DSR 路由发现中基于微支付的安全数据采集激励机制

刘 高[1,2], 闫 峥[1*], 付玉龙[1]

[1] 西安电子科技大学 综合业务网理论及关键技术国家重点实验室 网络与信息安全学院 西安 中国 710126
[2] 信息网络安全公安部重点实验室 上海 中国 201204

摘要 移动自组织网中的动态源路由(DSR)协议遭受各种主动攻击, 这些攻击主要集中在路由发现阶段。目前存在各种各样的攻击检测技术来检测这些攻击。这些攻击检测技术需要收集转发节点采集的安全数据。然而由于转发节点的负载、自私、低电量等情况, 转发节点不愿采集安全数据, 并且该问题一直未被解决。本文提出一种 DSR 路由发现中基于微支付的安全数据采集激励机制。允许转发节点将采集的安全数据添加在收到的控制信息中, 然后进行转发。转发节点可利用收到的控制信息作为收据在存款服务中心处充值。提出的激励机制能够抑制请求信息滥转发给源节点造成的巨额支付, 又尽可能让每个转发节点获得奖励, 极大地实现了公平性。

关键词 移动自组织网; 动态源路由; 路由发现; 微支付; 安全数据采集; 激励机制
中图法分类号 TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.01.01

A Micropayment-Based Incentive Mechanism for Security-Related Data Collection in Route Discovery of DSR Protocol

LIU Gao[1,2], YAN Zheng[1*], FU Yulong[1]

[1] The State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710126, China
[2] Key Laboratory of Information Network Security Ministry of Public Security, Shanghai 201204, China

Abstract In Mobile Ad Hoc Networks (MANETs), Dynamic Source Routing (DSR) protocol suffers from different types of attacks, which mainly occur in route discovery. Currently, there exist various attack detection techniques for detecting these attacks. The existing attack detection techniques require security-related data that can be collected by forwarding nodes. However, the forwarding nodes might not be willing to collect security-related data due to overload, selfishness, low battery power, etc. This problem is still open and unsolved. We propose a micropayment-based incentive mechanism for security-related data collection in route discovery of DSR protocol. It allows the forwarding nodes to insert collected security-related data into control messages before forwarding them. The forwarding nodes request crediting their account by transmitting the received control messages to a deposit service center. The proposed incentive mechanism can not only constrain the amount of payment of a source node by preventing exceedingly forwarding RREQs, but also make each forwarding node obtain a reward as much as possible for the purpose of ensuring fairness.

Key words MANETs; DSR; Route discovery; Micropayment; Security-related data collection; Incentive mechanism

1 引言

移动自组织网(MANET)[1-2]是一种自组织、多跳、无固定基础设施的网络, 其允许用户在网内随意移动而保持通信。移动自组织网主要通过以下两种方式保证节点之间的相互通信。一, 若两个节点在相互的传输范围内, 它们可以使用配备的收发器进行直接的信息交换。二, 若两个节点不能进行直接通信, 其他节点会合作地帮助转发包, 这些节点被称为路由节点。如今, 移动自组织网得到了广泛应用。例如

通讯作者: 闫峥, 博士, 教授, Email: zyan@xidian.edu.cn。
本课题得到科技部重点研发计划 (No.2016YFB0800704) 和信息网络安全公安部重点实验室开放课题项目 (No.C18614) 资助。
收稿日期: 2018-10-01; 修改日期: 2018-11-02; 定稿日期: 2018-12-14

在战场[3-4]上, 移动自组织网可以保证信息及命令的实时传输; 由于移动自组织网的可快速、方便部署特性, 移动自组织网可以提供灾后营救服务[5-6]; 移动自组网可以帮助构建基于多方计算的电子投票系统[7-8]。移动自组织网具有以下特点:

1) 没有固定的基础设施;

2) 节点分享共同通信媒介, 也就是节点共享有限的带宽;

3) 网络拓扑具有动态性, 这是由许多原因导致的, 例如节点的移动性、节点的开关机、节点的故障等;

4) 节点蓄电能力有限;

5) 节点的物理安全等级较低, 例如容易被攻击者进行物理的恶意破坏;

