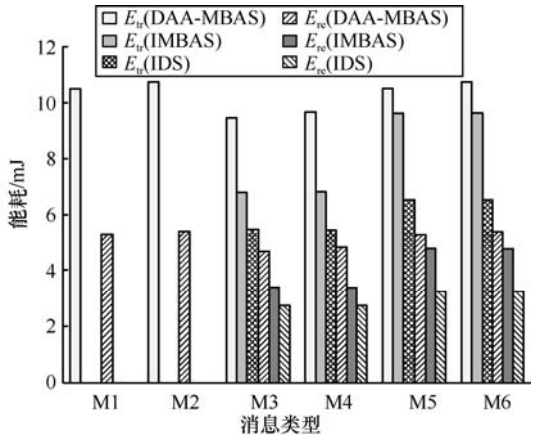


图 1　消息发送/接收能耗对比

用户注册与撤销消息仅在入网和离网时广播一次，更多的消息来自于用户入网后的广播及节点

对此消息的转发，即消息 M5 与 M6，因此以这 2 个消息的计算及通信能耗衡量各方案的开销(为简化分析，本节对 M5 与 M6 的长度不进行区分)。在泛洪广播下，每个节点接收来自邻居节点的 N 个消息(N 为邻居节点数)，发送一次，所需通信能耗 E 为

$$E=E_{\mathrm{tr}}+E_{\mathrm{re}}\times N=d\times 59.2\mu\mathrm{J}+d\times 28.6\mu\mathrm{J}\times N \quad (1)$$

3) 计算开销

DDA-MBAS 方案中，节点的计算开销主要来自预认证散列计算及对消息签名验证(相比签名验证，表查询操作的计算开销可忽略)。

设节点当前存储的密钥承诺为 K_i，接收的消息中散列密钥为 K_j，由于敌手可能用一个错误的散列密钥诱使正常节点进行大量的散列运算，因此必须规定运算的阈值 P，即超过 P 次运算无法从 K_j 得到 K_i，则认为该消息是伪造的。阈值的确定如下。

设网络中的丢包率为 p，对某发送方的任一广播消息，目的节点能正确接收的概率为 $1-p$，则目的节点连续丢失 m 个该发送方广播消息的概率为 p^m，如图 2 所示。

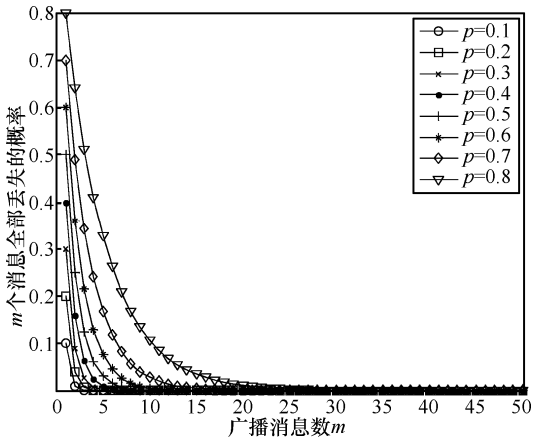


图 2　接收方连续丢包的概率

由于广播消息中的预认证密钥依据密钥链顺序依次使用，所以目的节点对来自发送方广播消息中预认证密钥的计算次数不会超过丢失的对应广播数。从图 3 可知，在网络丢包率不太高的情况下，如 $p\leqslant 0.6$ 时，目的节点以超过 99%的概率收到发送方 10 个广播消息中的一个，即使丢包率为 0.8，目的节点也以超过 99%的概率收到发送方 21 个广播消息中的一个。因此，进行预认证散列计算的阈值可根据网络通信状况来确定，一般情况下($p\leqslant 0.6$)，阈值设为 10 即可。相对于进行签名认证的计算量，预认证密钥的计算开销基本可以忽略，因此以签名认证的能耗来衡量不同方案中传感器节点的计算开销。

DDA-MBAS 与 IMBAS 方案采用 vBNN-IBS 签名，验证过程的主要运算为 3 个 ECC 点乘，IDS 方案采用 Hass 的 IBS 签名，主要运算为 2 个双线对运算[8]。3 种方案中进行一次签名验证的计算开销如表 3 所示。

