# 无线传感器网络安全系统的研究与设计①

何伟文

(广东工贸职业技术学院, 广州 510510)

**摘 要**: 无线传感器网络(WSN)是一种新型无线网络, 它有许多优点; 但是也存在一些问题, 这些问题让攻击者能够更轻易的分析网络安全漏洞, 进行攻击并摧毁整个网络. 本文设计了一个安全的无线传感器网络模型. 它能够抵御大多数已知的网络攻击, 且不会明显降低传感器节点(SN)的能量功率. 我们建议对网络组织进行聚簇以降低能耗, 并基于对信任级别的计算以及可信节点之间信任关系的建立来保护网络, 基于集中式的方法对信任管理系统进行运作. 实验结果表明:本文设计的无线传感器网络模型解决了高效节能的设计任务, 信任管理系统在防御攻击上的结果令人满意.

**关键词**: 无线传感器网络; 聚簇; 信任管理系统(TMS); 信任评估

## Research and Design of Wireless Sensor Network Security System

HE Wei-Wen

(Guangdong Polytechnic of Industry & Commerce, Guangzhou 510510, China)

**Abstract**: Wireless sensor network (WSN) is a new type of wireless network. It has many advantages, but there are also some problems, which allow adversary much easier to analyze network vulnerabilities, to conduct an attack and destroy a whole network. This paper proposes a model of secure wireless sensor network, which is able to defend against most of known network attacks and doesn't significantly reduce the energy power of sensor nodes (SN). We propose clustering as a way of network organization, which reduces energy consumption. Network protection is based on the calculation of the trust level and builds trusted relationships between trusted nodes. Operation of trust management system is based on a centralized method. The experimental results show that the wireless sensor network model designed in this paper solves the task of development of energy efficient; TMS shows satisfied results in preventing the attacks.

**Key words**: wireless sensor network; clustering; trust management system (TMS); trust evaluation

## 引言

无线传感器网络(WSN)是一种基本的新型无线网络, 它基于无限个由有限量电池供电的微型传感器, 旨在收集信息和监控对象. WSN 有优点, 如无线通信信道、动态改变拓扑结构; 但也存在缺点, 如基础设施不足、大数据流和无限量节点、有限电池供电及节点的移动性. 这些问题让攻击者能够更轻易的分析网络安全漏洞进行攻击并摧毁整个网络或某个控制对象. 一般来说, 绝大多数的攻击集中于禁用传感器节点、路由协议定向障碍以及对整个网络的破坏. 目前, 一般有两种防止攻击的方法——加密措施和非加密措施.

加密措施的主要目的是防御外部入侵并防止入侵者渗入网络. 在这种情况下, 如果一个节点被攻击者攻破或捕获, 则作为一个整体网络, 其他节点也会受到威胁[1]. 加密措施在处理和通信中需要大量占用内存并且高功耗, 这使其不适合资源有限的 WSN. 因此, 有必要使用其他安全措施.

非加密方法的目的是防止网络遭受内部攻击. 攻击分析表明, 大多数的攻击都可称之为主动攻击[2]. 在 WSN 中, 主动攻击呈现不同的手法, 数据包可通过

① 收稿时间:2015-11-16;收到修改稿时间:2016-01-29 [doi: 10.15888/j.cnki.csa.005314]

内部攻击者自由进入无线信道. 为使 WSN 网络免受大多数的内部攻击, 我们提供了一个信任管理系统.

本文的目的是为 WSN 开发一套安全的体系结构、算法和协议, 而不会明显降低网络的持续时间和效率. 为实现该目标, 我们需要进行以下工作:

① 开发 WSN 信任管理系统(TMS)的体系结构.

② 开发 WSN 模型及节点模型, 包括拟定的安全方法.

③ 为移动聚簇无线传感器网络的管理, 开发安全协议.

④ 使用模拟的方式评估开发系统的有效性.

## 1 基于聚簇的WSN模型

在许多科学和工程领域, 聚簇一直是将大量的对象组织整理成合适的群组的基本方法. 每一个簇 / 组都有一个领导者, 通常被称为簇头(CH). CH 负责对簇内的其他成员进行验证, 而基站(BS)负责对 CH 进行验证. 因此, 该网络包括了以下类型的节点:SN; CH; BS.