6) 不存在管理中心。

正由于这些特征, 移动自组织网遭受不同的攻击。在 Liu 等人[9]的调研中, 主要攻击被分在了四个层上, 即物理与 MAC 层、网络层、传输层和应用层。在物理与 MAC 层, 主要存在阻塞攻击[10-14]; 在网络层, 主要存在虫洞攻击[15-17]、Rushing 攻击[18-19]、黑洞攻击[20-21]、灰洞攻击[22-23]、丢包攻击[24-25]、睡眠剥夺攻击[26-27]和女巫攻击[28-29]; 在传输层, 主要存在 SYN 泛洪攻击[30-32]和中间人攻击[33-34]; 在应用层, 主要存在虫洞攻击[35-37]。

移动自组织网中的动态源路由(DSR)协议[38-39]也遭受各种主动攻击。DSR 协议包含路由发现和路由维护阶段。而攻击的发生主要集中在路由发现阶段, 这些攻击主要包括虫洞攻击、黑洞攻击和灰洞攻击。目前存在许多攻击检测技术来检测这些攻击。这些攻击检测技术需要收集转发节点采集的安全数据, 例如时间戳、位置信息。然而由于转发节点的负载、自私、低电量等情况, 转发节点不会采集安全数据, 并且该问题一直未被解决。因此, 不能保证攻击检测技术获得充分的安全数据, 这将导致攻击检测的准确率降低, 甚至使得攻击能够避开检测。

1.1 本文工作

本文提出一种 DSR 路由发现中基于微支付的安全数据采集激励机制。也就是使用虚拟货币或者小额付款方法[40-41]来激励转发节点采集安全数据然后提供给配备攻击检测技术的源节点。具体来说, 转发节点把收到的控制信息作为收据存储在本地, 将采集的安全数据添加在收到的控制信息中, 然后转发控制信息。当转发节点和存款服务中心的连接为快速连接时, 例如 WIFI、4G, 转发节点通过向存款服务中心发送存储的收据发起充值请求。存款服务中心根据报告的收据及报告者身份, 最终对涉及的节点进行充值扣费操作。提出的数据采集激励机制尽可能让每个转发节点获得奖励, 极大地实现了公平性。除此之外, 它允许源节点根据预算限制请求信息转发形成树的最大深度及每个深度上每个节点挑选的接收它请求信息的邻居节点个数, 从而能够抑制请求信息滥转发给源节点造成的巨额支付。

1.2 相关工作

已经有大量工作[42-44]研究 DSR 路由发现中的攻击检测技术, 这些攻击检测技术涉及安全数据的采集, 但绝大多数文献没考虑对安全数据采集的激励。DSR 路由发现中安全数据采集的激励机制与节点之间相互合作转发包的激励机制[45-47]类似。但若源节点需要奖励所有提供转发服务的节点, 目前的激励机制很少能抑制请求信息滥转发引起的巨额支付。并且在有些激励机制中, 源节点只奖励寻找到的路由中的节点, 从而对其他提供过转发服务但未在寻找到的路由中的节点不公平。所以本文提出一种 DSR 路由发现中安全数据采集的激励机制, 该机制能激励转发节点转发包含采集的安全数据的控制信息, 同时可以抗滥转发和实现公平性。

1.2.1 DSR 路由发现中的攻击检测

在 DSR 路由发现的选择性黑洞攻击(即灰洞攻击)中, 恶意节点故意广播到目的节点的最小跳数来尽可能参与到选择的路由路径中, 最后选择性地丢失数据包。Mohanapriya 和 Krishnamurthi[42]提出一种修改的动态源路由协议来检测并阻止选择性黑洞攻击。在该入侵检测系统中, 入侵检测节点被设置成一种混合模式来检测节点转发的包的数量异常。当检测到任意异常, 入侵检测节点将广播阻塞信息来通知网络中的全部节点, 最终网络将隔离恶意节点。但是安全数据的采集及处理, 和阻塞信息的广播需要资源耗费, 缺少机制来激励节点去做这些工作。

