

一种改进的应用于无线传感器网络的拜占庭容错方案

张 钰, 王 鑫, 蒋 华, 刘建明

(桂林电子科技大学 计算机科学与工程学院, 广西 桂林 541004)

摘 要: 研究了传统拜占庭容错方案并针对无线传感器网络的特定环境加以改进, 减少了传统方案中网络节点间消息交换轮数, 提高了效率并降低了通信开销和能量消耗, 仿真结果表明: 设计的方案在使所有正常网络节点达成一致的同时, 其使用的消息交换轮数与传统拜占庭方案相比有显著的下降。

关键词: 无线传感器网络; 错误容忍; 拜占庭容错方案

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2014)10-0052-04

An Improved Scheme for Byzantine Fault-Tolerance in WSNs

ZHANG Yu, WANG Xin, JIANG Hua, LIU Jian-ming

(School of Computer Science & Engineering, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: This paper designs an improved byzantine fault-tolerant scheme in allusion to the specific environment of wireless sensor networks. Compared to the traditional byzantine scheme, this scheme can reduce the number of rounds of messages exchange greatly between network nodes so that improving the efficiency and reducing communication overhead and energy consumption. Simulation results show that by using the improved fault-tolerant scheme, not only can all the normal network nodes reach an agreement, but also the number of rounds of messages exchange are much less than that of traditional byzantine scheme.

Key words: WSN; fault tolerance; byzantine fault-tolerant scheme

1 引言

目前, 对拜占庭容错方案应用性的研究主要是在分布式计算系统和无线 Mesh 网络领域^[1-6]. 传统拜占庭容错方案通过网络节点间持续地交换和收集消息从而排除错误网络节点, 但是忽视了以下两个特点: (1) 正常网络节点的数目至少为 $n - (n-1)/3$, 并且这些网络节点可以正确和诚实地发送消息. (2) 从正常网络节点收到的消息总数始终大于从错误网络节点收到的消息总数. 即来自正常网络节点的消息一直占大多数, 如果比较这些来自正常网络节点的消息, 就可以更快地找出共同值. 因此, 本文充分利用以上 2 点设计了一种改进的拜占庭容错方案, 可使所需要的消息交换轮数变少, 能耗和通信量得以降低, 提高了方案自身效率.

2 改进的拜占庭容错方案

出本文方案的假设条件:

- (1) 网络节点发出的消息都能够被正确的送达.
 - (2) 接收方知道该消息的发送方.
 - (3) 当网络节点总数为 n 时, 出现错误的网络节点数目最多为 $(n-1)/3$ 个.
 - (4) 在第一轮消息交换中, 只有一个网络节点可以发送消息.
 - (5) 网络中需要任意选出一个网络节点作为源网络节点, 并且第一轮信息交换中, 只有源网络节点可以将自己的初始值发送给包括自己在内的所有节点.
- 并且, 所有错误网络节点均行为表现异常, 即错误网络节点的发送给不同网络网络节点的值不相同

收稿日期: 2014-01-02; **修回日期:** 2014-02-27

基金项目: 国家自然科学基金重点项目(61262074)

或者错误网络节点的发送值与正常值有差异.

2.1 容错方案中使用的 M-树

在本文方案中,每个网络节点使用一种特定树来储存从其他网络节点收到的消息值.该树定名为 M-树(message tree),其结构如图 1 所示.在消息交换过程中,源网络节点首先将自己的初始值 $V(s)$ 发送给其他网络节点和自身,由于消息的发送方是可识别的,所以所有正常网络节点能识别出该消息的发送网络源节点并将该值保存在 M-树的根节点上.之后,每轮消息交换收到的消息值都会储存到 M-树中对应的节点上.从 M-树中的第二层开始,各个节点以储存值的发送方和父节点来命名,如第二层某节点的储存值来自网络节点 x ,则该节点命名为 $V(sx)$;第三层某节点的父节点为 $V(sx)$,其储存值来自网络节点 y ,则该节点命名为 $V(sxy)$;其他层的节点名以此类推.名称中有连续重复网络节点的节点名(如 $V(sxx)$, $V(syy)$, $V(sxxy)$ 等)不保存在 M-树中,用来避免错误网络节点会周期性的发送错误消息,使错误消息反复保存在 M-树中,导致误判.