① 传感器节点(SN):它可发送多种类型的报文:信标包用于通告簇中传感器情况; 数据包用于传递正常环境事件的信息; 位置信息提醒 CH 或相邻节点其在空间中的节点位置; 从 CH 接收控制信息; 通过计算信任级别, 参与 CH 的选举.

② 簇头(CH):它发送信标包; 接收并分析来自 SN 及 CH 的报告、警告和信标; 将数据传送至 BS; 验证 SN; 通过分析来自节点和网络流量的数据, 参与信任级别的计算, 并发送通告给 BS.

③ 基站(BS):它保存关于每个 CH 的信息(ID 号及 MAC 地址); 监视 CH 的活动并在遇到攻击时做出决策; 参与节点信任级别的计算; 分析从 CH 得到的数据; 与外部网络进行通信.

## 2 信任管理系统(TMS)

在文献[3]虽然提出了一种水下无线通信网络分级信任管理模型, 但是, 该网络模型没有考虑基站(BS)的决策作用; 另外, 它也没有提供一种安全协议, 以实现网络的安全机制及相关算法. 该模型的簇头是相对固定的, 而我们系统里的簇头是动态、可变的, 为此, 我们设计了簇头重选的算法, 这样, 我们的系统就更能够适应现实环境的复杂性及可变性.

我们设计信任管理系统的主要目的是保护 WSN 免受攻击者恶意行为的伤害. 为实现这一目标, 我们需要进行以下工作:探测攻击者的非法行动; 阻止恶意节点; 防止攻击; 确定真正的节点; 在真正的节点间建立可信连接; 检测出有缺陷的节点并将其拦阻.

我们系统的主要目的之一是在能效和可靠性之间寻找平衡点. 我们将可靠性与尽可能长时间的抵御攻击的能力相结合. 能效指的是使用较少的能量, 尽可能长时间的维护网络的可操作性的能力. 为降低能耗, 我们采用以下措施:

① 一个可以降低传感器功耗的方法是将其从活动状态转变为“休眠”状态, 使其能耗最小化. 这可以通过减少节点间的分组转发来实现. 在该模型下, WSN 被分为多个簇.

② 减少 SN 的计算量.

③ 使用数据聚合的方法使 WSN 中的能耗最小化.

④ 采用聚合器(或 CH)收集来自其他节点的信息, 计算聚合函数, 并将其值传送至网络协调器(或 BS). 与没有聚合器的情况相比, 信息传递的总成本明显降低了.

TMS 架构如图 1 所示.

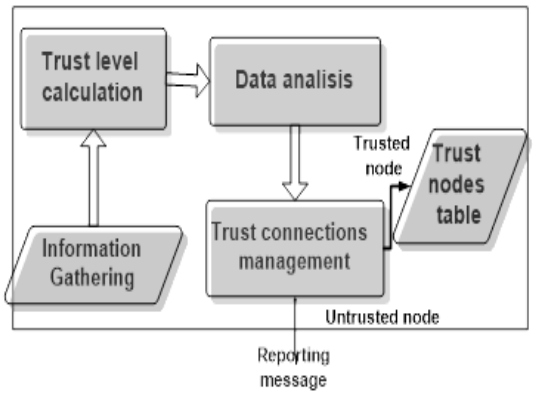


图 1　信任管理系统(TMS)架构

信息采集模块从 SN 获取信息并用来计算信任级别. 然后, 根据节点类型, 对结果进行分析. SN 没有信任连接管理模块. 该模块处理有关节点 N 的信息. 如果节点 N 成功通过测试, 则与 N 有关的数据会进入信任节点表中. 因此, 在同一个簇中的所有节点都将收到关于节点 N 的报文. 如果节点 A 检测到节点 B 存在异常, 则节点 A 会对 CH 发出信息, 由 CH 做出有关节点

B 的决定.

