(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113225741 A
(43)申请公布日 2021.08.06

(21)申请号 202110537346.5

(22)申请日 2021.05.17

(71)申请人 国网山东省电力公司济南供电公司
地址 250012 山东省济南市市中区泺源大街238号
申请人 国家电网有限公司

(72)发明人 张德才 何峰 胡旭冉 朱凯枫 周兴福 蒋超 窦昊宁 张灿华 廖德胜

(74)专利代理机构 济南诚智商标专利事务所有限公司 37105
代理人 黄晓燕

(51)Int.Cl.
H04W 12/121(2021.01)
H04W 84/18(2009.01)

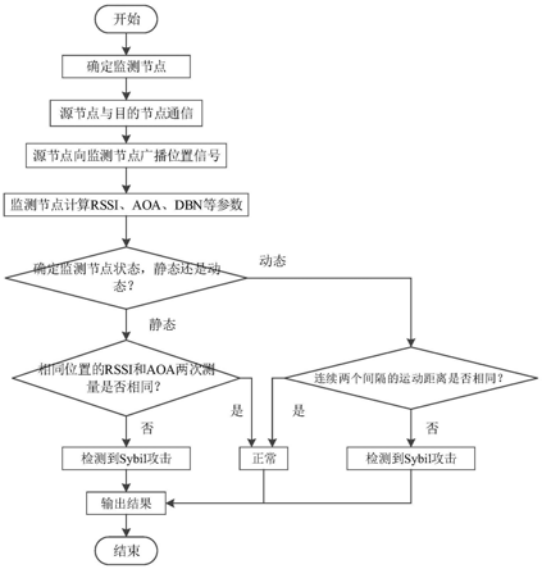
权利要求书2页 说明书5页 附图3页

(54)发明名称

移动自组织网络的分布式混合Sybil攻击检测方法及系统

(57)摘要

本发明提供了移动自组织网络的分布式混合Sybil攻击检测方法及系统，所述方法包括确定监测节点；建立源节点与目的节点的通信，且源节点向监测节点广播位置信号；监测节点进行参数计算，并基于所述参数确定当前节点状态；若为静态，则基于相同位置处的参数差值确定是否存在Sybil攻击；若为动态，则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。



CN 113225741 A

1.移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述方法包括以下步骤:

确定监测节点;

建立源节点与目的节点的通信,且源节点向监测节点广播位置信号;

监测节点进行参数计算,并基于所述参数确定当前节点状态;

若为静态,则基于相同位置处的参数差值确定是否存在Sybil攻击;若为动态,则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

2.根据权利要求1所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述监测节点通过节点的邻居密度确定。

3.根据权利要求1所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述监测节点计算的参数包括无线信号接收强度RSSI、到达角AOA和各节点之间的位置距离DBN。

4.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述无线信号接收强度RSSI的计算具体为:

$$RSSI = 10\log\frac{P_{rx}}{P_{ref}}(dBm)$$

式中,P_{rx}为接收功率,P_{ref}为参考功率。

5.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述到达角AOA的计算具体为:

$$\theta = \arccos\frac{\Delta\partial\times\rho}{-2\pi d}$$

式中,θ为到达角,$\Delta\partial$为相邻天线之间的相位偏移,d为两个天线之间的距离,ρ为信号的波长。

6.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述各节点之间的位置距离DBN计算具体为:

$$\left|DBN_{ij}\right| = \sqrt{\frac{P_{tx}\times\alpha\times\beta\times\mu}{(4\pi)P_{rx}\times\phi}}$$

式中,α为发射器增益,β为接收器增益,Φ为系统损耗,μ为波长,P_{rx}为接收功率,P_{tx}为发射功率。

7.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述基于所述参数确定当前节点状态的具体过程为:

将当前时刻的参数值与上一时刻参数值进行比较,得到差值F;

若所述差值F大于窗口值W,则节点状态为动态,否则为静态。

8.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述基于相同位置处的参数差值确定是否存在Sybil攻击的具体过程为:

两个位置相同的节点,其RSSI值和/或AOA值不同,则存在Sybil攻击。

9.根据权利要求3所述移动自组织网络的分布式混合Sybil攻击检测方法,其特征是,所述基于相邻时间间隔下的参数差值确定是否存在Sybil攻击的具体过程为:

对同一节点,连续两个时间间隔下,其移动距离不同,则存在Sybil攻击。

10.移动自组织网络的分布式混合Sybil攻击检测系统,其特征是,所述系统包括:

节点分析单元,用于确定监测节点;

通信单元,用于建立源节点与目的节点的通信,且源节点向监测节点广播位置信号;

参数计算单元,用于调用监测节点进行参数计算,并基于所述参数确定当前节点状态;

攻击分析单元,用于根据节点状态,分析Sybil攻击:若为静态,则基于相同位置处的参数差值确定是否存在Sybil攻击;若为动态,则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

移动自组织网络的分布式混合Sybil攻击检测方法及系统

技术领域

[0001] 本发明涉及移动自组织网络安全技术领域,尤其是移动自组织网络的分布式混合Sybil攻击检测方法及系统。

背景技术

[0002] 随着我国社会经济的迅速发展,移动自组织(Ad-hoc)网络(MANETs)由于其活跃和适应性强逐渐成为社会各界探讨的热点。然而移动自组织网络是一个分布式网络,没有合适的技术来认证节点的特性,因此有大量恶意节点在网络中中断,同时隐瞒其个性特征,并预备支持相邻的节点,从而逃避重要的证据,并在节点间的分布上为网络造成破坏性和危险。

[0003] Sybil攻击,是会对MANETs网络造成破坏性和危险的恶意攻击之一。Sybil节点将自身的数据直接伪造到网络中的剩余节点,为剩余节点获取数据,不将数据转发到终端,使正常节点误判。因此,Sybil路由协议会对网络的可靠通信造成实际的破坏,从而对无线自组织网络的正常运行产生很大的影响。发现并清除网络中的Sybil攻击是非常关键的。

发明内容

[0004] 本发明提供了移动自组织网络的分布式混合Sybil攻击检测方法及系统,用于检测Sybil攻击。

[0005] 为实现上述目的,本发明采用下述技术方案:

[0006] 本发明第一方面提供了移动自组织网络的分布式混合Sybil攻击检测方法,所述方法包括以下步骤:

[0007] 确定监测节点;

[0008] 建立源节点与目的节点的通信,且源节点向监测节点广播位置信号;

[0009] 监测节点进行参数计算,并基于所述参数确定当前节点状态;

[0010] 若为静态,则基于相同位置处的参数差值确定是否存在Sybil攻击;若为动态,则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

[0011] 进一步地,所述监测节点通过节点的邻居密度确定。

[0012] 进一步地,所述监测节点计算的参数包括无线信号接收强度RSSI、到达角AOA和各节点之间的位置距离DBN。

[0013] 进一步地,所述无线信号接收强度RSSI的计算具体为:

[0014] $$RSSI = 10\log\frac{P_{rx}}{P_{ref}}(dBm)$$

[0015] 式中,P_{rx}为接收功率,P_{ref}为参考功率。

[0016] 进一步地,所述到达角AOA的计算具体为:

[0017] $$\theta = \arccos\frac{\Delta\partial\times\rho}{-2\pi d}$$

[0018] 式中，θ为到达角，$\Delta\partial$为相邻天线之间的相位偏移，d为两个天线之间的距离，ρ为信号的波长。

[0019] 进一步地，所述各节点之间的位置距离DBN计算具体为：

[0020] $$\left|DBN_{ij}\right|=\sqrt{\frac{P_{tx}\times\alpha\times\beta\times\mu}{(4\pi)P_{rx}\times\phi}}$$