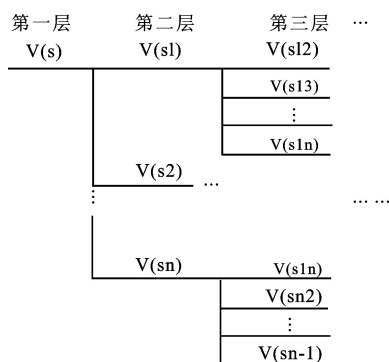


图 1 M-树结构

2.2 容错方案中的重要过程

当所有网络节点在在经过三轮消息交换后,就可以对 M-树中储存的消息值进行处理比较,这其中的重要过程有以下几个.

(1) 可信网络节点判定过程

三轮信息交换后,网络节点便进入可信网络节点的判定过程.首先判定 M-树次底层中每个节点(标为 $V(cx)$)的储存值是否等于其所有子节点值中占多数的值(记为 $\text{maj}(cx)$),如果符合,再判定各 $V(cx)$ 的子节点中与其对应的 $\text{maj}(cx)$ 值相同的节点总数(记为 $\text{cou_maj}(cx)$)是否不小于 $(n-(n-1)/3-1)$.如果以上两个条件均符合,则将 $V(cx)$ 储存值的发送方加入到自己即 x 的近似可信网络节点集(reliable-like network point set, RLNS, 记为 $\text{RLNS}(cx)$)中.同时也将

与 $\text{maj}(cx)$ 相同的子节点的发送方添加到 $\text{RLNS}(x)$ 中.总体而言,判定某一网络节点 y 可否添加到 $\text{RNPS}(cx)$ 中需要满足以下 3 个条件:

- ① $V(cx) = \text{maj}(cx)$
- ② $\text{cou_maj}(cx) \geq (n-(n-1)/3-1)$
- ③ $V(cxy) = \text{maj}(cx)$

之后,统计各个网络节点在次底层所有 RNPS 集中的累计总数(记为 $\text{cou_RLN}(z)$),如果某网络节点的 $\text{cou_RLN}(z)$ 不小于 $(n-(n-1)/3-1)$,则该网络节点为可信网络节点.图 2 中显示在一个有 4 个网络节点的 WSN 中某网络节点确定可信网络节点的具体过程.

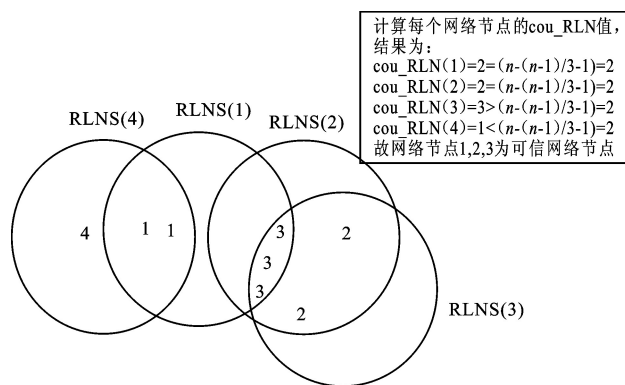


图 2 确定可信网络节点

(2) 修正错误消息过程

在添加新可信网络节点之后,每个网络节点会修正 M-树中来自不可信网络节点的消息,用以加快共同值的推举速度.这里会检查 M-树次底层所有节点的子节点,如果子节点储存值与所在子树中发送方为可信网络节点的节点储存值集中占多数的值(记为 $\text{maj}(\text{RNN}(cx))$)不同并且该子节点储存值的发送方不是可信网络节点的话,该子节点的值会被替换为 $\text{maj}(\text{RNN}(cx))$.

(3) 共同值选举过程

错误消息替换完毕后, M-树从次底层的每个子树中选出多数派值,之后向上一层逐层选出多数派值,直到根节点为止,得出该网络节点的共同值.其具体过程演示如图 3 所示.

2.3 容错方案的整体运行流程

根据以上的设计,本方案消息交换需要的最小轮数为 5,从第 4 轮开始,如果连续两轮各网络节点都未发现新的可信网络节点的话,即所有正常网络节点已全部达成一致后,方案运行结束.容错方案的算法过程如下:

