

移动自组网中一种优化的局部声誉系统

谭长庚, 陈松乔, 王建新

TAN Chang-geng, CHEN Song-qiao, WANG Jian-xin

中南大学 信息科学与工程学院, 长沙 410083, China

School of Information Science and Engineering, Central South University, Changsha 410083, China

E-mail: cgtan@mail.csu.edu.cn

TAN Chang-geng, CHEN Song-qiao, WANG Jian-xin. Optimized local reputation system in mobile Ad hoc networks. Computer Engineering and Applications, 2008, 44(9): 20-23.

Abstract: In mobile ad hoc networks, nodes cooperate by forwarding packets for each other to allow them to communicate. The cooperation of nodes is very important. With lack of a prior trust relationship, the cooperative security schemes offer the effective solution to resolve the uncooperative behavior which launched by the malicious and selfish nodes in the mobile ad hoc networks. we present that an Optimized Local Reputation System. In our approach, reputation is exchanged in k -hop neighborhood, which not only can reduce the cost of system but also can fully learn the experiences from its neighbors. Binary Exponential Backoff Algorithm is adopted to deal with the uncooperative nodes. Our approach can effectively inspire the nodes to cooperate, and enhance the performance of mobile ad hoc networks.

Key words: mobile Ad hoc networks; network security; reputation system; cooperation

摘 要: 移动自组网节点间的通信由多个节点相互协作来完成, 节点合作与否是实现通信的关键。在缺少预先约定的信任关系时, 合作性的安全机制是解决网络内部恶意节点和自私性节点不合作行为的有效方法。提出了一种优化的局部声誉值合作性方案, 该方案只在 k 跳邻居内交换声誉值, 系统开销小, 并能充分学习邻居的经验。采用二进制指数后退算法对不合作节点进行处置, 能有效激励节点的 cooperativeness, 提高网络的性能。

关键词: 移动自组网; 网络安全; 声誉系统; 合作性

文章编号: 1002-8331(2008)09-0020-04 **文献标识码:** A **中图分类号:** TN913.24

1 引言

移动自组网是一种不依赖于固定网络设施, 能够快速展开的、自治的、多跳的网络结构, 它由多个带有无线收发装置, 可以自由移动的节点组成。这种网络建立方便快捷, 灵活, 不受网络基础设施的制约, 在需要固定网络设施支持的通信网络遭破坏后, 这种分布式控制和无中心的网络结构由于具有较好的鲁棒性与抗毁能力, 它能够维持剩余通信能力, 确保重要的通信指挥畅通, 因而可以用于救灾, 国防战备等需要建立临时通信网络的环境中, 具有广泛的应用前景。

在移动自组网中, 每个节点既是主机, 又是路由器, 节点间的通信通过无线信道、由多个节点转发来完成。它具有拓扑结构动态变化、传输范围与带宽有限、能源受限和分布式控制的特点。移动自组网本身的特点使其比固定网络更容易遭受各种安全的威胁: 无线通信的广播本质使其更容易受到窃听、通信量分析、篡改等攻击; 移动节点漫游中可能被俘获, 使自组网面临来自内部叛变节点的攻击; 网络拓扑结构变化频繁、节

点数不断变化, 节点信任关系也随之变化; 网络功能的执行需要多节点协作, 由于自私节点的存在, 这种协作易遭破坏等。由于移动自组网具有诸多系统脆弱性, 所以容易遭受多种攻击, 加之没有基础设施的支持, 没有可信任的认证中心来提供身份认证等服务, 传统的安全机制在移动自组网中难以实现。目前, 没有一种传统的安全机制能够比较有效地抵制来自内部恶意节点、叛变节点或自私性节点的攻击(把恶意节点、叛变节点和自私性节点统称为不合作节点), 因此需要采用新的方案来保证网络的安全。

针对移动自组网中节点的不合作行为, 本文给出了一个优化的局部声誉系统模型, 用以激励节点相互合作, 共同完成网络的基本功能。

2 相关研究工作

为了激励节点的合作性, Levente Buttyan 等提出了两种虚拟货币的合作性方案^[1]: 钱包方式(费用由发送方支付)和购买

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60403032); 博士点基金(Specialized Research Foundation for the Doctoral Program of Higher Education of China under Grant No.20060533057)。