表 3　　签名验证的计算开销

方案	耗时/s	耗能/mJ
DDA-MBAS	2.43	58.32
IMBAS	2.43	58.32
IDS	6.204	149

4) 综合能耗分析

根据通信开销及计算开销分析，处理一个合法广播消息的综合能耗 E_{all} 为

$$E_{\mathrm{all}}=E_{\mathrm{ver}}+E_{\mathrm{tr}}+E_{\mathrm{re}}\times N \quad (2)$$

其中，E_{ver} 为进行签名验证的计算开销，N 为邻居节点数，E_{tr} 与 E_{re} 分别为发送与接收消息的通信开销。当 N=40 时，3 种方案的综合能耗比较如图 3 所示。

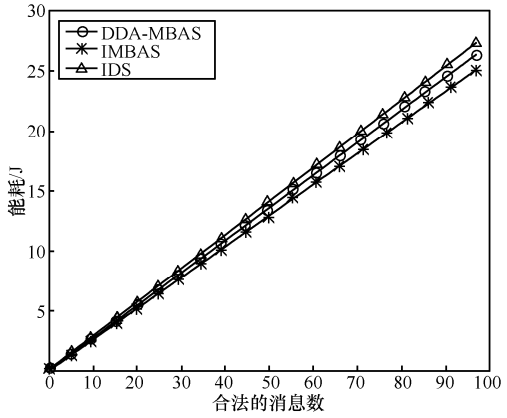


图 3　综合能耗对比

从图 3 可看出，3 种方案对一个合法消息进行认证所需的综合能耗相差不大。IDS 的通信开销最少，但其计算开销较大，综合能耗最高；DDA-MBAS 通信开销最大，计算开销优于双线对运算，综合能耗优于 IDS；IMBAS 综合能耗最优。

通过开销分析可知，DDA-MBAS 对合法消息进行认证的综合能耗与 IMBAS 及 IDS 的综合能耗处于同一层次，引入预认证方法不会消耗节点过多

能量。DDA-MBAS 的扩展性劣于 IMBAS 及 IDS，原因在于传感器节点资源有限，只能保存有限的节点及用户信息。但正如本文所提，仅靠用户公钥信息很难以低能耗的方式对虚假数据进行过滤；其次，本文方案中的受限用户数目指网络中同时存在的用户数，而不是总的用户数，可通过一定的调度方法进行协调；第三，由于传感器资源有限，网络中同时存在的用户数目不宜过多，否则很可能引起通信阻塞，降低网络性能。

4.2 安全性分析

DDA-MBAS 建立在 BNN-IBS 签名基础上，消息签名的安全性等同于 BNN-IBS，敌手伪造正确的签名困难性可归约为解决椭圆曲线离散对数问题(ECDLP, elliptic curve discrete logarithm problem)，而该问题是困难问题，具体安全性证明可参考文献[10]。

1) 抗节点妥协

设网络中有多个传感器节点妥协，敌手可获得妥协节点的所有秘密信息。由于节点中只存有基站与网络中用户的身份、位置、邻居预认证密钥等公开信息，敌手想通过公开信息得到基站或用户的私钥，其难度等同于解决椭圆曲线离散对数问题。其次，基于单向函数的性质，即使有多个节点妥协，敌手也只能得到某用户或节点已经公布的密钥承诺 K^i，无法伪造其未公布的预认证密钥 K^l，$l>i$。因此，妥协节点的数目无助于敌手生成正常用户或基站的合法签名。妥协节点的增加可以增大虚假消息覆盖范围，妥协节点的邻居可通过表查询或散列运算进行虚假消息过滤，不会带来高的能耗。

对于多用户广播认证方案 IMBAS 与 IDS，分别采用 vBNN-IBS 签名及 IBS 签名，妥协节点的数目无助于生成合法的签名且虚假消息可以严格控制在妥协节点的一跳范围内，但妥协节点的增多可增大虚假消息的覆盖范围，使更多的节点进行多次公钥签名验证。

2) 抗主动攻击

DDA-MBAS 中，接收方通过比较消息中的时间、标号与节点存储的时间及标号检查消息的新鲜性，重放攻击无法奏效。敌手假冒某用户或节点的身份发动攻击时，接收方通过邻居关系检查消息源。即使通过消息源检查，因敌手无法获得所假冒对象未公布的预认证密钥，伪造消息也无法通过认证过程 2)，接收方通过散列计算可将该消息过滤。