(1) 首先进行必要消息交换阶段,第一轮消息交换,源网络节点将自己的初始值 $V(s)$ 发送给自身和

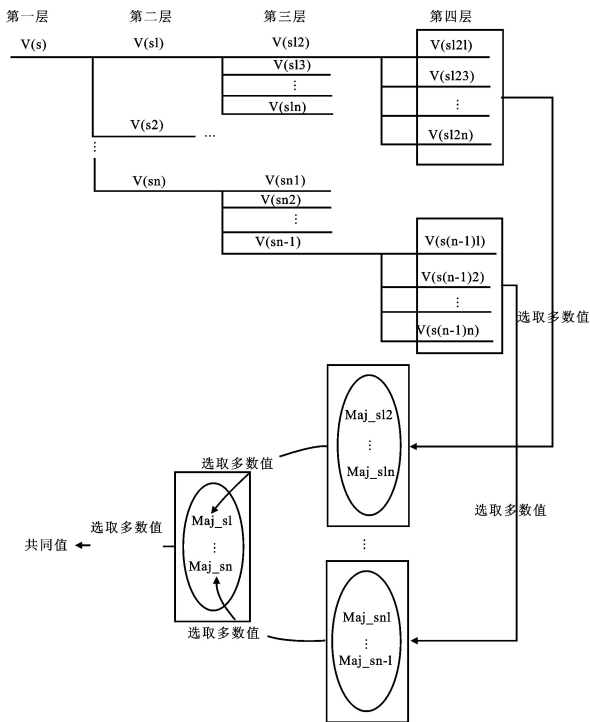


图3 共同值选举过程

其他网络节点,每个节点将该值储存在 M-树的根节点上,之后进入步骤 2。

(2)第二轮消息交换,每个网络节点将 M-树中根节点值发送给自身和其他所有网络节点,每个节点将接收的值储存在 M-树的第二层中对应节点上,之后进入步骤 3。

(3)第三轮消息交换,每个网络节点将 M-树中第二层储存的值发送给自身和其他所有网络节点,每个节点将接收的值储存在 M-树中的第三层中对应节点上,之后进入步骤 4。

(4)从第三轮消息交换后开始,各个网络节点进入决策判定阶段,首先进行可信网络节点判定过程,节点判定过程结束后,检查累计变量空消息交换(cou_nullmess,初始值为 0)是否小于 2,如果不小于 2,方案运行结束.如果小于 2,继续判断是否添加了新的可信网络节点,如果判定为真,cou_nullmess 归 0,进入步骤 5;如果判定为假,cou_nullmess 累计加 1,并开始下一轮消息交换,其过程与步骤 3 类似。

