浙江理工大学学报(自然科学版),第 33 卷,第 2 期,2015 年 3 月
Journal of Zhejiang Sci-Tech University (Natural Sciences)
Vol. 33, No. 2, Mar. 2015

文章编号: 1673-3851 (2015) 02-0219-09

无线传感器网络在线代码分发最新研究进展

张国萍

(浙江理工大学信息学院, 杭州 310018)

摘　要: 无线传感器网络在线代码分发是在传感器网络首次部署完成后对其进行远程任务再分配、节点软件更新和网络功能再配置的过程,是拓展无线传感器网络应用生命周期的重要手段。纵观现有在线代码分发相关研究,它们大致可以分成三类:以减少数据包的传输、提高能耗有效性为目的的传输对象优化算法;以增强代码分发安全性为目的的基于非对称密钥加密的安全认证算法研究;以增强代码分发安全性为目的的基于对称密钥的安全认证算法研究。比较发现,在现有的研究中,基于高效的网络编码的代码分发算法能较好的降低通信负载,基于非对称密码体制的安全认证方案虽然计算和存储开销比较大,但是能大大增强代码分发的安全性,因此它是提高代码分发安全性的主流方法。最后总结了现有代码分发算法存在的问题:基本都是集中式、缺乏量化分析、抗 DoS(Denial of Service)攻击问题等缺陷,并给出了针对这些问题展开进一步研究的建议。

关键词: 无线传感器网络; 代码分发; 安全认证; 重编程

中图分类号: TP393.0　　**文献标志码**: A

0　引　言

无线传感器网络(WSNs, wireless sensor networks)是近年来兴起的新型网络,已被广泛应用于工业控制、国防军事、生态保护、环境监测等各个领域。传感器节点一旦部署完毕将会长期工作于无人看守的或恶劣的工作环境中。随着时间的推移,经常需要增加一些新的功能或者修复软件中存在的问题,这就需要对整个网络进行代码更新。在一些网络规模较大或者是节点部署环境较恶劣的情况下,通过人工的方式,手动地对所有节点编程将是一项非常耗时、耗力甚至是不可能完成的工作。为此在 WSNs 中需要一种有效的方法能够通过无线的方式自动地远程对节点进行升级或更新。WSNs 网络重编程(network reprogramming)技术又称在线代码分发(online code dissemination)技术是一种较为行之有效的解决方法。

WSNs 在线代码分发的通用定义是在 WSNs 初次完成部署后,对节点上运行的远程任务进行再分配、软件升级或更新和网络现有功能的再配置过程。由于 WSNs 的无线通信特性,使得其网络重编程技术与有线网络存在很大区别,其相关算法的研究遭遇了很大的挑战,因此受到了国内外众多研究人员的高度关注,迅速成为了研究的热点,并取得了大量的研究成果。现有的对在线代码分发技术的研究主要集中在以下三个方面:a)以减少数据传输量、提高能耗有效性为目的的传输对象优化算法;b)以增强代码分发安全性为目的的基于 PKC 的安全认证算法研究;c)以增强代码分发安全性为目的的基于对称密钥的安全认证算法研究。现就这三个方面对国内外已经开展的相关研究工作进行分析。

1　代码分发中的传输对象优化算法

传输对象优化算法主要研究各种代码映像组织、产生方法和传输目标的优化等问题,以减少网络数据传输量、降低系统代码分发能耗为研究目标。

这类算法的标志性成果是 Culler 等[1]提出的增量式多跳代码分发算法 Deluge。Deluge 首先将更新程序进行分页和分包处理,页按序逐页传输,页

收稿日期: 2014－07－31

基金项目: 国家自然科学基金项目(61100214、61100057);浙江省教育厅项目(Y201432073)

作者简介: 张国萍(1977－),女,浙江上虞人,实验师,硕士,主要从事无线传感器网络和 FPGA 应用方面的研究。

内数据包允许乱序方式传输，其工作过程主要分为三步：Advertise→Request→Update。基于效率考虑，Deluge 采用了多种消息压缩机制和空间多路传输。但是它没有考虑任何安全方面的问题，容易受到多种类型的攻击，也没有为减少传输代码映像的规模做任何优化。由于 Deluge 的广泛流行性，其已经集成到流行的 TinyOS 操作系统中并成为了代码分发协议事实上的标准，已成为后续算法的标杆或重要的实现框架，许多研究者在 Deluge 基础上做了许多进一步的工作。

Rajesh 等[2-3]针对 WSNs，提出了一个低负载的无线重编程算法 Stream。Stream 采用将程序映像分割成独立的两部分。一个程序映像是重编程协议的单独封装，预先安装在各个传感器节点上。另一个程序映像是应用程序本身的功能和侦听代码更新请求等少许重编程功能的封装，它也预安装在各个传感器节点上。通过这种功能分离策略，Stream 能较大地减少数据传输量。而针对现有代码分发算法主要以多跳方式为主的现象，Krasniewski 等[4]指出选择单跳还是多跳应该主要依据网络规模、节点密度和链接的可靠性。在 Stream 的基础上，他们提出了一个 DStream 系统，实现了单跳和多跳两种代码分发方式，并进一步给出了各种网络参数下选择单跳和多跳代码分发方式的原则[4]。文献[5-7]提出了通过喷泉码(fountain codes)来减少不可靠无线网络上代码分发的数据包重传，以解决 Deluge 不能扩展到通道错误恢复和多接收者的缺陷。Krasniewski 等[8]提出的 Freshet 则针对多源情况进行了优化，并通过有限的位置信息来确定节点休眠时机以此来降低延时，提高可靠性。