[0021] 式中，α为发射器增益，β为接收器增益，Φ为系统损耗，μ为波长，P_{rx}为接收功率，P_{tx}为发射功率。

[0022] 进一步地，所述基于所述参数确定当前节点状态的具体过程为：

[0023] 将当前时刻的参数值与上一时刻参数值进行比较，得到差值F；

[0024] 若所述差值F大于窗口值W，则节点状态为动态，否则为静态。

[0025] 进一步地，所述基于相同位置处的参数差值确定是否存在Sybil攻击的具体过程为：

[0026] 两个位置相同的节点，其RSSI值和/或AOA值不同，则存在Sybil攻击。

[0027] 进一步地，所述基于相邻时间间隔下的参数差值确定是否存在Sybil攻击的具体过程为：

[0028] 对同一节点，连续两个时间间隔下，其移动距离不同，则存在Sybil攻击。

[0029] 本发明第二方面提供了移动自组织网络的分布式混合Sybil攻击检测系统，所述系统包括：

[0030] 节点分析单元，用于确定监测节点；

[0031] 通信单元，用于建立源节点与目的节点的通信，且源节点向监测节点广播位置信号；

[0032] 参数计算单元，用于调用监测节点进行参数计算，并基于所述参数确定当前节点状态；

[0033] 攻击分析单元，用于根据节点状态，分析Sybil攻击：若为静态，则基于相同位置处的参数差值确定是否存在Sybil攻击；若为动态，则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

[0034] 发明内容中提供的效果仅仅是实施例的效果，而不是发明所有的全部效果，上述技术方案中的一个技术方案具有如下优点或有益效果：

[0035] 本发明公开的Sybil攻击检测方法，通过区分节点的状态进行进一步分析Sybil攻击；如果节点是静态的，则通过比较两个相同位置的RSSI强度和AOA测量值来检测sybil攻击。如果节点在移动，且连续两个间隔的移动距离不同，则认为是Sybil攻击。相比精确Sybil攻击检测(ASAD)方法，本发明的方法能够最大限度使计算开销和检测延迟最小化。

附图说明

[0036] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0037] 图1是本发明所述方法实施例的流程示意图；

[0038] 图2是评价指标中检测延迟的曲线图；

[0039] 图3是评价指标中受影响数据包的曲线图；

[0040] 图4是评价指标中计算开销的曲线图；

[0041] 图5是评价指标中检测精度的曲线图。

具体实施方式

[0042] 为能清楚说明本方案的技术特点，下面通过具体实施方式，并结合其附图，对本发明进行详细阐述。下文的公开提供了许多不同的实施例或例子用来实现本发明的不同结构。为了简化本发明的公开，下文中对特定例子的部件和设置进行描述。此外，本发明可以在不同例子中重复参考数字和/或字母。这种重复是为了简化和清楚的目的，其本身不指示所讨论各种实施例和/或设置之间的关系。应当注意，在附图中所图示的部件不一定按比例绘制。本发明省略了对公知组件和处理技术及工艺的描述以避免不必要地限制本发明。

[0043] 如图1所示，本发明移动自组织网络的分布式混合Sybil攻击检测方法，所述方法包括以下步骤：

[0044] S1，确定监测节点；

[0045] S2，建立源节点与目的节点的通信，且源节点向监测节点广播位置信号；

[0046] S3，监测节点进行参数计算，并基于所述参数确定当前节点状态；

[0047] S4，若为静态，则基于相同位置处的参数差值确定是否存在Sybil攻击；若为动态，则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

[0048] 移动自组织网络MANETs是一种无基础设施的移动自组织网络，具有动态拓扑、无线通信的特点。由于在移动Ad-Hoc网络中每个节点既是主机又是路由器，所以容易遭受针对路由信息的攻击。

[0049] 步骤S1中，所述监测节点通过节点的邻居密度确定，具体为：根据节点的邻居密度(ND)将一定的节点集合指定为监测节点(MN)。其中，节点邻居密度(ND)与显示相邻节点数的节点度(N_Deg)密切相关。它被用来寻找连接到节点的邻居节点的平均距离。