### 2.1 信息采集模块

处于相同无线传输及接收范围内的两个节点称为邻居. 由于无线介质的广播特性, 给定的节点可收集有关数据包的第一手资料, 通过侦听 MAC 层收到的所有帧并记录数据包的传输数据, 将其相邻节点的行为进行转发[4]. 如果是基于簇的 WSN, 则还须增加一个条件, 即节点必须处于同一个簇中. 为检测恶意行为, 我们应先明确攻击的属性. 简而言之, 这些参数如下:

① 接收/转发/发送数据包;

② 接收/转发/发送路由数据包;

③ 接收/转发/发送控制报文;

④ 能荷水平;

⑤ 带信任度值的报文;

⑥ 改变分组地址;

⑦ 基于信标包的可用性.

### 2.2 信任级别计算模块

在文章[5]中给出了一些用于计算信任级别的公式.

$$T_i^{A,B} = \frac{a_i S_i^{A,B} - b_i F_i^{A,B}}{c_i S_i^{A,B} - d F_i^{A,B}} \quad (1)$$

此处, $Ti^{AB}$ --- 为节点A关于节点B的信任值, $Si^{AB}$ ---为A测得B的i型事件的成功数量, $Fi^{AB}$ 为A测得B的i型事件的失败数量, 而ai、bi、ci、di 代表了成功事件的权重 / 重要性相对于失败事件的权重 / 重要性.

每个网络事件都将计算信任度值, 并在表中进行考虑. 然后将这些与行为相关的信任值乘以权重因子($W_i$), 反映其在安全层级的重要性, 再相加以得出整体节点的可靠性, 如以下公式所示.

$$DT^{A,B} = \sum_{i=1}^{k} W_i * T_i^{A,B} \quad (2)$$

在此步骤中, 应计算以下数值:

① $Q_i^k(E)$- 剩余能量水平;

② $M_Y$ – 节点的流动性级别;

③ d – 与基站的距离[6];

④ S – 稳定性级别;

$$S = \frac{\omega_1 Q_i^k + \omega_2 DT^{A,B}}{\omega_3 M_Y} \quad (3)$$

### 2.3 信任连接管理模块

该模块按照以下算法工作, 以确定置信水平:

步骤1: CH从分析仪获取参数.

步骤2: CH请求传感器节点$N_i$提供$Q_i^k(E)$和$DT^{ni}$

步骤3: CH用公式2根据接收的参数计算$DT^{nj}$.

步骤4: CH将值进行比较:如果$DT^{ni} = DT^{nj}$, 则继续算法, 否则发送了不正确值的$N_i$将变为不受信任.

步骤5: CH将($Q_i^k(E)$)与发送的数据包数量(总包量Total pack)进行比较. 应保持下列条件:

1) $\begin{cases} Q_i^k(E) = \max \\ \text{Total pack} = \min, \text{average} \end{cases}$

2) $\begin{cases} Q_i^k(E) = \text{average} \\ \text{Total pack} = \text{average}, \text{threshold} \end{cases}$

3) $\begin{cases} Q_i^k(E) = \max \\ \min < Total\ pack < max \end{cases}$

步骤6:如果可保持这些条件, 则Ni是可信的, 否则需要对发送的数据包类型进行分析:

① 如果大多数数据包为管理型, 则$N_i$ =不可信

② 如果大多数数据包为路由型, 则$N_i$ =不可信

③ 如果大多数数据包为数据型, 则$N_i$ =不确定

## 3 用于管理移动聚簇无线传感器网络的安全协议

本文的主要目的之一在于提供一种协议, 以保护移动传感器网络免受所有主要类型的网络攻击, 同时不会明显降低节点的功耗及其网络的预期寿命. 在拟定的协议中, 我们实现了以下安全机制及算法:用于确定网络节点置信水平的算法; 协议初始化算法; 簇头预选算法; CH 重选算法; 节点迁移算法[7].

### 3.1 节点初始化算法

① 基站将初始化消息(MsI)发送至所有网络节点.

② 所有节点(N)因此收到 MsI, 并根据超时定义以相同的方式发送一个响应消息 R-MsI 至 BS. BS 接收到有关节点 ID 的信息并检查序列号(SerNum)的比率.

③ 初始化过程中的最后一步是一个来自基站的报文 ACK-MsI. 这个报文会发送到所有配置的节点, 而如果有节点未收到该报文, 则 BS 将会认为其是可疑的或存在恶意的.

