基于概率博弈的空天地一体化网络安全路由算法

李嘉淳[1]，张唯炯[2]，邱令存[2]，张乐[1]

（1. 上海交通大学 计算机科学与工程系，电子信息与电气工程学院，上海 上海 200240； 2. 上海航天电子技术研究所，上海 201109）

摘　要：针对空天地一体化网络存在的安全问题，本文提出了使用路由证据的方法来对洪泛攻击，灰洞/黑洞攻击进行防御的方案。该方案可以检测出自组织网络中存在的恶意节点，保证路由的安全可靠性。本文克服了已有方案存在的不足，可以自适应的在空天地一体化网络等容断容迟网络中应用。最后，搭建了仿真平台，通过仿真验证的手段，证明了该方案可以检测出90%以上的恶意节点，证明了有效性。

关键词：空天地一体化网络；路由证据；洪泛攻击；灰洞攻击；黑洞攻击

中图分类号　文献标志码：　DOI：

Secure Routing Algorithm Based on Probabilistic the under Space-Air-Ground-Integrated-network

LI Jiachun[1], ZHANG Weijiong[2]，QIU Lingcun[1], ZHANG Le[2]

（1. Department of Computer Science and Engineering, School of Electronics Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, Shanghai, China; 2. Shanghai Aerospace Electronic Technology Institute, Shanghai 201109, China）

Abstract: Aiming at the security problems in the space-air-ground integrated network, this paper proposes a scheme, which utilizes routing evidence to defend against flooding attacks and grey hole/black hole attacks. The scheme can detect malicious nodes in the ad-hoc network to ensure the security and reliability of routing. This paper overcomes the shortcomings of the existing schemes and can be adaptively applied in the delay tolerant network such as the space-ground integrated network. Finally, a simulation platform was built. By means of simulation verification, it is proved that the scheme can detect more than 90% of the malicious nodes, which proves the effectiveness of the scheme.

Keywords: Space-ground integrated network; Routing evidence; Flooding attack; Grey hole attack; Black hole attack

0　引言

随着物联网技术的发展，空天地一体化网络在军事，民用，商业等等领域迅猛发展。在军事信息应用方面，空天地一体化网络技术主要体现在天地一体化通信系统组网，抗干扰技术，战术数据链，先进水下通信等方面[1]；在民用通信保障方面，主要有天基信息中继应用，全球移动宽带，航空管理信息，海洋管理信息等服务[2]；在商业通信应用，广泛应用于移动通信服务，广播业务，空中上网等多个领域[3]。因此，空天地一体化网络研究受到各国政府的高度重视，中国信通院在 2021 年发布的 6G 技术白皮书中提出三步走战略，强调持续演进，加速空天信息网络标准一体化-通信网建设[4]，美国在 2019 年提出推动空天地一体化通信网络建设，出版美军作战通信系统采用自组织网络协议[5]。

随着空天地一体化网络的发展，其中的安全问题也愈发受到关注，更是保障空天地一体化通信技术发展的基础。近年来针对空天地一体化网络的攻击频频发生，例如 2018 年北约军演时 GPS 卫星遭俄罗斯干扰[6]，2018 年赛门铁克公司发现一系列对美国和东南亚等国卫星的攻击[7]，2018 年网络安全 Black Hat 会议上提出了针对空天地一体化通信系统攻击[8]，在 2022 年俄乌战争中俄罗斯方意图催毁星链卫星网络[9]，从而破坏空天地一体化网络。根据 2022 年中国工程院于全院士的《空天信息网络关键问题》[10]，其中指出，空天安全已经成为国家重点战略与前沿方向。

因为空天地一体化无线自组织网络有如下特征：卫星节点暴露、信道开放、高时延大方差间歇链路、星上节点计算能力有限、异构网络互连、网络拓扑动态变化等[11]。所以目前的空天地一体化网络主要存在以下三个层面的安全威胁：在数据层面，存在着身份伪造、数据窃取；在运行层面，存在着黑洞攻击、欺骗攻击；在物理层面，存在着物理损毁、信号干扰等[12]。