(5)判定并添加了新的可信网络节点后,每个网络节点开始修正错误消息过程,替换 M-树中不可信网络节点发送的消息,之后进入步骤 6。

(6)每个网络节点进行共同值选举过程,得出当前已找到的正常网络节点的共同值,并开始下一轮消息交换。

应用于 WSNs 的拜占庭容错方案

定义

$V(cx)$: M-树中的节点

$maj(cx)$: M-树节点 $V(cx)$ 的子节点值中占多数的值

$cou_maj(cx)$: M-树节点 $V(cx)$ 子树中与 $maj(cx)$ 相等的节点的总数

$RLNS(x)$: M-树中节点 $V(cx)$ 储存值发送方的近似可信网络节点集

$cou_RLN(z)$: 网络节点 z 在 M-树所有近似可信网络节点集中出现的总数

RNN : 某网络节点 M-树中的可信网络节点

$maj(RNN(cx))$: M-树节点 $V(cx)$ 子树中发送方为可信网络节点的子节点值中占多数的值

cou_nm : 没有发现新可信节点的消息交换轮数的总数,初始值为 0

必要消息交换阶段

第 1 轮

源网络节点将自己的初始值 $V(s)$ 发送给自身和其他网络节点,每个节点将该值储存在 M-树的根节点上。

第 2 轮

每个网络节点将 M-树中根节点值发送给自身和其他所有网络节点,每个节点将接收的值储存在 M-树中的第二层中。

第 3 轮

每个网络节点将 M-树中第二层储存的值发送给自身和其他所有网络节点,每个节点将接收的值储存在 M-树中的第三层中。

决策判定阶段

//可信网络节点判定过程

foreach M-树某层所有节点

```
{
  If ( $V(cx) = maj(cx)$  and  $cou\_maj(cx) \geq (n - (n - 1)/3 - 1)$ ) then
```

```
{
  将网络节点  $x$  添加至  $RLNS(x)$  中;
  while( $V(cx)$  的子节点是否搜索完毕)
```

```
{
  If ( $V(cxy) = maj(cx)$ ) then
```

```
{
  将网络节点  $y$  添加至  $RLNS(x)$  中;
}
```

```
}
}
foreach 每个网络节点  $z$ 
```

```
{
  统计 M-树中所有  $RLNS$  中的  $cou\_RLN(z)$ ;
  If ( $cou\_RLN(z) \geq (n - (n - 1)/3 - 1)$ ) then
```

```
{
  网络节点  $z$  认定为可信网络节点;
}
```

```
}
//判定方案是否停止
```

```
If( $cou\_nm < 2$ ) then
```

```
{If ( $RNN$  中加入新可信网络节点) then
```

```
{
   $cou\_nm = 0$ ;
```

```
//修正错误消息过程
```

```
foreach M-树该层所有节点
```

```
{
  while( $V(cx)$  的子节点是否搜索完毕)
```

```
{
  If ( $V(cxy)$  储存值的发送者不在  $RNN$  中 and  $V(cxy) \neq maj(RNN(cx))$ ) then
```

```
{
   $V(cxy) = maj(RNN(cx))$ ;
```

```
}
```

```

}
//共同值选举过程
从 M-树的次底层节点子树开始,逐层选出多数派值,从而得出共同值;
}
else
{
cou_nm = cou_nm + 1;
}
//开始新一轮消息交换
每个网络节点将 M-树中当前最底层储存的值发送给自身和其他所有网络节点;
每个网络节点将接收的值储存在 M-树中的新的层中;
//开始重新决策判断
goto 决策判定阶段;
}

```

3 仿真分析

为了研究本文设计的容错方案与传统拜占庭容错方案在消息交换轮数方面的性能表现,仿真实验网络模型主要参数如表 2 所示. 仿真场景的自变量有 2 个:错误网络结点数 $\{5, 10, 15, 20, 25\}$ 和错误网络节点是否为源网络节点,变换场景时只能改动一个自变量,所以总共为 10 个场景,每个场景均模拟 10 次,每次模拟直到容错方案结束运行为止,最终数据为 10 次模拟数据的平均值.

表 2 仿真网络模型参数

场景参数	设置值
部署环境/ m^2	300×300 节点通信半径/m
节点数量	80
网络传输率/ $(\mu s/bit)$	4
数据分组长度/byte	32

图 4 所示为源网络节点非错误网络节点情况下本文方案和传统拜占庭方案在消息交换轮数上的结果比较,显见与传统拜占庭方案相比本文方案有着明显的优势,在错误网络节点数较少时,本文方案的消息交换轮数一直保持在最低设计轮数,直到错误网络节点数接近网络设计的最大值时,才略有上升. 这是因为整个网络中正常网络节点始终为大多数,即这个正确值在各个网络节点的 M-树中也一直是多数派,使得最终共同值也会与该值相等,无需通过传统拜占庭方案中至少 $(n-1)/3 + 1$ 次消息交换排除错误节点来确定最终共同值,从而减少了消息交换轮数.

图 5 中显示源网络节点为错误网络节点的情况下本文方案和传统拜占庭方案在消息交换轮数上的结果比较,与图 2 相比可以看出,本文方案在错误网络节点数相同的情况下,源网络节点为错误网络节点时所需的消息交换轮数普遍大于源网络节点非错误网络节点时的消息交换轮数. 这是由于当源网络节点为错误网络节点时,其发送给所有网络节点的初始值

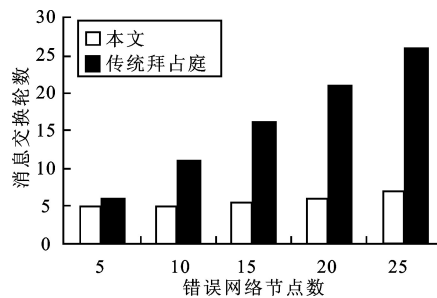


图 4 本文方案与传统拜占庭方案的消息交换轮数比较
(源网络节点非错误网络节点)

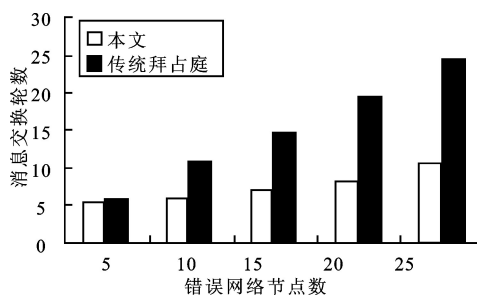


图 5 本文方案与传统拜占庭方案的消息交换轮数比较
(源网络节点为错误网络节点)

是不同的,加大了正常网络节点确定共同值的难度,所需的消息交换轮数也相应增加. 但本文方案与传统拜占庭方案相比所需的消息交换轮数依旧较少.

4 结束语

本文对传统拜占庭容错方案进行研究并加以改进,设计出一种应用于无线传感器网络的容错方案^[7],仿真实验,也证实了无论源网络节点是否为错误网络节点,本文提出的方案与传统拜占庭容错方案相比在消息交换轮数上均有大幅下降. 在今后的研究工作中,将着重解决本文设计方案中的实时性问题,即优化方案的代码和过程,缩短所有网络节点达成一致的时间.