④ 已初始化的节点会标记为可信的. 另一方面, BS 也会将这些节点加入可信节点的列表中, 且将来的簇头将会在这些节点中选出. 初始化流程有两个目的. 第一, 在基站和节点间建立可信的连接. 第二, 基站可存储该网络中受信节点的预加载列表并将其获取的数据与自己的动态列表进行比较.

### 3.2 簇头预选算法

① BS 宣布 CH 甄选开始并向每个节点发出一个特殊消息 ECH-Msg.

② BS 执行“3.1 节点初始化算法”的第③和第④步, 以确定网络节点的置信水平.

③ 如果一个节点已被成功验证, 则基站会注明该节点可以成为 CH.

④ BS 请求已验证的节点提供($Qi^k(E)$).

⑤ BS 对 $Qi^k(E)$的值进行评级并计算出平均值.

⑥ 如果 Ni 的($Qi^k(E)$)值大于或等于平均值, 则将被选为临时 CH.

⑦ 基站向每个节点发出簇头选举完毕的消息.

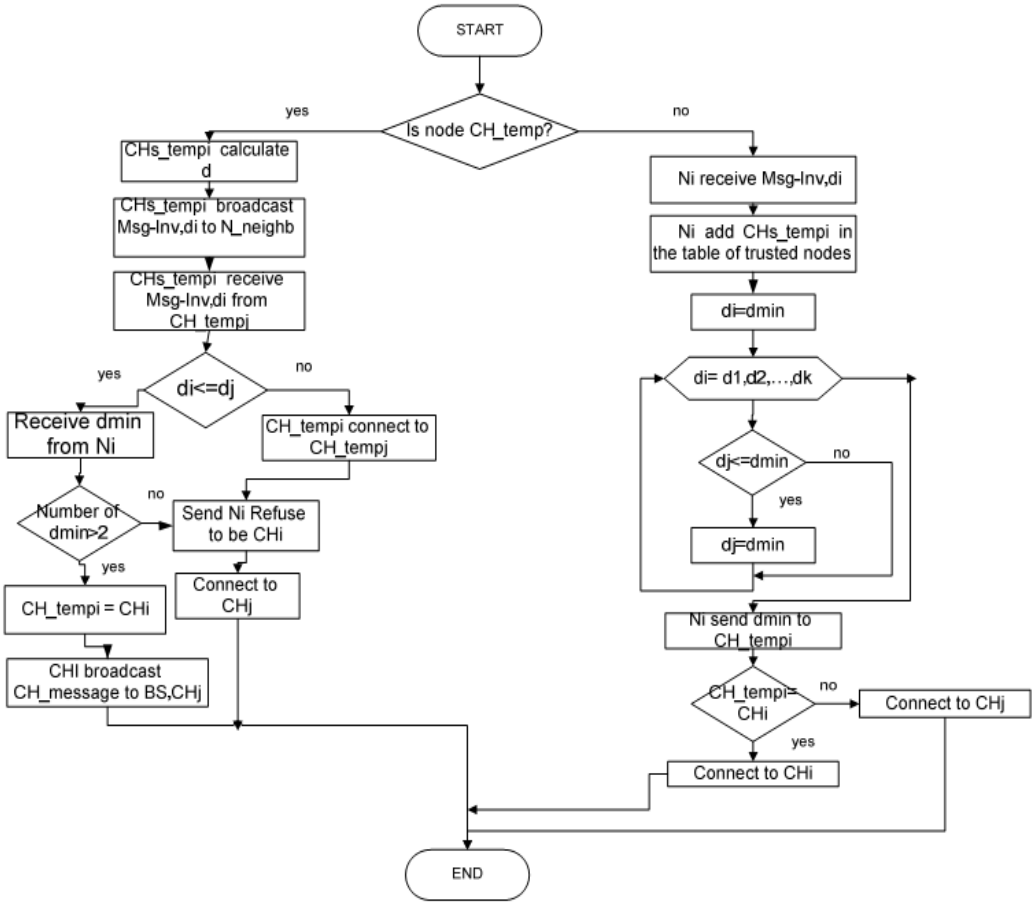


图 2　网络聚簇算法

此外, BS 向每个潜在的簇头 CH_temp 发送其有可能成为 CH 的消息.