目前的学术研究针对物理层，运行层，数据层的安全威胁都进行了相关的研究。以数据传输层为例子，日本东京大学，IEEE Fellow Kato Nei[13]教授指出在空天地一体化网络中，存在一种 SYN 洪泛攻击，该攻击会不断消耗网络资源，通过大量传输恶意报文，导致网络服务崩溃。牛津大学 Ivan Martinovic[14]教授提出在空天地的天基平台上，同样存在着类似的安全威胁。比如在无人机天基平台，存在着地面消息洪泛，虚假消息注入，恶意消息洪泛等诸多安全威胁。上述安全威胁可能导致空天地网络瘫痪，影响军事民用等方面的基本服务。

同样，严重影响空天地一体化网络的还有灰洞/黑洞攻击。该攻击指的是恶意节点在受到报文后，在具备转发条件的时候，自私丢包等行为。加拿大滑铁卢大学，中国工程院院士，IEEE Fellow，Sherman Shen[15]教授提出，某些敌手为了破坏 SAGIN 中的路由协议，进行灰洞/黑洞攻击，进行选择性转发攻击。在灰洞攻击的情况下，敌手节点会自私丢包，而在黑洞攻击中，恶意节点会丢弃所有的需要转发的报文。通过这些行为，可以造成对空天地网络的安全威胁。日本东京大学，IEEE Fellow Kato Nei 教授[13]阐明灰洞/黑洞攻击，攻击者将最便宜或最短的伪造路径广播到目的地，并且以一定比例或者只在一定时间段内丢包，从而防止被检测到。综上所述，在空天地网络中存在着多种安全威胁（如洪泛攻击，灰洞/黑洞攻击），但是由于其容断容迟网络的特点，对恶意行为和恶意节点进行检出是困难的，因此本文的工作提出了一种空天地一体化网络下安全路由方案，保证网络的安全可靠。

针对空天地场景中的研究挑战，网络开放性对攻击检测的挑战；不可信网络对快速路由选择的挑战等，本文拟解决如下问题：异构节点融合的精确协同检测问题，以及复杂时空环境下的可信路由选择问题等。

本文针对空天地一体化网络的容断容迟特点，在对网络和攻击者建模的基础上，设计相应的安全机制来保证路由的安全可靠。本文提出了基于路由证据的恶意节点检出机制，提出了可信任路由方案。具体而言，本文定义了路由转发历史证据和路由联络历史证据，通过对网络中节点的位置信息、传递信息的前向路径信息以及节点之间的连接信息进行分析。本文检测洪泛，灰洞/黑洞三种攻击行为，保证空天地一体化网络路由安全。最后，通过对空天地一体化无线自组织网络路由机制的仿真，本文应用仿真平台，对设计的安全机制进行验证与分析。

1　问题描述

由于空天地一体化无线自组织网络是跨陆、海、空、天多层级建设的异构网络，加之天基网络的特殊性导致其具有卫星节点暴露、信道开放、异构网络互连、拓扑高度动态变化、传输高时延、时延大方差及星上处理能力受限等特点，因而面临诸多安全挑战。在空天地一体化网络中，常见的几种攻击为流量洪泛攻击、黑洞攻击以及灰洞攻击。

其中，流量洪泛攻击指的是空天地一体化网络中某些恶意的路由节点在短时间内向周围路由节点大量发送消息或转发重复的消息，由于空天地一体化的网络流量信道通常不具备较高的带宽，高频率的消息发送会抢占正常的通信信道造成信道阻塞，从而导致正常的消息发送产生较长的发送时延或者因路由阻塞导致丢包，从而影响整个空天地一体化网络中的消息发送。

黑洞攻击是指空天地一体化网络中存在的恶意节点对收到的路由消息拒绝进行转发，从而在某个区域形成消息只进不出的“黑洞”现象，由于空天地一体化网络具有网络拓扑结构高度动态变化的特点，使得一些消息的传播过程中存在某些必经节点，因此，空天地一体化网络中少量恶意节点发出的黑洞攻击便能严重影响整个网络的通信质量。