作者简介: 谭长庚(1963-), 男, 博士研究生, 副教授, 主要研究方向: 移动自组网的路由协议和性能评价; 陈松乔(1940-), 男, 教授, 博导, 主要研究方向: 软件工程与计算机网络; 王建新(1969-), 男, 博士, 教授, 博导, 主要研究方向: 路由算法及网络性能评价。

收稿日期: 2007-11-13 **修回日期:** 2007-12-26

方式(费用由接收方支付)。在钱包方式中,源节点将发送报文所需的虚拟货币数放入钱包内,钱包随报文一起发送,每经过一个节点,钱包内货币数减1,直至目的节点。该方式中,源节点难以精确计算报文转发的费用,有可能源节点所放的筹码数少于转发报文所需的筹码数,最终使报文不能到达目的节点。在购买方式中,中间节点从其上游节点购买下该报文,然后加上本节点的转发费用再卖给下游节点,直到目的节点。该方式因为发送者无需支付发送费用,可能存在滥发报文的情况。这两种方式每个报文都要携带货币,增加了报文的长度,增加了开销。另外难以防止中间恶意节点私自侵吞货币。文献[2]作者提出了改进方案,每个节点都安装有一个防止用户修改的安全卡以记录各节点报文发送筹码。Sprite^[9]用清算中心 CCS(Credit Clearance Service)替代了安全卡。清算中心存储每个节点的筹码数,计算每个节点的开销(发送报文数)和收入(转发报文数)。当节点转发一个信息时,该节点保留其票据,然后与清算中心联系,上传该票据。清算中心根据报文转发情况付给参与转发节点相应的筹码,同时减去发送节点发送报文总筹码。此方案优点是不需要硬件支持,防止发送方发送大量无用报文发起拒绝服务攻击。缺点是由于清算中心的存在,容易引起单点失败。

Watchdog and pathrater^[4]方案通过 Watchdog 来检测具有不良行为的节点,由 pathrater 根据不同的行为来更改相应节点的声誉值,并根据路径中节点的平均声誉值水平来选择路由,避开不良节点。该方案只是简单标记了节点的声誉值,在路由选路时绕过不良节点,并没有惩罚不良节点。

CONFIDANT^[5]的目标是检测并孤立不合作节点,以此来促使节点的相互合作,并根据节点的声誉水平选择路由。该协议使用全局声誉值,通过发送报警信息来达到共享声誉信息的目的。这样可以充分学习别人的经验,快速的惩罚不合作节点。但报警信息在传输过程中有可能被篡改,且存在错误控告等问题。

CORE^[6]通过使用联合监测技术和声誉值机制来激励节点合作。由两部分组成:看门狗机制和声誉值表。看门狗用来检测节点的不良行为,声誉值表用来存储节点的声誉值。表中每行由四部分组成:节点 ID、自己观察所得的自主声誉值、由其他节点所提供的间接声誉值和功能性声誉值。综合这三种类型的声誉值计算节点声誉值,当某节点的声誉值低于阈值时,其他节点拒绝为其提供服务,从而将不合作节点排除出网络。该协议也使用全局声誉值,通过交换正的声誉值来达到共享的目的。考虑到网络中各功能的重要性不同,CORE 对不同的信息发送赋予不同的权值,但增加了声誉值系统的复杂性。另外,声誉值在传输过程中有可能被篡改,节点有可能发送不真实的声誉值。

OCEAN^[7]和 LARS^[8]都采用本地声誉值,每个节点只保留到它一跳邻居的声誉值,声誉值的更新只依赖自己直接观察所得,不存在声誉值的交换。OCEAN 方案中节点声誉值初值为0,如果是良好行为则加1,不良行为则减2。当某一节点其声誉值低于-40时,就将其加到错误列表中。该方案由五部分组成:邻居监控用来检测邻居节点行为;路由级别表用来存储每一个邻居节点的声誉值;路由选择根据节点的声誉值来选择路由,避免选择包含有错误列表中节点的路由;恶意流拒绝器用来拒绝从恶意节点发出的信息。LARS 为了减轻自私节点和恶意节点的影响,当一个不合作节点被辨别出来后,它的 k 跳邻居都会接到警告信息,从而拒绝为不合作节点服务。为了防止错误