[0050] 节点邻居密度的表达式为 $$ND=\frac{N\_Deg}{\pi\times\zeta} \quad (1)$$

[0051] (1)式中，ζ为通信范围。

[0052] 步骤S2中，源节点(S)与目的节点(D)通信时，源节点(S)会向所有的监测节点广播一个位置信号(LOC_CL)。

[0053] 步骤S3中，监测节点计算的参数包括无线信号接收强度RSSI、到达角AOA和各节点之间的位置距离DBN。

[0054] RSSI是接收信号的强度指示，主要应用于发射机和接收机之间的距离测量。通常情况下，链路质量与RSSI成正比，即：

[0055] $LQ\propto RSSI$ (2)

[0056] 无线信号接收强度RSSI的计算具体为：

[0057] $$RSSI=10\log\frac{P_{rx}}{P_{ref}}(dBm) \quad (3)$$

[0058] (3)式中，P_{rx}为接收功率，P_{ref}为参考功率。

[0059] 在MANETs中，节点随机分布在监测区域内，其中部分节点能够通过携带自身定位设备或人工部署的方式获得自身的精确位置，此类节点被称为锚节点(anchor node)；其他未知节点(unknown node)只能根据锚节点位置按照某种定位机制估算出自身位置。AOA用θ表示，通过某些硬件设备感知发射节点信号的到达方向，计算接收节点和锚节点之间的相对方位或角度。相邻天线之间的相位偏移△∂由下式给出：

[0060] $$\Delta\partial = -2\pi \frac{d\cos(\theta)}{\rho} \qquad (4)$$

[0061] (4)式中，d是两个天线之间的距离。信号的波长ρ可以由信号的频率推导出来。

[0062] 因此，到达角(AOA)可以计算为：

[0063] $$\theta = \arccos \frac{\Delta\partial \times \rho}{-2\pi d} \qquad (5)$$

[0064] 两个节点之间的距离使用以下的自由空间传播模型计算。

[0065] $$\left|DBN_{ij}\right| = \sqrt{\frac{P_{tx} \times \alpha \times \beta \times \mu}{(4\pi) P_{rx} \times \phi}} \qquad (6)$$

[0066] (6)式中，α为发射器增益，β为接收器增益，Φ为系统损耗，μ为波长，Prx为接收功率，Ptx为发射功率。

[0067] 基于所述参数确定当前节点状态的具体过程为：将当前时刻的参数值与上一时刻参数值进行比较，得到差值F；若所述差值F大于窗口值W，则节点状态为动态，否则为静态。

[0068] 步骤S4中，基于相同位置处的参数差值确定是否存在Sybil攻击的具体过程为：两个位置相同的节点，其RSSI值和/或AOA值不同，则存在Sybil攻击。

[0069] 基于相邻时间间隔下的参数差值确定是否存在Sybil攻击的具体过程为：对同一节点，连续两个时间间隔下，其移动距离不同，则存在Sybil攻击。

[0070] 本发明还提供了移动自组织网络的分布式混合Sybil攻击检测系统，所述系统包括节点分析单元、通信单元、参数计算单元和供给分析单元。

[0071] 节点分析单元用于确定监测节点；通信单元用于建立源节点与目的节点的通信，且源节点向监测节点广播位置信号；参数计算单元用于调用监测节点进行参数计算，并基于所述参数确定当前节点状态；攻击分析单元用于根据节点状态，分析Sybil攻击：若为静态，则基于相同位置处的参数差值确定是否存在Sybil攻击；若为动态，则基于相邻时间间隔下的参数差值确定是否存在Sybil攻击。

[0072] 下面与现有精确Sybil攻击检测ASAD方法进行比较，对本发明达到的有益效果进行突出说明。

[0073] 首先，设置如下表所示实施参数。

[0074]

网络规模	100 nodes
面积大小	1000 ×1000 m
MAC 协议	IEEE 802.11
交通模型	恒定比特率
攻击者数量	2 -10
传播	TwoRayGround
天线	OmniAntenna
指定能量	15 Joules
发送功率	0.8 W
接收功率	0.5 W

[0075] 确定模拟的威胁模型考虑了MANET的外部和内部攻击者,考虑的攻击有DoS攻击和丢包攻击。性能评价指标包括检测延迟、受影响数据包、检测精度和计算开销的比例。