一些学者研究了运行着多个不同应用程序的 WSNs 中的代码分发问题[9-10]。Du 等[9]提出了一个自适应缓冲区管理策略以提高这种多应用的 WSNs 中代码分发的能量有效性，算法主要利用了多个应用程序常常共享一些代码的事实。Li 等[10]提出了一个能量有效的代码分发协议 MCP。MCP 也采用类似于 Deluge 的 Advertise-Request-Update 更新三部曲，通过有状态的多播代码分发协议来获得能量有效性。另一些研究人员则针对移动无线传感器网络中的代码分发算法展开了研究[11-12]。Bence 等[11]提出了一个选择性代码分发算法，周虹宇等[12]将基于传染病模型的代码分发机制引入了容延迟移动传感器网络中，从而实现了在容延迟性网络环境下节点在线更新。

从编译器层面来优化程序映像，减少传输能耗也是这类算法的一个重要研究方向。Zhang 等[13]和 Li 等[14-15]先后针对 WSNs 中代码分发的能量有效性问题提出了一个考虑代码更新的编译器设计技术 UCC(update-conscious compilation)。UCC 在编译旧代码做出各种编译决定时就考虑了后续代码更新的需求，提出了考虑更新的寄存器分配策略、基于阈值的数据分配策略和数据布局算法，最大程度地减少了代码更新过程的数据传输。但是，UCC 在减少数据传输量的同时可能增大新程序映像的运行时间，而且 UCC 需要从编译器层面上进行修改，增大了算法实施的难度。为了避免编译器层优化的高复杂性，Rajesh 等[16-17]提出了采用基于应用层代码优化的多跳增量式代码分发算法，以减少 WSNs 中代码分发的数据传输量和能耗，其基本工作原理如图 1 所示。针对纯粹的字节级比较产生增量 Delta 的方法容易导致增量膨胀的问题，Rajesh 等[16]提出了一个 Zephyr 算法，其采用在字节级比较前，进行应用层修改的方式，将函数调用固定于内存中的某个地址，在该地址上存储真正的调用语句，通过这种函数间接调用的方法来消除函数移动所带来的 Delta 膨胀问题。在 Zephyr 的基础上，Rajesh 等[17]又提出了改进的 Hermes 算法。Hermes 除了采用函数间接调用的技术以外，还新引入了一种全局变量处理策略来消除全局变量移动所带来的影响。同时算法为了降低函数间接调用对程序运行时间的影响，在 image rebuild and load stage 阶段将函数间接调用又转换回了直接调用。