报告和声誉值不一致问题,警告信息在广播前,必须得到 m 个一跳邻居节点的签名。对不合作节点,OCEAN 和 LARS 都采用了二次机会制,让错误节点有机会再参与网络运行,并采取了一定的措施来解决错误控告和声誉值不一致问题,但增加了协议的复杂性。另外,由于使用二次机会机制,不像全局声誉值系统那样严厉的惩罚不良节点,可能会带来恶意节点的重复攻击。

文献[9]给出了一个声誉机制评价模型,提出了基于声誉机制的安全路由协议 S-DSR。S-DSR 协议在选路过程中,只选择满足一定声誉值的节点,RREQ 包携带一个请求声誉值和一个黑名单,避免包含不满足条件的节点。该协议给出了比较合理的声誉值的计算与更新过程,而且能根据用户自己的需求来定义安全级别,但对不合作节点没有采取惩罚措施,只是绕过不合作节点。

3 一种优化的局部声誉值的合作性方案

本文提出了一种优化的局部声誉值系统模型 OLSR(an Optimized Local Reputation System),该方案采用局部声誉值,即每个节点都保持有到它 k 跳内邻居节点的声誉值,声誉值的交换只在 k 跳邻居内进行。这样既可以减少声誉值在网络中的传输,又可以充分学习别人的经验来提高自己的判断能力。

移动自组网由于节点的传输范围有限,节点间的通信往往需要经过多个节点转发来完成。但节点更关心的是其周围邻居节点的合作性,因此节点没有必要记录远离自己的节点的声誉情况。在移动自组网中,节点的移动具有连续性,移动节点必定是先在邻居区域内移动。如果节点只记录其一跳邻居的声誉情况,节点移动时,当它移出原一跳邻居范围时,其声誉值丢失。其他节点因没有它的声誉记录,把它当作新加入节点重新记录其声誉情况。如果节点记录有到它 k 跳以内邻居的声誉情况,在一个局部范围内,节点间可以相互学习彼此的经验。对一个表现良好的节点,它当然希望自己辛苦建立起来的声誉得到更多的人认可,可以保持尽可能长的时间。对于表现不良的节点,当然是知道的人越多越能抵制它的破坏行为。

3.1 模型组成

本文对所研究的优化的局部声誉值方案将工作在如下的网络环境中:

- (1)双向链路。即在 T 时刻,节点 A 可以收到节点 B 发给它的信息,反过来节点 B 也可以收到节点 A 发给它的信息;
- (2)节点工作在混杂侦听模式下,能侦听到其邻居节点的行为;
- (3)节点有唯一的 ID,且在网络运行期间不能随便改动;
- (4)节点有足够的存储空间和计算能力;
- (5)节点不属于单个权威机构,它们没有共同的目标,网络中存在恶意节点和自私节点,没有事先定义的信任关系。

OLSR 由以下三部分组成:邻居监视、声誉系统和路径管理。

邻居监视:当节点给其下游节点发送一个信息包时,缓存该信息包,打开监控模式,侦听下游节点是否转发该数据包,并与缓冲区的数据包比较。若匹配,则证明发送成功,释放缓冲区的信息包;若不匹配,则说明下游节点修改了该信息包。如果在规定时间内节点没有侦听到下游节点转发该信息包,则说明下游节点丢弃了该包。邻居监视将所侦听到的情况告知声誉系统。

声誉系统包含两个部分:声誉值表和声誉管理。声誉值表由五部分组成:节点 ID,信任水平(Trust),自主声誉值(Subjective Reputation),声誉值(Reputation)和标志(Flag)。信任水平

表示该节点的可信程度,自主声誉值是节点直接观察所得的声誉值,声誉值是由自主声誉值和从其他节点发送过来的间接声誉值计算得来的声誉值,用来作判断节点行为好坏的标准。标志(F)用来标记某节点是否为不合作节点。当一个节点的声誉值低于某个阈值时,即为不合作节点,其标志位置 1;合作节点的标志位为 0。声誉管理负责节点声誉值的计算、更新以及与其他节点间进行声誉值的交换。

路径管理根据节点的声誉值来选择路径。主要有以下几个功能:

(1)负责路由选择。根据节点的声誉值来选择一条比较可靠的路径,避免不合作节点参与路由;

(2)处理节点发起的路由请求。根据节点的声誉值来定义发送优先级,优先发送声誉值高的节点的路由请求,拒绝恶意节点发起的路由请求;