[0076] 如图2所示,随着节点的增加,DHSAD的时延从8.3s增加到31.7ms,ASAD技术的检测时延从14.9ms增加到38.3ms。由于通过监测节点的协同检测来快速检测攻击,DHSAD的检测时延比ASAD小32%。

[0077] 如图3所示,随着节点数目的增加,DHSAD的断裂由1.11增加到4.8,ASAD的比例由1.4增加到6.4。由于DHSAD检测到未经授权的攻击和Sybil攻击,受影响数据包的比例比ASAD小23%。

[0078] 如图4所示,随着节点的增加,DHSAD的开销从373增加到897Kb,ASAD的开销从782增加到1190Kb。由于DHSAD不使用任何跟踪数据,它的开销比ASAD小36%。

[0079] 如图5所示,随着节点的增加,DHSAD的精度由98.7%下降到92.1%,ASAD技术的精度由91.4%下降到89.1%。由于DHSAD中执行了基于距离的攻击预测和基于MAC的认证,因此与ASAD相比,其检测精度提高了8%。

[0080] 实施结果表明,所提出的方法使移动自组织网络攻击检测的计算开销和检测延迟最小化。

[0081] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,所属领域技术人员应该明白,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

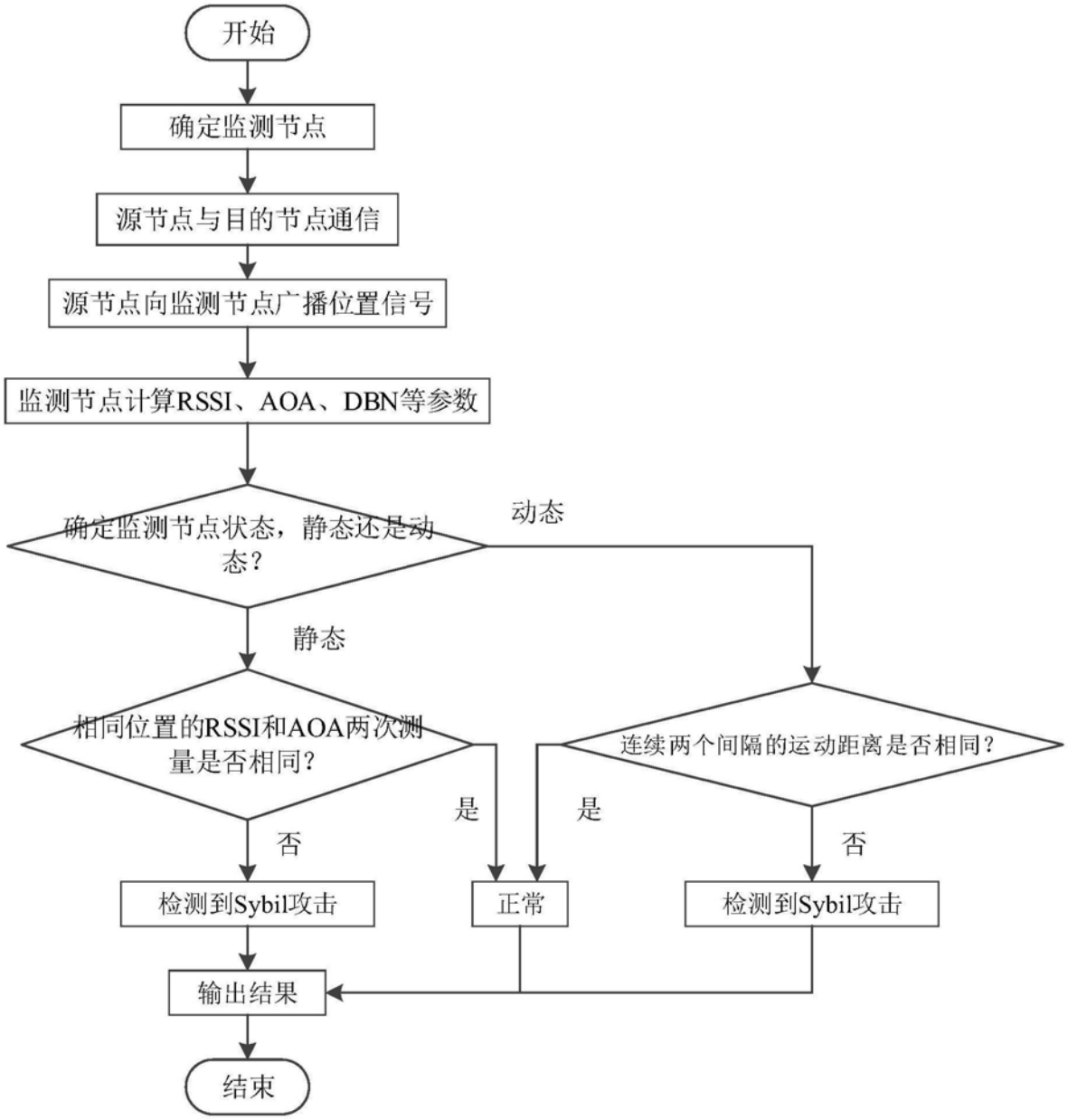

开始
确定监测节点
源节点与目的节点通信
源节点向监测节点广播位置信号
监测节点计算RSSI、AOA、DBN等参数
确定监测节点状态，静态还是动态？
动态
静态
相同位置的RSSI和AOA两次测量是否相同？
连续两个间隔的运动距离是否相同？
是
是
否
否
检测到Sybil攻击
正常
检测到Sybil攻击
输出结果
结束