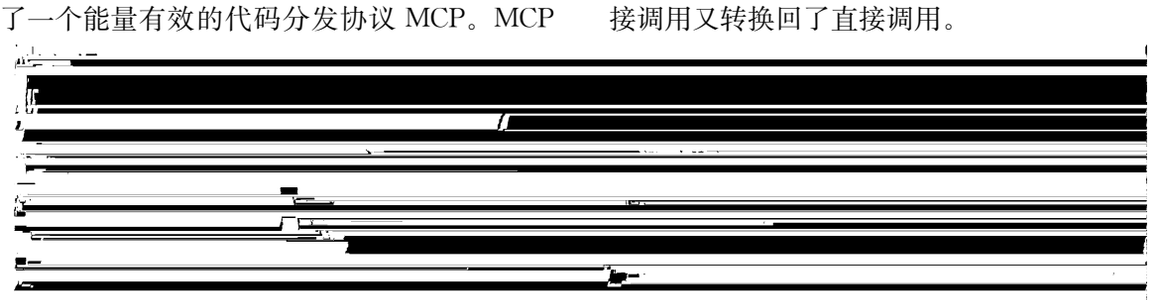

图 1 Zephyr 和 Hermes 算法的工作原理

2　基于 PKC 的安全认证算法研究

这类算法的主要策略是采用单向 Hash 函数辅以数字签名的方法,以认证发起代码更新的基站的身份以及更新代码包的有效性。

Lanigan 等[18]提出的 Sluice 方法是最早的面向网络代码分发的安全认证方案。Sluice 将更新代码首先分成固定大小的页,然后从最后一页开始,通过简单的 Hash 函数计算每页的 Hash 值,并将其嵌入前一页的末尾,如此不断地重复,形成一条单向 Hash 链。最后,对该链第一个元素及待更新程序映像的其他需要保护的信息比如程序版本号等进行数字签名,其工作过程与图 2 类似。因为只有基站才拥有唯一的私钥,因此该数字签名可以用来认证哈希链链首元素的有效性,再通过哈希链的单向性,其余页的有效性也可依次得到验证,从而确保更新代码的完整性。Sluice 能一定程度上防御网络中节点被俘获后发动的内部攻击,且只需一次数字签名,有效降低了计算开销。但是,由于 Sluice 采用的"页级"Hash 方法粗粒较粗,一旦认证失败,将被迫重传整个页面,这既加大了传输能耗,也带来了安全隐患,有利于攻击者实施 DoS 攻击。不同于 Sluice,Dutta 等[19]提出了细粒度的"包级"Hash,其工作过程如图 2 所示。该算法能即时验证数据包,从而避免了一个数据包被破坏导致整个页面需要重传的现象。然而后一个包的 Hash 值嵌入前一个包进行传输的工作方式使得要实现即时包验证,数据包的到达必须严格有序。但是,由于传输的无线特性,使得丢包和包乱序到达在 WSNs 中非常常见。针对这种包的乱序到达问题,Deng 等[20-21]提出了另一个代码分发安全认证方案,不同的是其基于 Hash 树。该方案中,基站首先将更新代码分成大小相等的一系列数据包,并对每个数据包计算哈希值以形成哈希值集合,然后对哈希值集合中两两相邻的两个哈希值进一步进行哈希操作,形成新一层的哈希值,如此重复,直到产生只有一个哈希值的树根,Hash 树的产生过程如图 3 所示的"树"状图。Hash 树的 root 值用基站私钥进行加密,产生一个数字签名以对其真实性和完整性检验。在传输代码数据包前,基站首先传输该 Hash 树,如果 Hash 树中所有 Hash 节点均可靠接收并通过验证,更新代码包就能乱序到达,并且能够被及时验证。这种方法需要为更新代码这样的大数据对象构建一棵 Hash 树,而且需要保留大量的内存空间来存储树中的节点值。为此,他们提出了一个改进方法[20],不是为整个映像而是为每个数据页建立一个 Hash 树,这种方法虽然能够减轻存储空间的压力,但付出的代价是需要进行多次数字签名运算,计算开销较大。为了解决多哈希树的多次签名问题,他们又提出了哈希链与哈希树相结合的混合方案[20],其工作原理如图 3 所示,混合方案的优点是结合了哈希树和哈希链的优点。它既能解决包乱序到达的问题,又只需一次数字签名。但是,混合签名方案每页要传输一棵 Hash 树,因此通信开销较大,而传感器节点只有有限的内存,很多 Hash 值只能存储在 EEPROM 中,这也将产生较大的能量消耗[22]。值得注意的是所有的这几种方案为了确保 Hash 树的可靠传输,需要采用逐层传输的方法,所以他们都没有完全解决包的乱序到达问题。

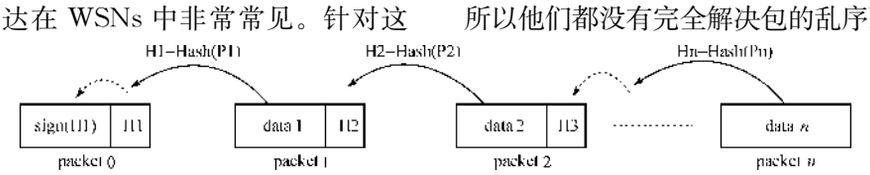

图 2　包级 Hash 方案的基本工作原理

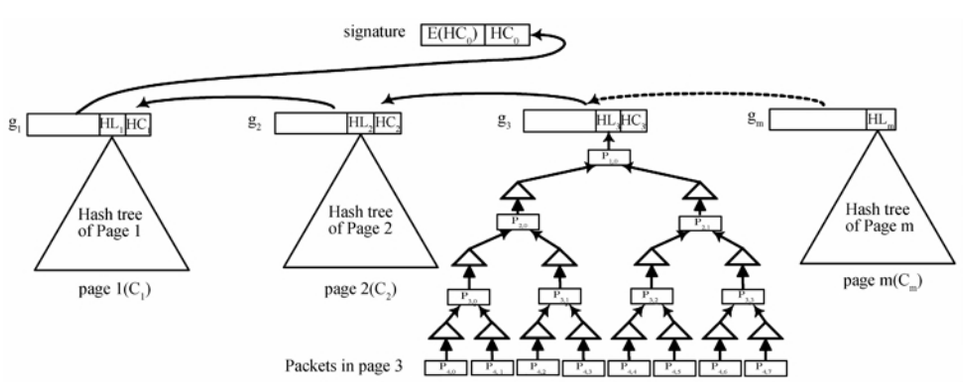

图 3　哈希树和哈希链的混合方案[20]