当 BS 完成潜在簇头的甄选, 则开始网络聚簇算法. 算法的构思为, 每个临时簇头(CH_temp)都必须计算 CH_temp 与 BS 之间的距离 d. 此后, CH_temp 将该 d 值与加入簇的提议一起发送给相邻的节点. 接下来, 每个节点都确定各自收到的最小值并确认相应的 CH_temp. 另一方面, 每个 CH_temp 都将各自的 d 值与邻居的 d 值(CH_neighb)相比较, 如果它自己的值最小, 则 CH_temp 可自封为簇头(CH)并通知其所有的邻居和 BS. 图 2 展示了网络聚簇算法.

### 3.3 CH 重选算法

重选 CH 的理由:

① 剩余能量水平低于阈值;

② CH 的置信水平低于阈值, 从而被认为是不可信的;

③ CH 处于 BS 和其他网络节点看不见的地方.

具体算法如下:

步骤1: BS定期向CH发送有关以下内容的请求:($Q_i^k(E)$、$D_{T^{A,B}}$、$M_Y$、d)

步骤 2: 如果下列任 一条件成立:

*当前* $Q_i^k(E)$ / 最大 $Q_i^k(E)$ ≤平均值

或*当前* $DT^{A,B}$≤*阈值* $DT^{A,B}$
或*当前* $M_Y$ / 最大 $M_Y$ ≥最大值
或d=最大值.
那么, BS开始重选.

步骤3: $N_i$使用公式3计算$S_i$和$d_i$, 并发送给CH.

步骤4: CH找出Si值最大的Ni
如果Si=Sj, 则CH找出di值最小的Ni

步骤5: di值最小的Ni成为CH_temp

步骤6: CH_temp将($Q_i^k$(E), $DT^{A,B}$, $M_Y$, d, S)发送给CHs和BS.

步骤7: 如果BS或CHs在其信任表中找到了CH_temp, 它们会向CH_temp发送消息(Msg-ACK)表示CH_temp可成为CH, 否则BS和CHs会使用公式3计算CH_temp 的Si. 如果Si > 阈值, 则BS向CH_temp发送Msg-ACK.

步骤8: CH_temp必需从超过半数的曾发过消息的CHs处得到回应(Msg-ACK), 这样, CH_temp才能成为新的CH.

## 4 安全WSN的模拟实验

我们使用 TRMSim –WSN5.0 模拟器来模拟我们的系统[8]. 该模拟器包含了已实现的信任管理模式, 且允许加入自己的模型. 软件可设置以下参数:现有的SN、恶意节点、BS、无线传输范围、执行次数、节点数、模拟网络的数量. 此外 TRMSim 还可以检查动态 WSN 并进行振荡攻击或共谋攻击.

我们进行了以下实验. 首先我们开启 4 个信任模型(BTRM[9]、Eigen[10]、TMS 和 PowerTrust[11]), 然后我们启动共谋攻击, 再然后启动振荡攻击, 最后同时进行所有的攻击. 实验中, 我们从 10%开始改变恶意节点的数量占比直至 90%. 下列参数用于评估其有效性:

① 能耗 – 所有网络节点所消耗的能量总和.

② 准确度 – 选择值得信用的服务器的百分比. 作为一个可接受的信任和信誉模型, 在我们看来, 可信用服务器的选择百分比应该大于或至少等于 70%. 比其小的比例可能导致模型存在某些安全缺陷; 而且可以明确, 如果选择百分比低于 50%, 则该模型完全没有作用[12].

### 4.1 共谋攻击实验

图 3 表示在 WSNs 中, 恶意服务器的百分比从10%到 90%时, 在共谋攻击下, TMS 及其他模型的准确度.

在图中所见, BTRM、Eigen 和 TMS 的结果基本相似, 直到恶意服务器的百分率小于 70 后, BTRM 的结果更佳, 但全部三个模型的准确率都大于 70%. 当恶意服务器的百分率大于 80 时, TMS 的准确率在 60 和 50%之间, 表明存在一定的安全缺陷; 但其他模拟模型的结果基本相同或更差, 而且我们的 TMS 可以对付70%的恶意节点, 这一结果是令我们满意的.