图1

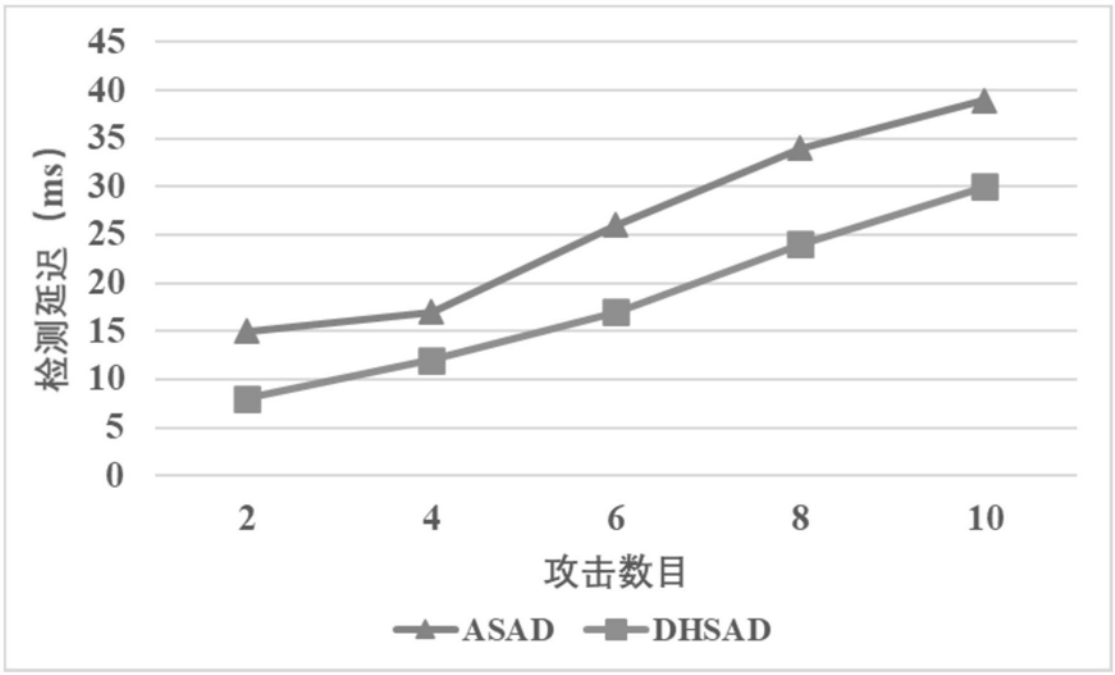

检测延迟（ms）
45
40
35
30
25
20
15
10
5
0
2
4
6
8
10
攻击数目
ASAD
DHSAD

图2

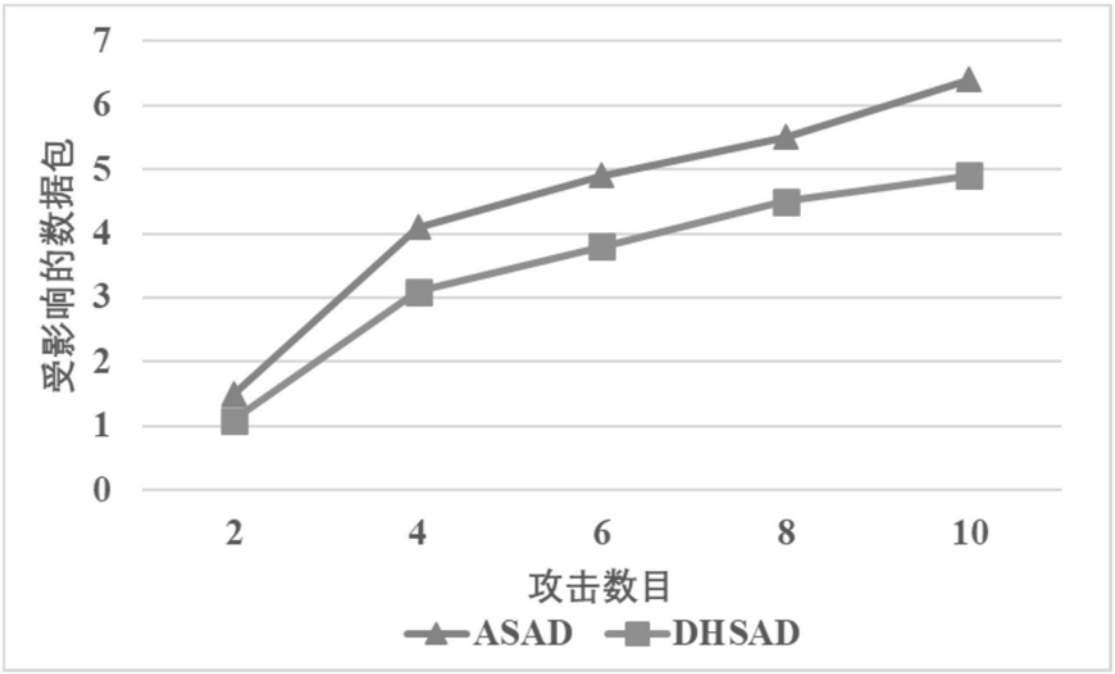