文献[23-30]针对代码分发中的 DoS 攻击提出了多种解决方法。Park 等[23]在文献[19-20]的基础上提出了一个应用增补哈希的方法来增强无线传感器网络代码分发安全性,该方法针对 WSNs 中由于丢包而引起的认证延时问题,提出了冗余哈希和页面摘要的两种解决方案。这两种解决方案都以增加通信负载为代价,且延时认证问题只是部分被解决了。Shaheen 等[24]提出了一个利用单向密钥链的方法来对待更新程序映像进行加密的代码分发算法,然而他们的算法只能处理单跳网络的程序映像分发,另外他们的算法也易受多种 DoS 攻击。针对利用数字签名验证的高复杂性而发动的 DoS 攻击,Dong 等[25]提出了基于密钥链和群的两种新过滤算法,但是这两种过滤算法都过分依赖于接收者和发送者之间密钥对的建立,而这将引入新的安全风险。Tan 等[26]针对 WSNs 中的代码信息可能敏感性的特点,提出了兼有机密性和抗 DoS 攻击的功能多跳代码分发协议。算法也采用 Hash 函数产生单向 Hash 密钥链,其中每个密钥对应待更新程序的一个版本;基站进行数据预处理的时候,采用从最后一个数据包开始计算 Hash 值,并将该 Hash 值追加到前一个数据包的最后,不同的是算法对每个数据包都用对称密钥加密方法进行了加密操作以保证代码分发的机密性,通过引入弱认证机制来防御基于数字签名的 DoS 攻击。他们提出的算法能有效防御多种 DoS 攻击,同时集成了代码分发的机密性,但是算法没有解决包乱数到达问题,同时提供机密性保证的同时引入了不小的加密计算开销,另外算法中对请求门槛值的设定也没有给出确定方法。针对代码分发中的 DoS 攻击,Hyun 等[27]和 Ning 等[28]提出了一个安全的抗 DoS 攻击的代码分发算法 Seluge。该算法也基于 Deluge 框架,基站在进行数据预处理时,从最后一个页面开始,计算页内每个数据包的 Hash 值,不过每个包的 Hash 值不是内嵌到前一个数据包,而是内嵌到前一页位置相对应的包中,如此重复直到第一页,其工作过程可以用图 4 表示,算法为第一页所有 Hash 值建立一个 Merkle Hash 树,其建立过程可以用图 5 表示。通过引入 MSP(message special puzzle)弱认证机制,以避免节点进行无谓的数字签名认证操作,另外算法为了防御基于 SNACK(selective negative acknowledgment)的 DoS 攻击,引入了簇密钥来进行局部广播认证,但是算法不能唯一地标识节点,所以一个被俘获节点还是很容易冒充其邻居节点,采用簇密钥来发起 DoS 攻击。Zhang 等[29]也提出了一个基于 CPK 的安全且抗 DoS 攻击的网络重编程协议,算法采用了类似的 Hash 链处理方法,Du 等[30]则从代码分发的底层广播特性,提出了一个防御 DoS 攻击的广播授权算法。

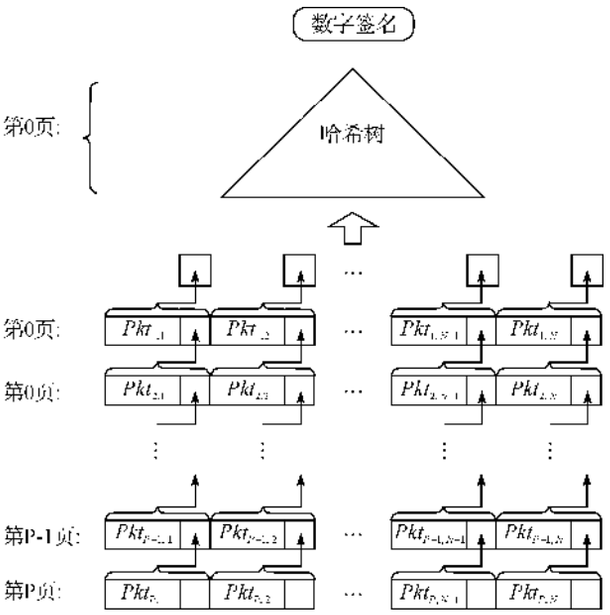

图 4 安全认证的包预处理过程[27-28]

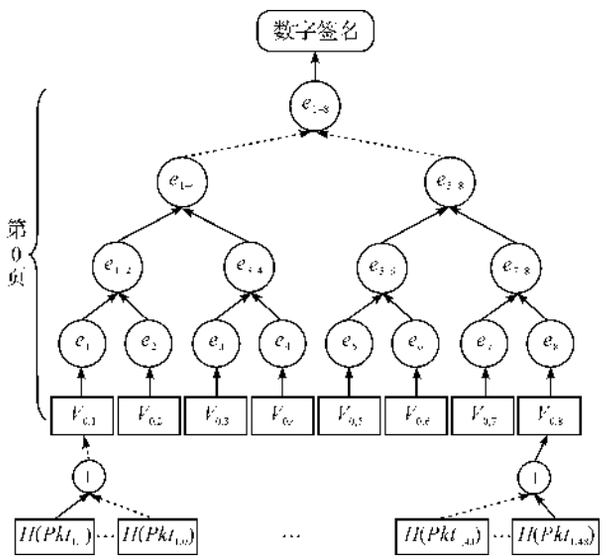

图 5 Merkle Hash 树建立方法

在线代码分发中利用网络编码的思想能降低代码分发过程中的能耗,均衡负载,但是很多算法没有考虑安全性。为此,Law 等[31]和 Zhang 等[32]在引入网络编码的思想后,进一步考虑了安全性。Law 等[31]提出了一个安全的无率 Deluge 算法,算法能有效抵御污染攻击,Zhang 等[32]在文献[27]的基础上提出了一个 LR-Seluge 算法,算法基于 Seluge 框架,不仅实现了 Seluge 所有的安全属性,还能有效