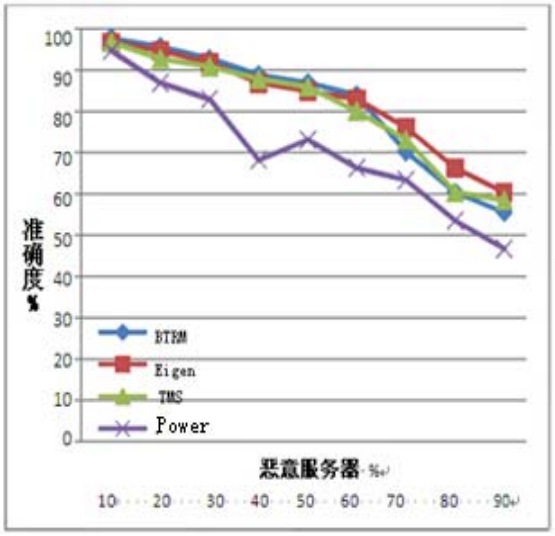


图 3 共谋攻击下动态 WSN 的准确度

表 1 中表示了共谋攻击动态 WSN 的能耗. 我们可以看到, TMS 在所有模型中的能耗最低. 因此, 我们实现了在能耗和可靠性之间的权衡.

表 1 共谋攻击下动态 WSN 的能耗

| 模型 / 恶意服务器(%) | BTRM | Eigen | TMS | Power |
|---|---|---|---|---|
| 10 | $8{,}3*10^9$ | $3{,}1*10^{11}$ | $4{,}4*10^9$ | $5{,}5*10^9$ |
| 20 | $2{,}5*10^{10}$ | $5{,}8*10^{11}$ | $4{,}0*10^9$ | $1{,}7*10^{11}$ |
| 30 | $8{,}7*10^{10}$ | $3{,}2*10^{12}$ | $4{,}0*10^9$ | $1{,}8*10^{11}$ |
| 40 | $1{,}9*10^{11}$ | $6{,}7*10^{12}$ | $4{,}8*10^9$ | $2{,}7*10^{11}$ |
| 50 | $5{,}1*10^{11}$ | $8{,}8*10^{12}$ | $4{,}5*10^9$ | $1{,}7*10^{12}$ |
| 60 | $2{,}5*10^{12}$ | $8{,}4*10^{12}$ | $5{,}2*10^9$ | $2{,}8*10^{12}$ |
| 70 | $1{,}7*10^{12}$ | $8{,}5*10^{12}$ | $7{,}4*10^9$ | $6{,}2*10^{12}$ |
| 80 | $3{,}5*10^{12}$ | $1{,}1*10^{13}$ | $1{,}1*10^{10}$ | $1{,}7*10^{13}$ |
| 90 | $5{,}8*10^{12}$ | $2{,}4*1^{13}$ | $3{,}1*10^{10}$ | $5{,}2*10^{13}$ |

### 4.2 振荡攻击实验

在振荡网络中, 我们的准确度更高. 在图 4 表明: 除了 PowerTrust 以外的所有模型, 其准确度都高于 70%.

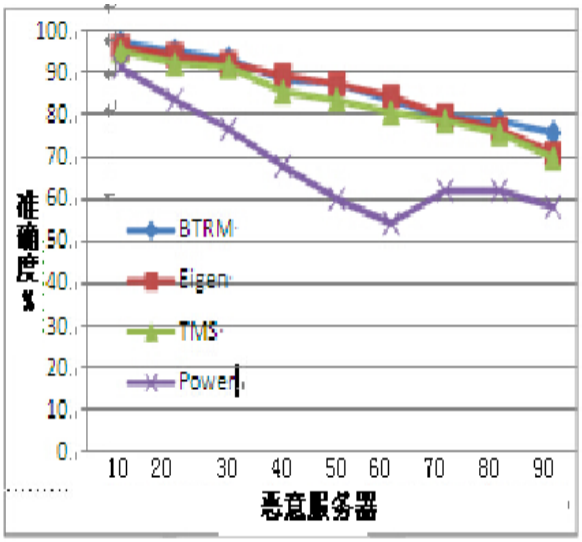


图 4　振荡攻击下动态 WSN 的准确度

表 2 表示振荡攻击下动态 WSN 的能耗. 其能耗小于共谋攻击下的能耗. 而 TMS 的能耗值最小.