受影响的数据包
7
6
5
4
3
2
1
0
2
4
6
8
10
攻击数目
ASAD
DHSAD

图3

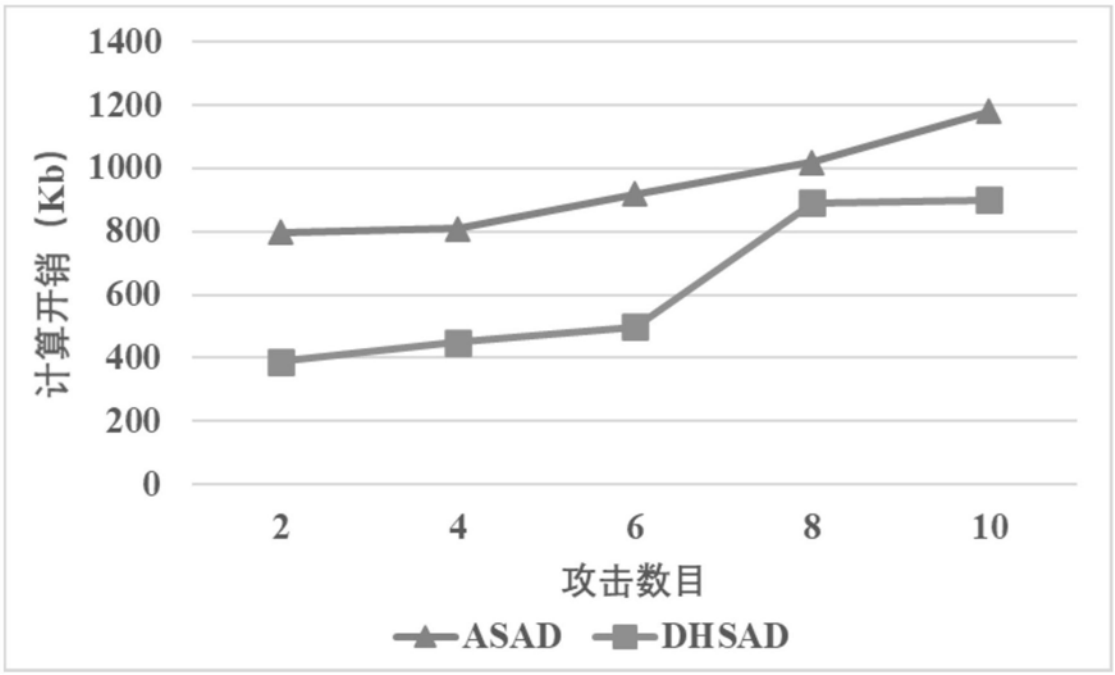

1400
1200
1000
800
600
400
200
0