车联网(VANET)遭受许多攻击, Malathi 和 Sreenath[44]测试了关于路由协议和黑洞攻击的安全特性, 并提出一种改进的 DSR 协议(MDSR 协议)来检测并阻止黑洞攻击。该协议分为两个阶段: 路由建立前的检测阶段, 和路由发现中的恶意节点检测阶段。其检测原理主要是基于以下事实: 恶意节点可能丢包或者修改包。在路由建立前的检测阶段, 检测节点通过发送包含虚假目的节点的 *RREQ* 来试探是否有节点返回包含到虚假目的节点的路由路径的 *RREP*, 若有, 说明返回 *RREP* 的节点为一个黑洞恶意攻击者。每个检测节点将黑洞恶意攻击者的身份记录下来。在路由发现中的恶意节点检测阶段, 每个检测节点检测它缓存里的路由路径是否有攻击

者, 若有的话, 检测节点将丢弃这条路由路径, 重新寻找新的不包含攻击者的路由路径。该检测机制主要以诱导形式检测, 节点可能不愿意帮助攻击者转发 *RREP*, 缺乏促进节点之间相互合作转发的激励机制。

为了检测带内虫洞攻击, Choi 等人[48]利用事实: 控制信息 *RREQ* 或 *RREP* 经过一个虫洞连接比经过一个正常连接慢。给定控制信息在未经转发情况下能够传播的距离 *TR*, 控制信息的传播速度 V_p, 及节点的平均移动速度 V_n, 有门限值 $WPT = 2 * V_n * TR / V_p^2$. 源节点在时间 T_a 发送 *RREQ* 给目标节点, 并且在时间 T_b 收到来自目标节点的 *RREP*. 因此, 通过采集 T_a 和 T_b, 源节点可以计算出每跳的延迟时间, 即 $Delayperhop = (T_a - T_b) / Hopcount$, 其中 *Hopcount* 为控制信息经过的所有跳数。当 $Delayperhop > WPT$ 时, 源节点就确认有虫洞攻击的存在。虽然安全数据采集都在源节点端完成, 但安全数据采集的完成基于转发节点的相互合作, 否则源节点无法收到 *RREP*, 从而无法采集 T_b, 缺少激励转发节点相互合作的激励机制。

Xu 和 Boppana[49]提出一种安全路由协议, 该协议要求源节点和目的节点分别验证 *RREP* 和 *RREQ* 的延迟来确定带内虫洞攻击的存在。第一, 源节点发送目标节点包含发送时间的 *RREQ*。第二, 目标节点收到 *RREQ*, 根据 *RREQ* 里的发送时间和其接收到 *RREQ* 的时间, 计算延迟时间。第三, 目标节点过滤掉那些每跳延迟超过一定门限的重复的 *RREQ*, 然后利用一个可接受的 *RREQ* 来更新门限。类似地, 源节点利用来自目标节点的 *RREP* 来检测带内攻击。若没有转发节点的合作参与, 源节点和目标节点不能收集到控制信息的发送时间, 缺乏鼓励节点对安全数据采集转发的激励机制。

基于马尔可夫链分类器的修改版, Sun 等人[50]提出一个异常检测系统来检测由伪造的 *RREP* 造成的中断攻击。在 DSR 路由发现阶段, 节点采集以下特征作为该异常检测系统的输入, 即路由表项的变化率和跳数的变化率。然而安全数据的采集仍然需要转发节点之间的相互合作, 但缺乏这种激励机制。

Qazi 等人[51]提出一种安全的 DSR 路由发现方案来抵抗带内攻击。每个节点记录控制信息的接收时间, 然后将接收时间和转发时间添加到该控制信息中, 最终转发控制信息。因此, 源节点可以确定控制信息在两两转发节点之间的传输时间, 从而检查出是否存在虫洞攻击。然而目前并没有激励机制来鼓励转发节点采集接收时间和转发时间, 然后转发它们。

1.2.2 包转发激励机制

类似于激励 DSR 路由发现中转发节点采集并转发安全数据, 存在许多激励节点之间相互合作转发包的工作。

在路由发现阶段, Marchang 和 Datta[52]提出一个信任模型, 该模型利用流量来评估一条路由路径的信任值, 然后选择一条拥有最大信任值的路由路径来进行数据包传输, 这将有利于检测和阻止灰洞攻击。第一, 每个节点监测邻居节点的流量, 然后周期性地计算并广播它对该邻居节点的信任值。第二, 监测者和被监测者的共同邻居定期地计算并广播它对被监测者的信任值。第三, 通过使用接收到的信任值, 源节点计算包含监测者和被监测者的路由路径的信任值, 最终选择一条信任值最高的路由路径进行数据包传输。该信任模型具有激励性, 每个转发节点的诚实包转发行为都可以增加其他节点对自己的信任值, 从而可以实现公平性, 但抗滥转发性不适用于评估该模型, 因为滥转发不会对源节点造成损失。