抵御丢包攻击,工作在高噪声环境下。但是文献[31]在采用了无率编码方案后,包验证只有在收到足够解码数据包并成功解码之后才能进行,增加了验证延时容易受到延时类 DoS 攻击。文献[33-35]提出了分布式的代码分发算法,不同与上述的所有其它算法,它们在代码分发过程中可以允许不存在基站,而且可以由多个授权用户分别发起代码分发操作。DiCode 算法[33]主要采用了基于证书的代理签名技术,然而 DiCode 中,节点在一次代码分发操作中需要进行两次昂贵的数字签名认证操作。SDRP 算法[34-35]则采用了双线性配对密码技术来进行多用户授权,然而双线性配对的高复杂性使得算法的实用性受到了很大的影响。

3　基于对称密钥的安全认证算法研究

基于对称密钥的安全认证,需要在发送者和接收者之间事先建立一个共享密钥。因此,这类算法主要研究密钥的机密性保护和节点被俘获后的代码更新的安全认证。

Kim 等[36]提出了一个 Castor 对称密钥认证方案,该方案通过采用基于消息认证码的对称密钥广播加密认证方法来避免对哈希链的链首进行数字签名。另外,他们提出的方案也借鉴了认证组播源的思路[37]来解决"节点落下"问题,但是他们提出的方案需要网络具有严格的时间同步,而这本身就是一个非常困难的问题。而且,Castor 不能有效防御节点被俘获情况下的内部攻击。Krontiris 等[38]提出了一个 *r*-times 签名认证方案。该方案吸收了 HORS、一次签名和 Merkle Hash 树的一些思想,对 Hash 链链首元素进行数字签名时用的是对称密钥加密的方法。针对 HORS 和一次签名中公钥存储空间过大的缺陷,该方案将私钥作为 Merkle Hash 的叶子节点,分布到多个 Merkle Hash 树中,将每个 Merkle Hash 树的根作为公钥。签名一个消息时,通过与消息相关的下标值,从私钥集合中选取私钥子集并结合相应的授权路径组成消息的数字签名。验证时,首先重新计算消息的 Hash 值和各个索引下标,然后从公钥集合中选取相应的公钥值子集,最后通过计算签名的授权路径,产生每个 Merkle Hash 的根与通过索引所取的各公钥值进行比较,如果所有值均相等,则验证通过。该方案在公钥大小与签名长度两方面取得了平衡,公钥大小和签名长度的最小化特性使其能适用于无线传感器网络。由于在单个节点端的验证只需进行 Hash 操作和比较运算,因此验证时间和计算开销都较小。方案的"页级"的哈希粒度使其与其它类似算法一样不具有抗 DoS 攻击的能力。Tan 等[39]则针对多跳的网络代码分发,提出了一个通过多个单向密钥链来加强其安全性的算法,他们利用了对称加密算法来加密当次使用的 Hash 密钥,而没有使用任何的非对称加密算法。这种算法能有效的防御部分巫师攻击(sybil attrack)和虫洞攻击(wormhole attack),但是被俘获节点还是可以利用接收数据包的时间差,将篡改过或伪造的数据包向同一群内的节点发送,从而发起巫师攻击。另外,算法没有解决包乱序到达时的即时认证问题。针对现有安全机制不适合于编码传输的代码分发,Bohli 等[40]提出了一个通过对称加密算法来加强采用喷泉码编码传输的代码分发的安全性。Dennis 等[41]针对密钥预安装在无线传感节点上所带来的安全风险,提出了一个利用 RSA 技术进行密码更新的方法,他们进一步提出了一个为节点群建立群密钥的方法来进行代码分发,这种方法由于 RSA 的引入而急剧增大了计算开销。

4　结　论

通过对上述已经展开的无线传感器网络在线代码分发相关研究的分析,可以发现由于 WSNs 的无线特性,使其在线代码分发技术迥异于有线网络,相关算法研究面临着以下三个方面的巨大挑战。

a) 代码分发的可靠性、迅速性和能量有效性。其主要原因是 WSNs 的能量有限性、高度动态性、无线通信环境的有损性和不可靠性。

b) 代码分发的安全性。WSNs 的无线传输特性使其比传统有线网络更加脆弱。另外,为了让需要更新程序映像快速分发到 WSNs 中的所有节点,现有在线代码分发服务大多具有"流行病"(epidemic)特性。为此,网络中任意的一个网络节点被攻击者攻破或俘获,局部的危害就将迅速"传染"至整个网络,并造成惨重的全局后果。

c) 代码分发的机密性。由于 WSNs 代码分发的无线特性,使得代码数据很容易被侦听,这对于军事和重要商业领域有时候将是致命的,而现有的机密性保障方案由于无线传感器节点自身的条件限制而无法直接采用。