表 2　振荡攻击下动态 WSN 的能耗

| 模型 / 恶意服务器(%) | BTRM | Eigen | TMS | Power |
|---|---|---|---|---|
| 10 | $1{,}1*10^{10}$ | $4{,}4*10^{10}$ | $4{,}1*10^{9}$ | $5{,}3*10^{9}$ |
| 20 | $1{,}3*10^{10}$ | $1{,}1*10^{11}$ | $4{,}3*10^{9}$ | $5{,}2*10^{9}$ |
| 30 | $1{,}1*10^{11}$ | $2{,}3*10^{11}$ | $4{,}1*10^{9}$ | $6{,}0*10^{9}$ |
| 40 | $2{,}7*10^{11}$ | $4{,}3*10^{11}$ | $4{,}7*10^{9}$ | $5{,}6*10^{9}$ |
| 50 | $2{,}7*10^{11}$ | $4{,}4*10^{11}$ | $4{,}5*10^{9}$ | $5{,}9*10^{9}$ |
| 60 | $1{,}9*10^{11}$ | $2{,}0*10^{11}$ | $4{,}0*10^{9}$ | $5{,}7*10^{9}$ |
| 70 | $1{,}6*10^{11}$ | $2{,}5*10^{11}$ | $4{,}6*10^{9}$ | $5{,}6*10^{10}$ |
| 80 | $1{,}7*10^{11}$ | $1{,}0*10^{11}$ | $4{,}1*10^{9}$ | $5{,}9*10^{10}$ |
| 90 | $1{,}8*10^{11}$ | $5{,}4*1^{11}$ | $4{,}1*10^{9}$ | $5{,}8*10^{10}$ |

因此, 虽然 TMS 在可信用服务器的选择百分比中未取得最好的结果, 但尽管如此, 其准确度的值仍高于 70%, 且 TMS 在所有实验过程中的能耗值最低. 这就是为什么我们可以说达成目标了.

### 4.3 共谋及振荡(同时)攻击实验

在进行共谋及振荡攻击时, PowerTrust 模型的表现都是最不尽如人意的. 如图 5 所示, 当恶意服务器的数量超过 40%时, 模型准确度就低于 70%, 可以说该模型有一些不足之处; 而其他模型可持续到恶意服务器达 60%.

当恶意服务器超过 70%, 准确度大约是 50%, 这一结果是可接受的. 总体而言, 我们的 TMS 模型在试验中表现良好, 且能耗水平比其他模型更低. 表 3 反映能耗水平.