与黑洞攻击类似，灰洞攻击是指空天地一体化网络中存在的恶意节点对收到的部分路由消息拒绝进行转发，这种恶意行为也能导致空天地一体化网络通信质量的降低，同时具有更高的隐蔽性，难以用正常方式检出。

2　系统模型概述

针对前文提到的空天地一体化网络中存在的恶意攻击行为，我们提出了一种空天地一体化网络中基于路由证据的路由节点恶意行为检测系统，参考一些现有工作[16][17][18][19]，考虑前文提到的空天地网络下存在的安全威胁，通过对网络中节点的位置信息、传递信息的前向路径信息以及节点之间的连接信息进行分析，可以判定网络节点是否存在攻击行为，从而保护网络安全，该系统主要是作为主体部分的恶意行为检出模块。

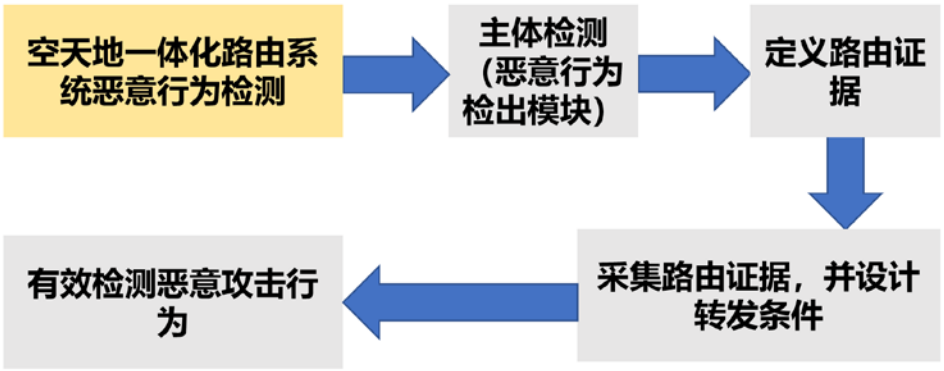

图 1　检测系统框图

Fig.1　Structure of the detection system

在本模块中，我们定义了“路由证据”这一数据。这一数据可以聚合网络中的关键信息，将转发历史进行记录，路由证据将由可信的骨干节点进行统一化管理和收集，通过对关键信息与对应节点的比对，可以实现对恶意行为的检查。

路由证据包括三个方面，路由审计证据（Evidence for delegation，E_D），路由转发证据（Evidence for forwarding，E_F）和路由联系证据（Evidence for contacting，E_C）。

我们定义从路由节点 i 到节点 j 的路由审计证据为：

$$E_D^{i\to j}=\left\{n_i,n_j,msg,T_S\right\} \tag{1}$$

其中，n_i，n_j分别表示路由节点 和 的编号，msg 为传播的消息内容，T_S为路由连接建立的起始时间戳，外部的大括号表示使用数字签名系统进行消息的签名。

定义从路由节点 i 到节点 j 的路由审计证据为：

$$E_F^{i\to j}=\left\{n_i,n_j,T_{send},Flag_{i\to j}\right\} \tag{2}$$

其中，n_i，n_j分别表示路由节点 和 的编号，T_{send}为路由传输开始的时间戳，Flag 为允许转发标志，它由由节点 j 是否存在于节点 i 对于该消息的前向通路集合中确定，外部的大括号表示使用数字签名系统进行消息的签名。

定义从路由节点 i 到节点 j 的路由联系证据为：

$$E_C^{i\to j}=\left\{n_i,n_j,msg,T_S,T_{left},Flag_{i\to j}\right\} \tag{3}$$

其中，n_i，n_j分别表示路由节点 和 的编号，msg 为传播的消息内容，T_S为路由连接建立的起始时间戳，T_{left}为消息剩余存活时间，外部的大括号表示使用数字签名系统进行消息的签名。