Li 等人[53]提出一种激励 P2P 网络中消息转发的激励机制。一个请求者试图寻找拥有相同信息的服务提供者之一。在该激励机制中, 若请求者发现一个服务提供者, 它将获得奖励, 否则它将不会获得奖励。在收到支付承诺之后, 请求者限制一个信息的传输距离, 即生存时间(Time-To-Live, TTL), 然后随机确定一些邻居节点, 最后转发信息给这些挑选的邻居节点并对这些节点作具有相同奖励的承诺。类似地, 若某个节点收到具有奖励承诺的信息, 它也随机确认一些节点, 并转发包含奖励承诺的信息给这些节点。当某个服务提供者收到这个信息, 它将按照信息转发的逆方向发送它的身份或地址给请求者。因此, 在路由中除了请求者的每个节点都可以从上游节点获得奖励, 并且请求者也可以获得奖励。该激励机制利用微支付实现激励的同时, 还可以抑制滥转发给请求者带来的巨额支付, 但是对提供了转发服务的却没在路由中的节点不公平, 因为它们不会获得任何奖励。

Zhong 等人[54]提出一种基于微支付的包转发激励机制。具体地, 转发节点保存收到的数据包, 然后转发新生成的数据包。转发节点可以在信任服务方利用保存的数据包作为收据来请求充值。在安全方面, 为抑制源节点与传输路径中的节点合谋,

当路由路径中最后的节点不报告收据给信用服务方时, 源节点需要向信用服务方支付一定金额。然后, 作者讨论了 DSR 路由发现的激励机制。该文献基于微支付, 对提供转发服务的转发节点给予奖励, 具有激励性。保证了每个转发节点都可以获得一定的奖励, 实现了公平性。但因控制信息的转发规模没有得到控制, 其不能抑制 DSR 路由发现阶段请求信息滥转发给源节点带来的巨额支付。

1.3 本文框架

本文框架如下: 第 2 节介绍基本知识; 第 3 节介绍 DSR 路由发现中基于微支付的安全数据采集激励机制概述; 第 4 节给出 DSR 路由发现中基于微支付的安全数据采集激励机制具体过程, 并给出示例; 第 5 节给出了对激励机制的分析。

2 基本知识

本节介绍预备知识。

哈希函数[5-56]

若 H 是安全的哈希函数, 它应该满足如下条件: 1.给定 $y=H(x)$, 多项式时间内不能获得 x。2.不能在多项式时间内找到使得 $H(x_1)=H(x_2)$ 的 (x_1,x_2)。

离散对数难题[57-58]

给定 q 阶乘法循环群 G_1, G_1 的生成元 g, 根据 $y=g^x$ 在多项式时间内计算出 x 是不可行的。

双线性对[59-60]

若 G_1 和 G_2 为 q 阶乘法循环群, g 为 G_1 的生成元。假设离散对数难题存在于 G_1 和 G_2 中。一个双线性映射 $e:G_1\times G_1\to G_2$ 应该满足以下三个要求: 1.双线性: 给定任意 $P,Q\in G_1$, $a,b\in Z_q^*$, $e(P^a,Q^b)=e(P,Q)^{ab}$ 且 $e(P,P)\neq 1_{G_2}$; 2.非退化性: 存在使得 $e(P,Q)\neq 1_{G_2}$ 的 $P,Q\in G_1$; 3.可计算性: 对任意 $P,Q\in G_1$, 可高效地计算 $e(P,Q)$。

间隙 Diffie-Hellman(GDH)群[61-63]

若 g 为乘法循环群 G_1 的生成元。

计算 Diffie-Hellman(CDH) 问题: 对于任意 $a,b\in Z_q^*$, CDH 问题是根据 (g^a,g^b) 计算 g^{ab}。

决策 Diffie-Hellman(DDH)问题: 对于任意 $a,b,c\in Z_q^*$, 给定 (g^a,g^b,g^c), DDH 问题是确定 g^{ab} 是否等于 g^c。