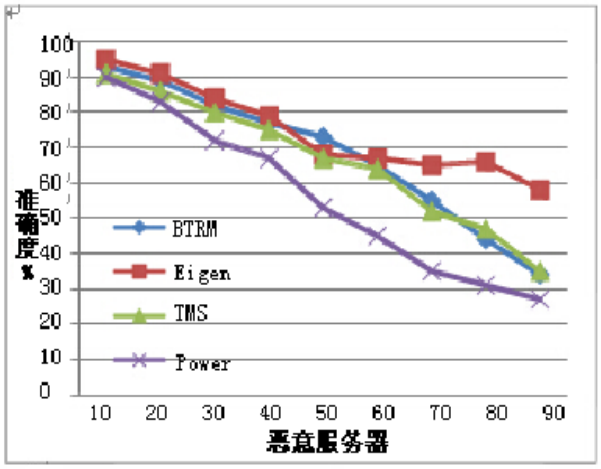


图 5　共谋及振荡攻击下动态 WSN 的准确度

表 3　共谋和振荡攻击下动态 WSN 的能耗

| 模型 / 恶意服务器(%) | BTRM | Eigen | TMS | Power |
|---|---|---|---|---|
| 10 | $1{,}9*10^{10}$ | $4{,}5*10^{12}$ | $4{,}0*10^{9}$ | $4{,}8*10^{9}$ |
| 20 | $2{,}6*10^{10}$ | $5{,}6*10^{12}$ | $4{,}5*10^{9}$ | $5{,}2*10^{9}$ |
| 30 | $2{,}8*10^{11}$ | $2{,}6*10^{13}$ | $4{,}6*10^{9}$ | $6{,}0*10^{9}$ |
| 40 | $3{,}2*10^{11}$ | $6{,}3*10^{13}$ | $4{,}7*10^{9}$ | $5{,}6*10^{9}$ |
| 50 | $4{,}7*10^{11}$ | $8{,}0*10^{13}$ | $9{,}6*10^{9}$ | $5{,}9*10^{9}$ |
| 60 | $1{,}9*10^{11}$ | $1{,}5*10^{14}$ | $1{,}6*10^{10}$ | $6{,}7*10^{10}$ |
| 70 | $2{,}6*10^{11}$ | $2{,}5*10^{14}$ | $4{,}9*10^{10}$ | $3{,}6*10^{10}$ |
| 80 | $2{,}9*10^{11}$ | $1{,}0*10^{14}$ | $5{,}8*10^{10}$ | $4{,}9*10^{11}$ |
| 90 | $3{,}7*10^{11}$ | $5{,}4*1^{14}$ | $5{,}9*10^{10}$ | $5{,}8*10^{11}$ |

## 5　结语

在考虑信息安全的前提下, 本文研发了一个基于聚簇无线传感器网络的信任管理系统(TMS), 并且为了系统的高效、节能运行, 也设计出相应的安全协议. 该协议的运作方式可通过一组兼顾移动传感器网络特征的算法进行表示. 通过内置的可用于确定置信水平及节点间信任关系的算法, 该协议可保护网络免受恶意的内部入侵者的攻击.

根据模拟实验结果, 可关注到以下几点:

① 解决了高效节能的设计任务. 通过模拟实验进行的对比, 我们的系统实现了最低能耗;

② TMS 在对可信节点报文转发的检测中表现出

了良好的稳定性, 平均准确度的最大值和最小值没有显著的偏差.

③ TMS 在攻击防御上的结果令人满意.

因此, 我们可以得出结论, 开发的系统满足了规定的要求并解决了所有指定的任务.

## 参考文献


1 Kumar GEP, Titus I, Thekkekara SI. A comprehensive overview on application of trust and reputation in wireless sensor network. Procedia Engineering, 2012, (38): 2903−2912.

2 Che RS, Feng RJ, Liang X, Wang X. A lightweight trust management based on Bayesian and Entropy for wireless sensor networks. Security Comm. Networks, 2015, (8): 168−175.

3 杨光,魏志强,丛艳平.水下无线通信网络分级信任管理.中国海洋大学学报:自然科学版,2013,43(6):109−114.

4 Galkin PV. Analisys of energy units wireless sensor networks. SR. 2014. 2: 55−61.

5 Abramov ES, Basan ES. Development of the protected clustered wireless sensor network model. Proc. of SFedU. Engineering of information security, 2013, 12(149): 48−56.

6 Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007: 57−64. [doi:10.1109/SCIS.2007.357670.]

7 Abramov ES, Basan ES, Laxmi V. Development of secure protocol for mobile cluster sensor network management. Izvestiya SFedU. Engineering Sciences, 2014, 2(151): 101−107.

8 Marmol FG, Perez GM. TRMSim- WSN, trust and reputation models simulator for wireless sensor networks. Proc. of the IEEE International Conference on Communications, Communication and Information Systems Security Symposium. Dresden, Germany. jun 2009.

9 孟敬,刘寿强.基于仿生学信任信誉模型 BTRM 的无线传感器网络的信任协作研究与实现.科技导报,2011,29(24).

10Kamvar S, Schlosser M, Garcia-Molina H. The eigen trust algorithm for reputation management in P2P networks, WWW03: Proc. of the 12th International Conference on World Wide Web. 2003. 640−651.

11 Zhou R, Hwang K. PowerTrust: A robust and scalable reputation system for trusted Peer-to-Peer computing. IEEE Trans. on Parallel and Distributed Systems, 2007, 18(4): 460−473.

12 Mármol FG, Pérez GM. Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication Systems Journal. 2010. [doi:10.1007/s11235-010-9281-7.]