IMBAS 与 IDS 通过消息的时间检查新鲜性，可抵抗重放攻击；但若敌手伪造消息包含合法时间，IMBAS 与 IDS 必须进行签名认证，能耗明显高于本文方案。

3) 抗 DoS 攻击

考虑敌手发动以下 DoS 攻击时不同多用户广播认证方案的性能比较。

① 非法消息攻击。

如前所述，对于敌手伪造大量非法广播发动 DoS 攻击，本文方案以低能耗方式进行过滤，为使节点进行签名认证，敌手必须在其伪造消息中包含正确的预认证密钥，例如妥协节点可在消息中加入自己的预认证密钥使其邻居进行签名验证。由 3.3 节可知，对于一个可以通过预认证但没有通过签名认证的消息，接收方从自己的邻居表或用户表中删除发送方的相关信息。即不论一个敌手发送多少非法消息，最多使其邻居节点进行一次签名认证。对于 IMBAS 及 IDS 方案，敌手的邻居节点将进行 T 次签名认证，T 为 IMBAS 及 IDS 方案中的阈值。设敌手进行了 k 次虚假广播，$k\leqslant T$，敌手的邻居进行虚假消息过滤的能耗 E 为

$$E=E_{\mathrm{re}}+E_{\mathrm{ver}}=d\times 28.6\mu\mathrm{J}+E_{\mathrm{ver}} \tag{3}$$

E_{re} 为接收消息的能耗，d 为消息长度。结合 4.1 节中开销分析，各方案中敌手的邻居进行虚假消息过滤所需能耗如图 4 所示。

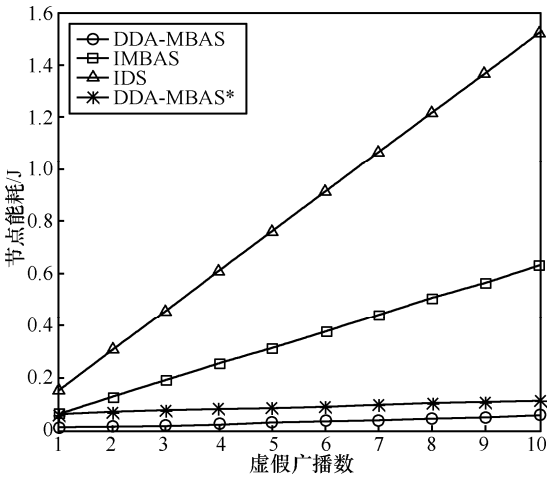


图 4 过滤虚假消息能耗比较

图 4 中 DDA-MBAS*指敌手在广播消息中加入正确的预认证密钥。可看出，由于 DDA-MBAS 采用了预认证密钥，敌手的邻居通过表查询或散列运算进行虚假消息过滤，所需能耗优于 IMBAS 及 IDS。显然。在网络中存在多个妥协节点并在较大

范围内进行多次非法广播时，本文方案中网络的整体能耗优势更明显。

② 妥协用户发起的 DoS 攻击。

对于妥协用户，由于该用户拥有合法身份及秘密信息，可向网络中注入大量可通过签名认证的广播，以达到使正常节点进行大量签名认证的目地。IMBAS 与 IDS 方案无法抵抗此类攻击。本文方案中节点拥有用户位置信息且对用户广播频率做了限制，可以有效限制此类攻击的威胁程度。对于用户的邻居节点，用户发出的 2 个连续的广播的认证时间间隔 ΔT 必须满足 $\Delta T \geqslant \beta$s，否则将不予转发。即正常节点在 βs 内对该用户发布的广播最多做一次签名验证。在 IMBAS 及 IDS 方案中，妥协用户可以连续快速地进行多次广播，节点对这些广播全部进行签名验证，能耗明显高于 DDA-MBAS 方案。设妥协用户在 Ts 内每 as 进行一次广播，网络节点总数为 N，每个用户的邻居节点数为 n，则以进行签名验证的节点数及每个节点进行的签名验证次数衡量 3 种方案能耗如表 4 所示。