之后，各骨干节点收集各节点交互的信息和路由证据，并将其聚合为路由证据簇上传至中央处理系统进行进一步的分析。

通过相应路由证据对空天地一体化网络中存在的恶意节点具体的判定方法

如下：

对于流量洪泛攻击，本系统通过对比检测节点的流量速度和整个空天地一体化网络中的流量速度来进行检测，对于任一节点 $node_i$，它在 t_{s1}时间向节点 $node_j$ 发送消息的流量速度被定义为：

$$Speed_i(t_{s1}) = \sum_{m \in set_{msg}} \frac{l_{msg}}{t_{msg}} \tag{4}$$

其中，Set_{msg}表示待转发消息的集合，l_{msg}表示消息的长度，t_{msg}表示通过路由证据获得的消息传输时间。

整个空天地一体化网络中的流量速度被表示为：

$$Speed_{mean} = \sum_{i=0}^{sum} \frac{Speed_i(t_{s1})}{sum} \tag{5}$$

其中 sum 表示骨干节点所管理的节点个数和，当某些节点的流量速度显著大于该速度均值时便被判定为恶意节点。

对于黑洞攻击和灰洞攻击，我们可以将路由场景进行简化，源节点 A 企图向目标节点 C 传输数据，在此过程中，中间节点 B 进入到 A 的通信半径内，A 将会把发往 C 的数据包发送给 B, 等待 B 进入 C 的通信半径时，B 再将数据发送给 C，从而完成了整个路由过程，此过程称为“机会路由”。

通过三种路由证据，分析获得需要被转发的消息集合 Q_{msg}，参与转发任务的消息 Q_{msg}^F，以及节点之间进行了联系的集合 Q_{msg}^{ct}，同时，构建所有数据下一跳的节点集合记为 Q_{next}，此时存在两种异常行为：

（1）存在该节点转发某条消息的下一跳节点不属于与该节点建立联系的节点集合时，即用公式表述为：

$$\exists msg \in Q_{msg}, msg \notin Q_{msg}^F, Q_{msg}^{ct} \neq 0 \tag{6}$$

说明在满足转发条件时，该节点未诚实进行数据转发，发生了自私的丢包行为。

（2）存在与该节点建立联系的节点，但不存在该节点转发消息的下一跳节点时，也可以用公式表述为：

$$\exists msg \in Q_{msg}, msg \notin Q_{msg}^F, Q_{next} \not\subset Q_{msg}^{ct} \tag{7}$$

说明此时的转发不符合路由规则，该节点属于恶意节点。

与已有工作相比，[20], [21]分别主要考虑了诸如洪泛攻击，黑洞攻击，灰洞攻击中的某一种，不够全面且复杂。本工作通过引入路由证据与对于流量的综合分析，可以实现全面的安全机制。本文提出适用于空天地一体化场景的路由证据，与其他方案不同[22]，可以进行事后审计，更加符合容断容迟网络自身特点，具备更有效的适用性。

3 实验分析

在实验分析，本文进行了一系列的仿真模拟实验，仿真实验使用 The ONE simulator[23]，同时所有的实验均运行在 i7CPU，64GB RAM 的 Unubtu18.04 系统中。

模拟实验的基本参数设置如表 1 所示。

表 1　模拟实验参数设置

Tab.1　Simulation parameters settings

地图设置	默认 Helsinki 街道地图
节点总数/(个)	100
恶意节点比例	10%
节点移动速度/(m·s^{-1})	0.5~1.5
路由事件时间间隔/(s)	25~35
路由信息大小/(MB)	0.5~1
模拟时间/(h)	12h