(3)处理收到包含恶意节点的路由应答包。当发现路由应答包中包含有恶意节点时,删除该源路由。

3.2 信任水平和声誉值的计算与更新

3.2.1 信任水平 T 的计算

在许多声誉系统中,声誉值通常作为信任的一个度量。Sonja Buchegger 等在文献[10]中对信任和声誉做了区分。对任一节点,声誉水平代表了这个节点行为好坏如何,用来判断这个节点是合作节点还是不合作节点;而信任水平则代表了这个节点诚实程度,用来判断该节点是否可信。本文提出了一种新的信任水平描述方法,即用节点有效报文转发率 T 来表示:

$$T = \frac{\text{successful_chipcounts}}{\text{chipcounts}} \quad (1)$$

其中, chipcounts 是节点给下游发送报文的数目, $\text{successful_chipcounts}$ 则是下游节点成功转发的报文数。每当节点给下一跳节点发送一个报文时, chipcounts 加 1, 节点通过侦听下一跳节点的发送情况, 若转发成功, 则 $\text{successful_chipcounts}$ 加 1。每个节点的 T 的初始值为 0.5, 一旦参与转发报文后, 节点的信任水平 T 就会发生变化。信任水平只依赖于节点自己的观察, 节点的信任水平则制约着节点声誉值的更新。

3.2.2 声誉值的计算与更新

设 i, j, k 为任意节点, 有下面的定义:

定义 1 自主声誉值: 节点 i 通过自己的观察获得的节点 k 的声誉值, 称为 i 对 k 的自主声誉值, 记为 SR_{ik} 。

定义 2 间接声誉值: 由节点 j 发送给 i 的关于节点 j 对节点 k 的声誉值为间接声誉值, 记为 R_{jk} 。

一个节点的声誉值由自主声誉值与间接声誉值决定。自主声誉值与间接声誉值的变化会导致声誉值 R 的改变, 而这两者引起的变化往往不是同步的, 也就是说它们对声誉值的影响是独立的, 因此将分别就这两方面来计算声誉值 R 。

(1)自主声誉值的计算及其对声誉值的影响

节点通过自己的观察来改变相应节点的自主声誉值(如节点 i 观测到节点 k 的自主声誉值), 根据公式(2)和(3)来计算:

$$\text{合作行为: } SR_{ik} = SR_{ik} + \text{value1} \quad (2)$$

$$\text{不合作行为: } SR_{ik} = SR_{ik} - \text{value2} \quad (3)$$

其中, value1 和 value2 是相应增加或减少的值, 且 $\text{value1} < \text{value2}$, 即惩罚重于奖励, 以此激励节点的合作。

为了合理反映 SR 对 R 的影响, 对 SR 与 R 进行加权求和, 用公式(4)来表示 SR 对 R 的影响:

$$R_{ik} = SR_{ik} * \alpha + R_{ik} * \beta \quad (4)$$

其中, α, β 为权值, $\alpha + \beta = 1$, 且 $\alpha < \beta$, 表明旧声誉值的权重比较大。当节点对某节点的自主观测值 SR 的改变量超过某个门限值 ΔSR 时, 即会触发 R 的更新。

(2)间接声誉值对声誉值的影响及声誉值的交换

本方案通过交换节点声誉值来达到共享声誉信息的目的。声誉值的交换只在以下两种情况下发生:

①当某节点的声誉值低于某个阈值 R_u , 即该节点被认为是不合作节点时, 观测节点会将此情况告知其他节点;

②当某节点的声誉值大于 R_u , 且改变量大于阈值 ΔR 时, 也会触发声誉值的交换。

为了减少声誉值在网络中的传输量, 只给 k 跳邻居节点发送 REP 包(Reputation Exchange Packets), 该包包含了评价节点 ID、被评价节点 ID、被评价节点的声誉值、一个唯一标志包的序列号以及跳数。跳数设为 k , k 跳后该包将被丢弃。