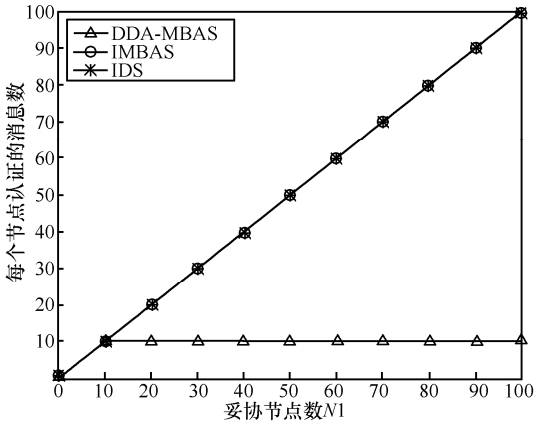
表 4　妥协用户攻击下 3 种方案认证比较

认证范围	DDA-MBAS		IMBAS		IDS	
	$a<\beta$	$a\geqslant\beta$	$a<\beta$	$a\geqslant\beta$	$a<\beta$	$a\geqslant\beta$
影响范围	n	N	N	N	N	N
认证次数	1	T/a	T/a	T/a	T/a	T/a

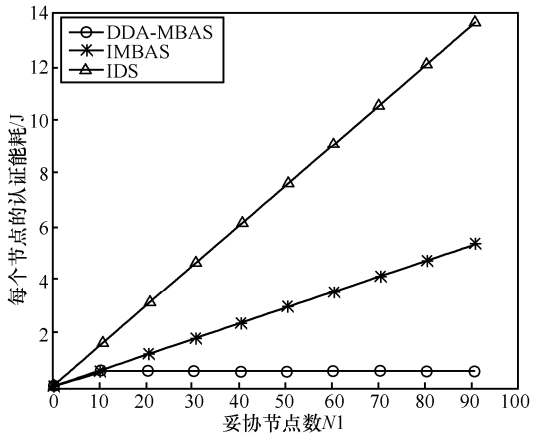
③ 妥协用户与妥协节点发动共谋攻击。

妥协用户可通过将自己的预认证密钥及私钥等信息发送给妥协节点，妥协节点利用这些信息生成大量可通过签名认证的合法广播来消耗正常节点的能量。设有 $N1$ 个妥协节点，则妥协节点一次可以广播 $N1$ 个合法消息。对于 IMBAS 及 IDS 方案，正常节点将对这 $N1$ 个消息全部进行签名认证。对于 DDA-MBAS 而言，为使节点进行尽量多的签名认证，各消息中应当包含不同的预认证密钥(若各消息中的预认证密钥相同，则节点只进行一次签名认证，后续消息被视为重复消息而丢弃)。由于 DDA-MBAS 中规定了散列运算阈值 P，因此妥协节点发出的广播中标号 i 应满足 $i_A<i\leqslant i_A+P$。设妥协节点随机选取标号 i 与对应的预认证密钥 K^i，在最坏情况下(节点依次收到标号为 $i_A+1,\cdots,i_A+P$ 的消息)，节点最多进行 P 次签名验证；若节点首先收到标号为 i_A+P 的消息，则只对一个消息签名验证。显然，当 $N1<P$ 时，每个节点最多做 $N1$ 个消息的签名认证；当 $N1\geqslant P$ 时，每个节点最多做 P 个消息的签名认证。

设本文方案中预认证散列计算阈值 P 为 10，3 种方案在妥协用户与妥协节点共谋攻击下每个节点的认证消息数及相应的认证能耗如图 5 所示。



(a)节点认证消息数比较



(b)节点认证能耗比较

图 5　抗共谋攻击比较

同时，DDA-MBAS 提供了在共谋攻击下妥协用户的简单检测方法，具体如下。

一般来说，用户 U 的邻居节点 v 先于 U 的非邻居节点收到 U 的广播，v 对该消息进行验证并转发。由于 U 与 v 之间为一跳通信，可靠性较高，若 v 连续接收到 L 个格式如消息格式 2 的广播，这些消息可通过签名验证且消息中广播源为 U，当 L 超过一定阈值 W，则可认为 U 是妥协用户并上报基站。

设一跳通信的丢包率为 p，$p\leqslant 0.2$，则 v 连续丢失 W 个 U 发出的广播消息的概率为 p^W，当 $W\geqslant 4$ 时，$p^W\leqslant 0.16\%$。即在此情况下，当 v 连续