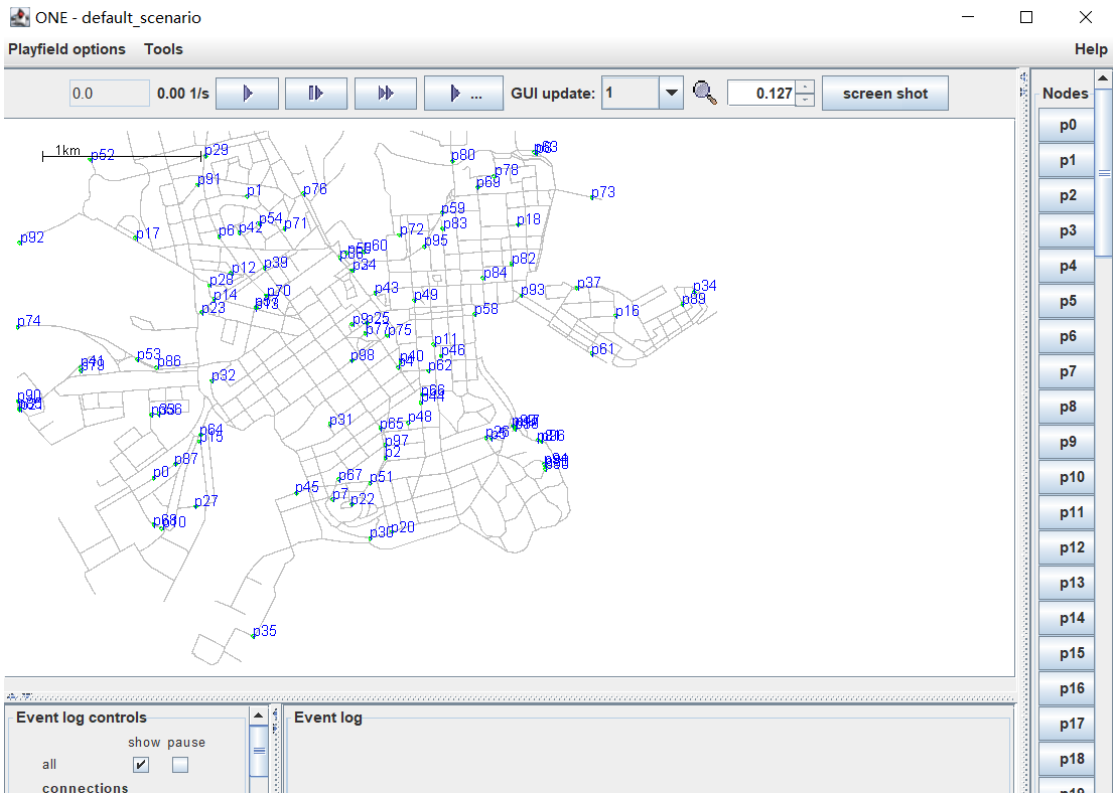

图 2　模拟仿真演示

Fig.2　Simulation demonstration

在基础的模拟实验基础上，同时，针对更复杂环境下系统的准确性和鲁棒性，本文也进行了一系列的模拟实验以验证不同情况对该系统的影响。本文探究系统中路由节点数目及恶意节点比例对于系统的影响。通过改变模拟实验中路由节点的数目以及恶意节点的比例，其结果如下列图表所示：

表 2　不同节点数及恶意节点比例下恶意节点检出比例

Tab.2　Proportion of malicious nodes detection rate under different number of nodes

检测比例 / 节点数 / 恶意节点比例	50	100	200
0%	0%	0%	0%
10%	0%	0%	35%
20%	10%	10%	58%
30%	50%	63%	97%
40%	90%	100%	98%
50%	90%	100%	98%