参考文献:

- [1] Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: a survey[J]. Communications Surveys & Tutorials, IEEE, 2008, 10(3): 6-28.
- [2] Correia M, Bessani A N, Verissimo P. On byzantine generals with alternative plans[J]. Journal of Parallel and Distributed Computing, 2008, 68(9): 1291-1296.
- [3] Kapron B M, Kempe D, King V, et al. Fast asynchronous byzantine agreement and leader election with full information[J]. ACM Transactions on Algorithms (TALG), 2010, 6(4): 68.

(下转第 59 页)

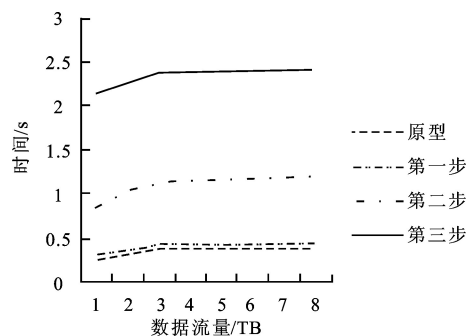


图4 每步处理后的检索时间图

超过3的单词,我们不做考虑,因为这些单词的存在将大大影响检索效率.总之,结果表明密文检索方法的效率和可行性还是令人满意的.

5 结束语

本文提出了新密文数据检索方法,能够确保云存储系统中的数据安全^[9].具体介绍了元数据处理用户输入单词的过程,能够使数据检索变得更加友好.将来的工作将主要分析元素的限制性能和密文数据检索的效率.

参考文献:

- [1] Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]//The IEEE Symposium on Security and Privacy(S&P2000). Piscataway IEEE, 2000:44-45.
- [2] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search [C] // EURO-CRYPT. Heidelberg, Springer, 2004(3027):506-522.
- [3] Park D, Kim K, Lee P. Public key encryption with

conjunctive field keyword search [C] // WISA 2004. Heidelberg, Springer, 2005(3325):73-86.

- [4] Dai Y, Shang J, Su Z. Quick index on encrypted database [J]. Journal of Tsinghua University (Sci. & Tech.) 1997(37):24-27.
- [5] Rivest R J, Adleman L, Dertouzos M I. On data banks and privacy homeomorphisms[R]. Foundations of Secure Computation, 1978.
- [6] Swaminathan A, Mao Y, Su G M, et al. Confidentiality preserving rank ordered search [C] // The 2007 ACM Workshop on Storage Security and Survivability (StorageSS2007). New York, ACM, 2007:7-12.
- [7] Gentry C. Fully homomorphic encryption using Ideal lattices[C]//The 41st Annual ACM Symposium on Theory of Computing (STOC 2009). New York, ACM, 2009:169-178.
- [8] Norvig P. How to write a spelling corrector[EB/OL]. [2014-05-22]. <http://norvig.com/spell-correct.html>.
- [9] 彭霖,李瑞轩.一种密文全文检索系统的安全索引结构[J].微电子与计算机,2012,29(1):1-7.

作者简介:

刘伯红 男,(1973-),副教授,硕士生导师.研究方向分布式系统、云计算.

王刚 男,(1989-),硕士研究生.研究方向云计算、密文检索.

王娟娟 女,(1988-),硕士研究生.研究方向云计算、密文检索.

史慧丽 女,(1988-),硕士研究生.研究方向云计算、密文检索.

(上接第55页)

- [4] Wang S S, Yan K Q, Wang S C. Achieving efficient agreement within a dual-failure cloud-computing environment[J]. Expert Systems with Applications, 2011, 38(1): 906-915.
- [5] Chiang M L. Eventually byzantine agreement on CDS-based mobile ad hoc network[J]. Ad Hoc Networks, 2012, 10(3): 388-400.
- [6] 王吉喆,赵蕴龙,吴静. WMN中拜占庭容错网络结构及算法[J]. 计算机工程, 2011(20): 28.
- [7] Klempous R, Nikodem J, Radosz L, et al. Byzantine algorithms in wireless sensors network[C]//Information and Automation, 2006. ICIA. International Con-

ference on. China: Weihai, IEEE, 2006: 319-324.

作者简介:

张钰 男,(1987-),硕士研究生.研究方向为网络信息安全.

王鑫 男,(1976-),副教授,硕士生导师.研究方向为物联网与信息安全.

蒋华 男,(1963-),教授,硕士生导师.研究方向为信息安全.

刘建明 男,(1975-),教授,硕士生导师.研究方向为无线传感器网络.