现有相关研究对这三方面都有涉及,传输对象优化方面,从编译器层面进行优化的算法,算法实施难度较大,影响了实用效果,而从应用程序预处理层面对函数和全局变量引用进行上层优化的方法是一

个重要的优化方向，另外基于高效的网络编码是优化的另外一个重要方向。

代码分发的安全和机密性方面，基于对称密钥的代码分发认证方法的特点是在接收者和发送者之间需要事先建立一个共享密钥。这使得在代码分发过程中，只要有一个传感器节点被攻破或俘获就意味着通信的共享密钥被泄露，进一步导致整个网络都不再安全。虽然基于非对称密码体制的安全认证方案计算和存储开销比较大，但是可以通过限定数字签名操作只运行一次来降低其复杂度，因此基于PKC的方法已经成为了增强代码分发协议安全性的主流方法。如上所述，虽然基于PKC的认证方法有不少研究工作已经展开，但是仍有很多问题解决得不好或没有受到重视，为各种外部或内部攻击留下了可乘之机，给在线代码分发带来了很大的安全隐患。这些问题包括：

a）现有算法基本都是集中式算法。现有算法都假设网络体系结构中存在一个基站，基站是唯一一个有权发起网络重编程的一方。而且，现有算法操作的是网络内的所有节点，即所有节点都无选择地全部进行了代码更新。在集中式的方案中，基站也是一个备受关注的攻击目标，很容易产生单点故障，系统不易扩充。但是目前为止，支持分布式的代码分发文献非常少，仅有的几篇因为提出的方法采用了较为复杂的密码算法，大大地增大了节点的开销，这对能量有限的无线传感器节点非常不利。

b）在线代码分发安全性的量化分析。现有文献都指出在线代码分发存在着很大的安全隐患，也定性分析了各种安全隐患存在的原因。但是，目前为止，还没有文献对在线代码分发的安全性进行量化分析，而量化分析有助于深入了解在线代码分发安全脆弱性的深层原因，为设计和评价安全的在线代码分发算法提供重要的指导。

c）抗DoS攻击问题。DoS攻击是在线代码分发过程中一个难以避免且最具威胁的攻击类型，攻击的类型和方式非常多，目前已有的在线代码分发认证方案都不能提供良好的抵御DoS攻击的能力，现有研究工作都只能抵御几种他们设定类型的DoS攻击，而且代价比较高或引入了其它潜在的安全隐患。在线代码分发面临着巨大的DoS攻击威胁。

d）缺乏对更新代码的机密性保护。已有的在线代码分发认证方案主要集中于解决代码分发程序映像数据包的一致性认证问题上，忽略了对代码数据包内容本身的保护。但是许多的程序映像尤其是涉及重要商业机密或军事用途的物理网应用环境，其内容本身也是敏感的，需要防止被侦听等。而现有文献鲜有对更新代码提供一致性认证的同时提供机密性保护。

e）缺乏对远程代码映像管理的安全保护。现有代码分发协议缺乏对远程代码映像管理类命令的安全认证，攻击者可以通过伪造程序版本号等简单低代价手段，针对Reboot、Erase命令发动攻击，诱使节点删除有用的代码映像或诱使节点重启到其它不期望或恶意的代码映像。

参考文献：

[1] Hui J W, Culler D. The dynamic behavior of a data dissemination protocol for network programming at scale [C]//Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. Baltimore: Association for Computing Machinery, 2004: 81-94.

[2] Rajesh K P, Khalil I and Bagchi S. Stream: low overhead wireless reprogramming for sensor networks[C]//In 26th Annual IEEE Conference on Computer Communications (INFOCOM), Anchorage: Institute of Electrical and Electronics Engineers Inc, 2007: 928-936.

[3] Rajesh K P, Bagchi S, Khalil I. Efficient wireless reprogramming through reduced bandwidth usage and opportunistic sleeping[J]. Ad Hoc Networks Journal, 2009, 7(1): 42-62.

[4] Rajesh K P, Khalil I, Bagchi S, et al. Single versus multi-hop wireless reprogramming in sensor networks [C]//In 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (Tridentcom'08), March 2008, Innsbruck: ICST, 2008: 52-61.

[5] Michele R, Giovanni Z, Luca S, et al. SYNAPSE: a network reprogramming protocol for wireless sensor networks using fountain codes[C]//2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'08), San Francisco: Inst of Elec and Elec Eng Computer Society, 2008: 188-196.

[6] Hagedorn A, David S, Trachtenberg A. Rateless deluge: over-the-air programming of wireless sensor networks using random linear codes [C]//In Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN'08), St Louis: Inst of Elec and Elec Eng Computer Societ, 2008: 457-466.