假设 i 为待更新节点, k 为 i 节点要更新其新声誉信息的节点, j 为向 i 发送 k 的更新声誉信息的节点。当 j 节点观察到 k 节点的声誉值超过某个阈值时给节点 i 发送节点 k 的声誉值 R_{jk} 。接收到该包的节点 i 首先查看评价节点 j 和被评价节点 k 的标志位, 若其中一个为 1, 则丢弃该包(评价节点标志位为 1, 说明该节点不可信, 应该丢弃其发起的 REP 包; 被评价节点标志位为 1, 则说明该节点为不合作节点, 不予更新其声誉值); 若都为 0, 则按公式(5)计算 i 对 k 的声誉评价价值 R_{ik} :

$$R_{ik} = R_{ik} + (R_{jk} - R_{ik}) * T_{ij} \quad (5)$$

其中 T_{ij} 表示节点 i 对节点 j 的信任水平。声誉值的更新根据发送声誉值节点的信任水平来更新, 信任水平高的则更新幅度大, 信任水平低的则更新幅度小, 这样可以有效减少错误控告的不良影响。

3.3 对不合作节点的处置

对不合作节点的处置, 一般采取两种方式: 一是一旦发现某节点为不合作节点, 则马上将其永久排除出网络中, 不再给其改过机会。这样的处罚过于严厉。由于邻居检测存在误判情况, 这样就有可能把由于暂时发生网络错误的节点当作不良节点, 从而将其永久排除。另一种方式是二次机会机制, 即一旦发现某节点为不合作节点, 不是将其永久排除而是禁止其使用网络, 一段时间后, 再让其重新加入网络中, 使其有机会再次参与网络的运行。这种方式比较公平, 但容易带来节点重复攻击。

本文提出了一种合理的处置方法: 二进制指数后退算法。即当某节点被认为是不合作节点时, 其标志位设为 1, 同时启动一个时钟, 时间设为 ReliveTimeOut , 在该段时间内禁止其使用网络, 不改变其声誉值。时钟超时后, 让其“复活”, 重新加入网络中, 标志位清零, 同时声誉值置为 R_u , 再根据其行为来更新声誉值。若其声誉值再次低于 R_u 时, 标志位设为 1, 将时钟时间设为 $2 * \text{ReliveTimeOut}$, 即是上一次的 2 倍。当节点第 n 次被认为是不合作节点时, 推后时间 $2^{n-1} * \text{ReliveTimeOut}$ 进入网络。犯错的次数越多, 等待的时间越长, 直至将其完全排除出网络中。这种方法可以让因为网络错误而导致有不合作行为的节点有重新改过的机会, 而又能比较有效的防止节点的重复攻击。

3.4 有效性分析

所提出的优化的局部声誉值系统模型 OLRs 可以有效的防止节点的不合作行为, 增强节点的合作性。

(1)采用局部声誉值, 即每个节点都只保持有到它 k 跳内邻居节点的声誉值, 声誉值的交换只在 k 跳邻居内进行。这样

既可以减少声誉值在网络中的传输,降低开销,又可以充分学习别人的经验来提高自己的判断能力。

(2)引入信任水平,根据节点的行为来评定节点的信任水平,且信任水平是连续的。根据节点的信任水平来更新相应节点的声誉值,不同信任水平对声誉值的更新权重不一样,使节点声誉值的计算比较合理,同时声誉值计算充分考虑了移动自组网的特性,具有一定的灵活性。

(3)对不合作节点的处置采用二进制指数后退算法,充分考虑了移动自组网自身的特点。由于移动自组网使用无线信道、节点可以自由移动、网络拓扑动态变化,节点间的链路可能会暂时断裂,因此我们给这些节点重新表现的机会,且能较有效的防止恶意节点的重复攻击。

(4)路由选择时,用户可以自定义路径中节点的声誉值水平,只有满足要求的节点才能参与路由,这样可适应不同用户对安全性的要求,具有一定的 QoS 保证。另外,根据节点的声誉值来定义发送优先级,优先发送声誉值高的节点的路由请求,拒绝恶意节点发起的路由请求。这样即惩罚了不合作节点,又给予合作节点相应的奖励,可以更有效的激励节点合作。

4 总结与进一步的研究工作

本文讨论了移动自组网中节点的不合作性问题及现有的典型合作性方案,提出了一种优化的局部声誉值的合作性方案。该方案中使用了一种新的信任水平度量与声誉值计算与更新方法,只在 k 跳邻居内交换声誉值,系统开销小,并能充分学习邻居的经验,采用二进制指数后退算法对不合作节点的处置公平、合理,可以有效激励节点的合作性,保障移动自组网的路由安全,提高网络的性能。进一步的研究工作包括:将本声誉值系统模型应用于具体协议中;把节点的声誉值作为衡量路由安全、链路稳定性的一个指标,在路由选择时综合节点的声誉值、剩余能量、带宽、跳数等因素来选择一条满足某种 QoS 保证的路径,以确保传输的可靠性。