接收到超过 4 个可通过签名验证的广播源为 U 的转发消息时，可以大于 99.84%的概率判定 U 为妥协用户。

综上分析，DDA-MBAS 方案提供了高的抗 DoS 攻击能力，以低能耗过滤伪造消息，而 IMBAS 与 IDS 通过高能耗的 ECC 点乘及双线对运算排除虚假消息；与 IMBAS 及 IDS 不能有效抵抗妥协用户发起的 DoS 攻击及共谋攻击相比，DDA-MBAS 通过用户广播速率控制及预认证密钥的计算阈值有效地减少了节点在妥协用户发动的 DoS 攻击及妥协用户与妥协节点共谋攻击下节点的能耗，同时，DDA-MBAS 提供了一种共谋攻击下妥协用户的简单检测方法。

5 结束语

针对目前抗 DoS 攻击的传感器网络广播认证方案不适于多用户环境，而现有的多用户传感器网络广播认证方案抗 DoS 攻击差的问题，本文提出一种抗 DoS 攻击的多用户传感器网广播认证方案 DDA-MBAS，与现有的多用户传感器网络广播认证方案 IMBAS 与 IDS 相比，在相同层次的通信开销及计算开销基础上，有效地以低能耗的方式对非法数据进行过滤，同时有效地减少了妥协用户发动 DoS 攻击及妥协用户与妥协节点发动共谋攻击对节点能耗的威胁。

由于节点资源限制，DDA-MBAS 中同时存在于网络中的用户数受限，扩展性劣于 IMBAS 及 IDS，同时，本文方案针对静态用户，在应用上受到一定限制。如何提高扩展性并在动态网络中有效地抵御 DoS 攻击是下一步的工作目标。

参考文献：

[1] PERRIG A, SZEWCZYK R, TYGAR J, *et al*. SPINS: security protocols for sensor networks[J]. ACM Wireless Network, 2002, 8(5): 521-534.

[2] LIU D G, PENG N. Multi-level μTESLA: a broadcast authentication system for distributed sensor networks[J]. ACM Transactions on Embedded Computing Systems (TECS), 2004, 3 (4): 800-836.

[3] 沈玉龙, 裴庆祺, 马建峰. MMμTESLA: 多基站传感器网络广播认证协议[J]. 计算机学报, 2007, 30 (4): 539- 546.
SHEN Y L, PEI Q Q, MA J F. MMμTESLA: broadcast authentication protocol for multiple-base-station sensor networks[J]. Chinese Journal of Computers, 2007, 30 (4): 539-546.

[4] WANDER A, GURA N, EBERLE H, *et al*. Energy analysis of public-key cryptography on small wireless devices[A]. Proc PerCom'05, IEEE[C]. 2005.324-328.

[5] NING P, LIU A, DU W, Mitigating DoS attacks against broad-cast authentication in wireless sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008(4):1-31.

[6] DONG Q, LIU D G, NING P. Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks[A]. Proceedings of the First ACM Conference on Wireless Network Security[C]. Alexandria, VA, USA, 2008.

[7] WANG R, DU W, NING P. Containing denial-of-service attacks in broadcast authentication in sensor networks[A]. MobiHoc'07: Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing[C]. 2007. 71-79.

[8] REN K, LOU W, ZENG K, *et al*. On broadcast authen- tication in wireless sensor networks[J]. IEEE Transactions on Wireless Communications (TWC), 2007,6(11): 4136-4144.

[9] CAO X, KOU W, DANG L, *et al*. IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks[J]. Computer Communications, 2008, 31:659-671.

[10] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes[A]. Proc EUROCRYPT 2004[C]. 2004. 268-286.

[11] MICA. datasheet[EB/OL]. http://www.xbow.com/ Products/ Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf/,2006.

[12] ZHANG Y C, LIU W, FANG Y G, *et al*. Secure localization and authentication in ultra-wideband sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(4): 829-835.

[13] BERTONI G M, CHEN L, FRAGNETO P, *et al*. Computing Tate pairing on smartcards[EB/OL]. http://www.st.com/stonline/products/families/smartcard/ches2005_v4.pdf/,2005.

[14] HESS F. Efficient identity based signature schemes based on pairings[A]. SAC 2002, Lecture Notes in Computer Science[C]. 2003. 310-324.

作者简介：

郭江鸿（1975-），男，山西长治人，西安电子科技大学博士生，主要研究方向为无线移动安全、网络安全。

马建峰（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学、移动与无线网络安全。