[7] Hou I H, Tsai Y E, Abdelzaher T F, et al. adapcode: Adaptive network coding for code updates in wireless sensor

networks [C]//27th IEEE Communications Society Conference on Computer Communications(INFOCOM'08), Phoenix: Inst of Elec and Elec Eng Computer Societ, 2008: 2189-2197.

[8] Krasniewski M D, Panta R K, Bagchi S, et al. Energy-efficient on-demand reprogramming of large-scale sensor networks[J]. ACM Transactions on Sensor Networks, 2008, 4(1): 114-164.

[9] Du W J, Li Y, Zhang Y T, et al. Adaptive buffer management for efficient code dissemination in multi-application wireless sensor networks[C]//In Proceedings of the 5th International Conference on Embedded and Ubiquitous Computing (EUC'08), Shanghai: Inst of Elec and Elec Eng Computer Societ, 2008: 295-301.

[10] Li W J, Du Y, Zhang Y T, et al. MCP: an energy-efficient code distribution protocol for multi-application WSNs[C]//In Proceedings of 5th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS'09), Marina del Rey: Springer Verlag, 2009: 259-272.

[11] Bence P, Luca M, Cecilia M, et al. Selective code dissemination in mobile wireless sensor networks[C]// Middleware'08 Companion, Leuven: Springer Verlag, 2008: 113-115.

[12] 周虹宇, 周激流, 林　锋. 一种容延迟移动传感器网络中的代码分发机制[J]. 四川大学学报: 自然科学版, 2008, 45(5): 1089-1094.

[13] Zhang Y T, Yang J, Li W J. Towards energy-efficient code dissemination in wireless sensor networks[C]//In Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS'08), Miami: Inst of Elec and Elec Eng Computer Society, 2008: 923-940.

[14] Li W J, Zhang Y T, Yang J, et al. UCC: update-conscious compilation for energy efficiency in wireless sensor networks[C]//In Proceedings of the 2007 PLDI conference, New York: Association for Computing Machinery, 2007: 383-393.

[15] Li W J, Zhang Y T, Yang J, et al. Towards update-conscious compilation for energy-efficient code dissemination in WSNs [J]. Transactions on Architecture and Code Optimization, 2009, 6(4): 214-228.

[16] Rajesh K P, Bagchi S, Midkiff S P. Zephyr: efficient incremental reprogramming of sensor nodes using function call indirections and difference computation [C]//In the USENIX Annual Technical Conference (USENIX'09), San Diego: Association for Computing Machinery, 2009: 411-424.

[17] Rajesh K P, Bagchi S. Hermes: fast and energy efficient incremental code updates for wireless sensor networks [C]//28th Conference on Computer Communications (IEEE INFOCOM 2009), Rio de Janeiro: Institute of Electrical and Electronics Engineers Inc., 2009: 639-647.

[18] Lanigan P E, Gandhi R, Narasimhan P. Sluice: secure dissemination of code updates in sensor networks[C]// IEEE International Conference on Distributed Computing Systems (ICDCS'06), Lisbon: Institute of Electrical and Electronics Engineers Inc., 2006: 201-208.

[19] Dutta P K, Hui J W, Chu D C, et al. Securing the deluge network programming system[C]//In Proc. of the 5th International Conference on Information Processing in Sensor networks (IPSN'06), Nashville: Inst of Elec and Elec Eng Computer Society, 2006: 326-333.

[20] Deng J, Han R, Mishra S. Secure code distribution in dynamically programmable wireless sensor networks [C]//ACM/IEEE Conference on Information Processing in Sensor Networks, Nashville: Inst of Elec and Elec Eng Computer Society, 2006: 292-300.

[21] Deng J, Han R, Mishra S. Efficiently authenticating code images in dynamically reprogrammed wireless sensor networks [C]//IEEE Third International Workshop on Pervasive Computing and Communication Security (PerSec'06), Pisa: Institute of Electrical and Electronics Engineers Computer Society, 2006: 272-276.

[22] Barr K, Asanovic K. Energy aware lossless data compression [J]. ACM Transactions on Computer Systems, 2006, 24(3): 250-291.

[23] Park K, Lee J H, Kwon T Y, et al. Secure dynamic network reprogramming using supplementary hash in wireless sensor networks[C]//Ubiquitous Intelligence and Computing-4th International Conference(UIC'07), Hong Kong: Springer Verlag, 2007: 653-662.

[24] Shaheen J, Ostry D, Sivaraman V, and Jha S. Confidential and secure broadcast in wireless sensor networks[C]//In IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Hong Kong: Institute of Electrical and Electronics Engineers Inc, 2007: 653-662.

[25] Dong Q, Liu D G, Ning P. Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks[C]//In WiSec'08: Proceedings of the first ACM conference on Wireless network security, New York: Association for Computing Machinery, 2008: 2-13.

[26] Tan H L, Ostry D, Zic J, et al. A confidential and

DoS-resistant multi-hop code dissemination protocol for Wireless Sensor Networks[C]//In Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec'09), Zurich: Association for Computing Machinery, 2009: 245-252.