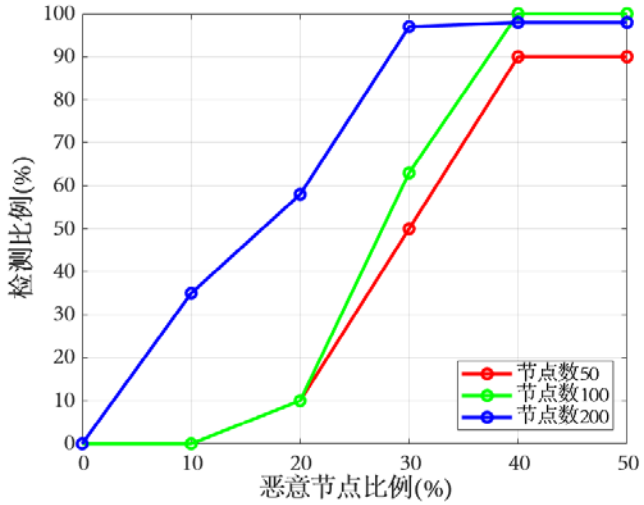

图 3　节点数目不同情况下检测情况

Fig.3　Detection rate when the number of nodes varies

可以看到，在路由系统中存在一定比例的恶意节点的情况下，本检测机制能够有效地对这些恶意节点进行检测，同时，当恶意节点数量较少时，虽然不能较为有效地将这些恶意节点检测出来，但此时恶意节点对系统通信的影响较小，系统仍可以保证较高质量的通信。

本文此后探究了路由节点移动速度对系统性能的影响。在空天地路由通信系统中，由于中继路由节点普遍具有较高的移动速度，从而容易出现节点通信意外中断的情况，探究节点移动速度对于本系统通信质量的影响同样是一个重要课题，因此本团队在模拟实验中，通过改变路由节点中恶意节点密度以及节点移动速度进行了一系列模拟实验。模拟实验的结果如下列的图表所示。

表 3　不同速度及恶意节点比例下恶意节点检出比例

Tab.3　Proportion of malicious nodes detection rate under node speed

检测比例 / 速度 / 恶意节点比例	0.5~1.5m/s	10.5~11.5m/s
0%	0%	0%
10%	35%	0%
20%	55%	5%
30%	97%	93%
40%	98%	98%

50%	98%	98%

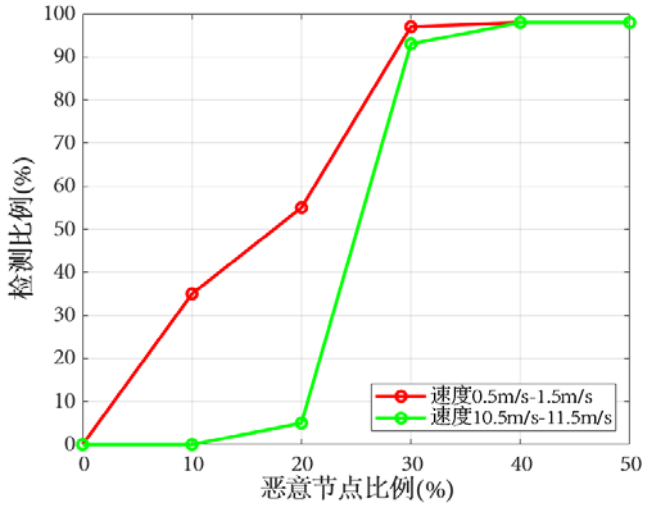

图 3　节点移动速度不同情况下检测情况

Fig.3　Detection rate when the speed of nodes varies

可以看到，虽然在节点速度较高时因为路由节点连接中断频率增加导致的恶意节点检出率有所下降，但在一定程度上仍然可以确保路由系统高质量的通信。

5　结束语

本文基于空天地一体化网络中的安全威胁，诸如洪泛攻击，灰洞/黑洞攻击，进行分析建模，并设计对应的防御对策。本文提出了路由证据的方案，对于空天地网络这类容断容迟网络进行检查，排除恶意节点，保证路由的安全性。最后通过模拟仿真，本方案可以高效检出恶意节点，保证路由可靠性，验证了方案的可行性与有效性。

参考文献

[1]张晓凯,郭道省,张邦宁.空天地一体化网络研究现状与新技术的应用展望[J].天地一体化信息网络,2021,2(04):19-26.

[2]田开波,杨振,张楠.空天地一体化网络技术展望[J].中兴通讯技术,2021,27(05):2-6.

[3]刘家祥,彭硕,蒋峥,佘小明.空天地一体化网络运营方法分析与挑战[J].移动通信,2022,46(09):45-50.