计算开销（Kb）
2
4
6
8
10
攻击数目
ASAD
DHSAD

图4

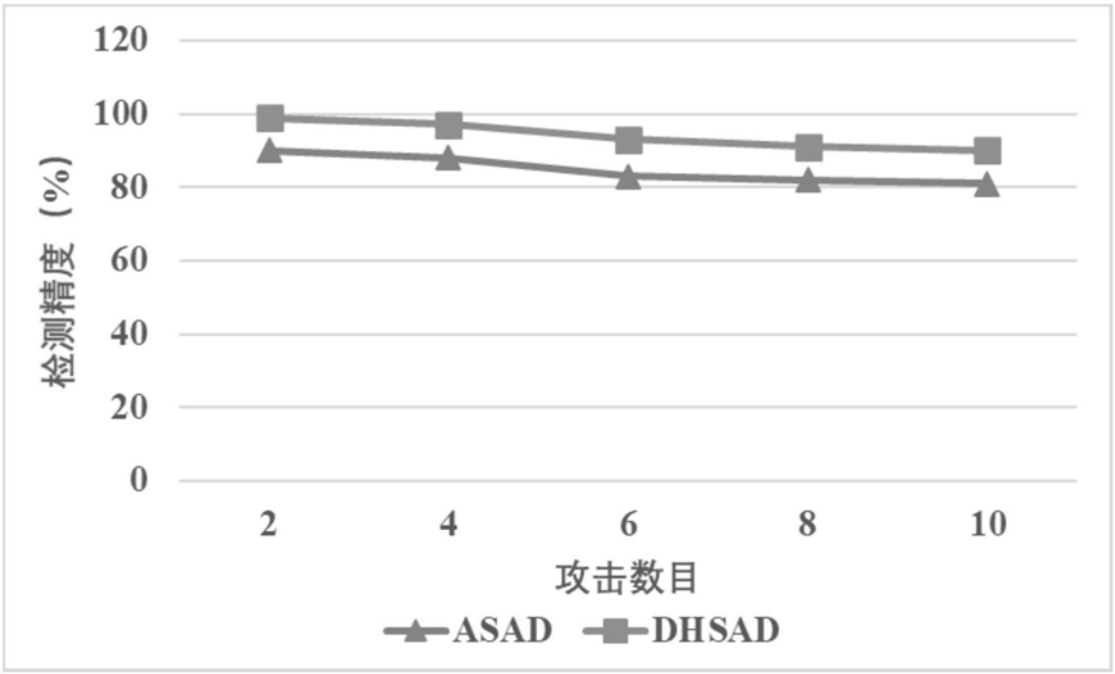

120
100
80
60
40
20
0
检测精度（%）
2
4
6
8
10
攻击数目
ASAD
DHSAD

图5