(上接 15 页)

针对信道和电路两方面常用参数范围,通过 MATLAB 计算仿真得到的结果表明,信道传输直接相关的射频输出功率与收发机电路功耗等参数大小分布不同,对于通信链路的能耗有较大的影响。在实际构建无线传感器网络时,应该综合考虑两方面的因素。除了应该尽可能减小电路工作和启动能耗外,在一定的参数条件下,存在较明显的最低能耗下的最佳误帧率和最佳帧长。

参考文献:

- [1] Karl H, Willig A. Protocols and architectures for wireless sensor networks[M]. [S.l.]: John Wiley & Sons Ltd, 2005.
- [2] Sankarasubramaniam Y, Akyildiz I F, Mclaughlin S W. Energy efficiency based packet size optimization in wireless sensor networks[C]// Proceedings of the 1st IEEE International Workshop on Sensor Network protocols and Applications(SNPA), Anchorage, AK, May 2003.

参考文献:

- [1] Buttyan L, Hubaux J-P. Enforcing service availability in mobile Ad-Hoc WANS[C]// Proc of the IEEE/ ACM Workshop on Mobile Ad Hoc Networking and Computing(MobiHOC), Boston, MA, USA, August 2000: 87-96.
- [2] Buttyan L, Hubaux J-P. Stimulating cooperation in self-organizing mobile Ad hoc networks[J]. Mobile Networks and Applications, 2003 (5): 579-592.
- [3] Sheng Zhong, Jiang Chen, Y R Yang. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks[C]// The 22nd Annual Joint Conf. IEEE Computer and Communications Societies(INFOCOM 2003), San Francisco, CA, 2003.
- [4] Marti S, Giuli T J, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]// Proc of the 6th International Conference on Mobile Computing and Networking(Mobicom2000), Boston, August, 2000: 255-265.
- [5] Buchegger S, Le Boudec J-Y. Performance analysis of the confidant protocol: cooperation of nodes-fairness in distributed Ad-hoc networks[C]// Proc of IEEE/ ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC2002), EPFL Lausanne, Switzerland, 2002: 226-236.
- [6] Michiardi P, Molva R. Core: a collaborative reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks[C]// 6th IFIP Conference on Security Communications and Multimedia(CMS2002), Portoroz, Slovenia, 2002: 107-121.
- [7] Bansal S, Baker M. Observation-based cooperation enforcement in Ad hoc networks, NI/0307012[R]. Stanford University, 2003.
- [8] Hu Jiangyi. Cooperation in mobile Ad hoc networks[EB/OL]. (2005-01-11). <http://www.cs.fsu.edu/research/reports/TR-050111.pdf>.
- [9] 王建新, 张亚男, 王伟平, 等. 移动自组网中基于声誉机制的安全路由协议设计与分析[J]. 电子学报, 2005, 33(4): 596-601.
- [10] Buchegger S, Le Boudec J-Y. A robust reputation system for P2P and mobile Ad hoc networks[C]// Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, 2004.

- [3] Behzad A, Rubin I. Impact of power control on the performance of ad hoc wireless networks[C]// Proceedings of INFORCOM 24th Annual Joint Conference of the IEEE Computer and Communication Societies, 2005, 1: 102-113.
- [4] Willig A. Intermediate checksums for improving goodput over error-prone links[C]// Proceedings of the IEEE Vehicular Technology Conference(VTC), Fall 04, Los Angeles, CA, September 2004.
- [5] Mangharam R, Rajkumar R, Pollin S, et al. Optimal fixed and scalable energy management for wireless networks[C]// Proceedings of INFORCOM 24th Annual Joint Conference of the IEEE Computer and Communication Societies, 2005, 1: 114-125.
- [6] Garzas J J E, Bousono C, Armada G. An energy-efficient adaptive modulation suitable for wireless sensor networks with SER and throughput constraints[J]. EURASIP Journal on Wireless Communications and Networking, 2007.