[4]IMT-2030(6G)推进组正式发布《6G 总体愿景与潜在关键技术》白皮书[J].互联网天地,2021(06):8-9.

[5]王红举,闫舟.美军战术级卫星通信系统在近距空中支援作战中应用研究[J].现代导航,2020,11(01):46-51.

[6] 刘娟,陈鼎鼎.俄罗斯反太空电子战能力[J].航天电子对抗,2019,35(05):56-59.DOI:10.16328/j.htdz8511.2019.05.013.

[7]贾铁燕,崔宁.对卫星通信系统的星地一体对抗技术初探[J].航天电子对抗,2019,35(05):28-31.DOI:10.16328/j.htdz8511.2019.05.007.

[8]亓玉璐,江荣,荣星,李爱平.基于网络安全知识图谱的天地一体化信息网络攻击研判框架[J].天地一体化信息网络,2021,2(03):57-65.

[9]陈山. 俄“暗示”可能攻击“星链”卫星[N]. 环球时报,2022-09-

21(008).DOI:10.28378/n.cnki.nhqsb.2022.008243.
[10] Yu Q, Wang J, Bai L. Architecture and critical technologies of space information networks[J]. Journal of communications and information networks, 2016, 1(3): 1-9.
[11] 沈学民,承楠,周海波,吕丰,权伟,时伟森,吴华清,周淙浩.空天地一体化网络技术：探索与展望[J].物联网学报,2020,4(03):3-19.
[12] 季新生,梁浩,扈红超.天地一体化信息网络安全防护技术的新思考[J].电信科学,2017,33(12):24-35.
[13] Guo, H., Li, J., Liu, J., Tian, N., & Kato, N. A survey on space-air-ground-sea integrated network security in 6G [J]. IEEE Communications Surveys & Tutorials, 2021, 24(1), 53-87.
[14] Strohmeier, M., Schäfer, M., Lenders, V., & Martinovic, I. Realities and challenges of nextgen air traffic management: the case of ADS-B [J]. IEEE Communications Magazine, 2014, 52(5), 111-118.
[15] Wang, Y., Su, Z., Ni, J., Zhang, N., & Shen, X. Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions [J]. IEEE Communications Surveys & Tutorials, 2021, 24(1), 160-209.
[16] Zhu, H., Du, S., Gao, Z., Dong, M., & Cao, Z. A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(1), 22-32.
[17] Zhu, H., Lin, X., Lu, R., Fan, Y., & Shen, X. Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks [J]. IEEE Transactions on Vehicular Technology, 2009, 58(8), 4628-4639.
[18] Chatterjee, R., Garg, S., Hajiabadi, M., Khurana, D., Liang, X., Malavolta, G., ... & Shiehian, S. Compact ring signatures from learning with errors [C]. In Annual International Cryptology Conference, Springer, 2021, 282-312.
[19] Rivest, R. L., Shamir, A., & Tauman, Y. How to leak a secret [C]. In International conference on the theory and application of cryptology and information security. Berlin, Heidelberg, Springer, 2001, 552-565.
[20] Xiang Y , Niu W , Tong E , et al. Congestion Attack Detection in Intelligent Traffic Signal System: Combining Empirical and Analytical Methods[J]. Security and Communication Networks, 2021, 1-17.
[21] Ouyang, Y., Liu, W., Yang, Q., Mao, X., & Li, F. Trust based task offloading scheme in UAV-enhanced edge computing network [J]. Peer-to-Peer Networking and Applications, 14, 3268-3290.
[22] Groba, C., Sartal, A., & Vázquez, X. H. Integrating forecasting in metaheuristic methods to solve dynamic routing problems: Evidence from the logistic processes of tuna vessels. Engineering Applications of Artificial Intelligence [J], 2018, 76, 55-66.
[23] Keränen, A., Ott, J., & Kärkkäinen, T. The ONE simulator for DTN protocol evaluation [C]. In Proceedings of the 2nd international conference on simulation tools and techniques, 2009, 1-10.