[27] Hyun S W, Ning P, Liu A, et al. Seluge: Secure and dos-resistant code dissemination in wireless sensor networks[C]//In Proc of the 5th International Conference on Information Processing in Sensor networks(IPSN'08), St Louis: Inst of Elec and Elec Eng Computer Society, 2008: 445-456.

[28] Ning P, Liu A, Du W L. Mitigating dos attacks against broadcast authentication in wireless sensor networks[J]. ACM Trans Sen Netw, 2008, 4(1): 1-35.

[29] Zhang Y, Zhou X S, Ji Y M, et al. Secure and dos-resistant network reprogramming in sensor networks based on CPK[C]//In the 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Dalian: Inst of Elec and Elec Eng Computer Society, 2008: 236-241.

[30] Du X, Guizani M, Xiao Y, et al. Defending dos attacks on broadcast authentication in wireless sensor networks [C]//In IEEE International Conference on Communications (ICC'08), Beijing: Institute of Electrical and Electronics Engineers Inc, 2008: 1653-1657.

[31] Law Y W, Zhang Y, Jin J M, et al. Secure rateless deluge: pollution-resistant reprogramming and data dissemination for wireless sensor networks[J]. EURASIP Journal on Wireless Communications and Networking, 2011: 1-22.

[32] Zhang R, Zhang Y. C. LR-Seluge: Loss-resilient and secure code dissemination inwireless sensor networks [C]//31st International Conference on Distributed Computing Systems (ICDCS 2011), Minneapolis: Institute of Electrical and Electronics Engineers Inc, 2011: 497-506.

[33] He D J, Chen C, Chan S, et al. DiCode: dos-resistant and distributed code dissemination in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2012, 11(5): 1946-1956.

[34] He D J, Chen C, Chan S, et al. SDRP: a secure and distributed reprogramming protocol for wireless sensor networks [J]. IEEE Transactions on Industrial Electronics, 2012, 59(11): 4155-4163.

[35] He D J, Chen C, Chan S, et al. Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks [J]. IEEE Transactions on Industrial Electronics, 2013, 60(11): 5348-5354.

[36] Kim D H, Gandhi R, Narasimhan P. Exploring symmetric cryptography for secure network reprogramming[C]//In International Workshop on Wireless Ad-hoc and Sensor Networks, Toronto: Institute of Electrical and Electronics Engineers Inc, 2007: 223-231.

[37] Perrig A, Canetti R, Song D, et al. Efficient and secure source authentication for multicast[C]//In Proceedings of Network and Distributed System Security Symposium, San Diego: Institute of Electrical and Electronics Engineers Inc, 2001: 35-46.

[38] Krontiris I, Dimitriou T. Authenticated in-network programming for wireless sensor networks [C]//In International Conference on Ad-Hoc Networks and Wireless, Ottawa: Springer Verlag, 2006: 390-403.

[39] Tan H L, Jha S, Ostry D, et al. Secure multi-hop network programming with multiple one-way key chains[C]//In WiSec'08: Proceedings of the 1st ACM Conference on Wireless Network Security, Alexandria: Association for Computing Machinery, 2008: 183-193.

[40] Bohli J M, Hessler A, Ugus O, et al. Security Enhanced Multi-Hop over the Air Reprogramming with Fountain Codes[C]//The 4th IEEE International Workshop on Practical Issues In Building Sensor Network Applications (SenseApp'09), Zürich: IEEE Computer Society, 2009: 50-857.

[41] Dennis K, Nilsson T R, Lindqvist U, et al. Key management and secure software updates in wireless process control environments[C]//In WiSec'08: Proceedings of the first ACM conference on Wireless network security, New York: Association for Computing Machinery, 2008: 100-108.

The Latest Research Progress on Online Code Distribution of Wireless Sensor Networks

ZHANG Guo-ping

(School of Information Science and Technology,
Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Online code distribution of WSNs (wireless sensor networks) is an important means to expand WSNs application life cycle. It is a process of re-assigning long-distance tasks, updating node software and re-configuring network functions after sensor networks complete deployment the first time. Existing online code distribution researches can be roughly classified into three types: the transmitting object optimization algorithm with the purpose of reducing the data package and improving energy consumption effectiveness; security authentication algorithm based on asymmetrical secret key cryptograph with the purpose of enhancing code distribution security; security authentication algorithm based on symmetric key with the purpose of enhancing code distribution security. It is found through comparison that in existing researches, code distribution algorithm based on efficient network code can well reduce communication load. Although security authentication scheme based on symmetric cryptosystem costs highly in calculation and storage, it can greatly enhance code distribution security. So, it is a mainstream method to boost code distribution security. Finally, this paper summarizes the following defects of existing code distribution algorithms: centralized-type, lack of quantitative analysis and anti-DoS (Denial of Service) attack. Besides, this paper provides suggestions on further studying these problems.

Key words: wireless sensor networks; code distribution; security authentication; reprogramming

(责任编辑:陈和榜)