若在 G_1 中, CDH 问题难解决, 但 DDH 问题可以有效解决, 则称 G_1 为间隙 Diffie-Hellman(GDH) 群。

动态源路由(DSR)协议的路由发现[64]

DSR 协议是一种按需路由协议。在 DSR 协议中, 每个节点保持一个存储着路由信息的路由缓存列表。DSR 协议包括两个阶段, 即路由发现阶段和路由维护阶段。

在路由发现阶段, 源节点产生 *RREQ*, 即 $\{source\ node\ address, destination\ node\ address, route\ list, ID\}$, 然后广播该 *RREQ*, 其中 *source node address* 是源节点地址, *destination node address* 是目的节点地址, *route list* 记录该 *RREQ* 经过的节点的地址, *ID* 是源节点给该 *RREQ* 分配的标识。在收到 *RREQ* 后, 每个节点首先检验它是否已经接受或者转发过该控制信息。若节点确认收到的 *RREQ* 是新鲜的, 它将把自己的地址放入 *route list*, 最终广播新生成的 *RREQ* 给邻居节点。若目的节点或拥有到目的节点的中间节点接收到 *RREQ*, 它们将产生 *RREP*, 即 $\{source\ node\ address, destination\ node\ address, route\ list\}$, 其中 *route list* 包含从源节点到目的节点的完整路由路径。最终, *RREP* 将被按照 *route list* 逆方向转发到源节点。

3 DSR 路由发现中基于微支付的安全数据采集激励机制概述

图 1 展示了提出的 DSR 路由发现中基于微支付的安全数据采集激励机制框架, 其包括两种类型的实体, 即存款服务中心以及普通节点。存款服务中心负责普通节点的注册及对它们的账户进行充值扣费操作。普通节点作为用户可以在移动自组织网中利用注册的数字证书进行安全通信。

DSR 路由发现中, 源节点作为一个攻击检测者[51], 它需要路由发现中各节点采集的安全数据, 包括时间戳、位置信息, 然后执行相应的攻击检测算法来检测发现的路由路径是否安全。因此所有帮助它采集安全数据的节点应该从它那里获得一些奖励。而源节点应该奖励所有帮助它采集过安全数据的节点。于是在路由发现过程中, 允许转发节点采集安全数据, 然后将之添加到收到的控制信息中, 并将新生成的控制信息转发。当与存款服务中心的连接为快速连接时, 转发节点可以利用收到的控制信息作为收据, 向存款服务中心报告请求充值。存款服务中心利用所有收到的控制信息及报

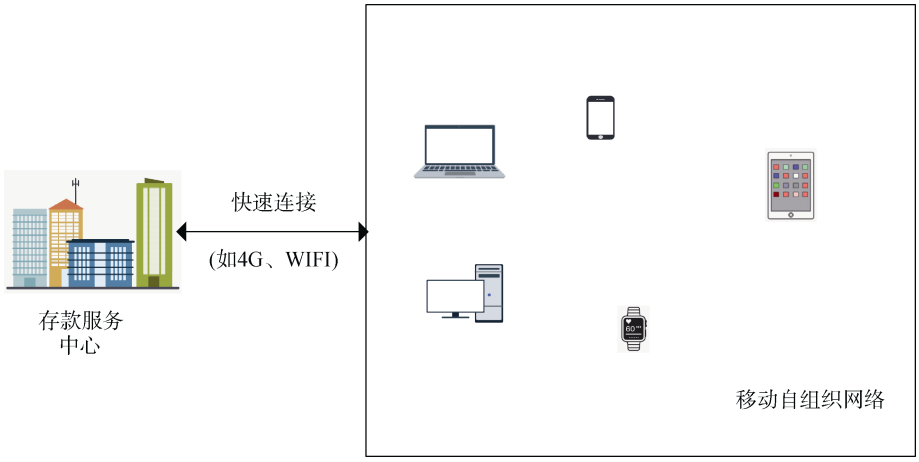

图 1　系统框架

Figure 1　System Architecture

告者身份建立树和连续虚拟回复路径，最终对相应节点的账户进行充值扣费操作。其流程如图 2 所示。

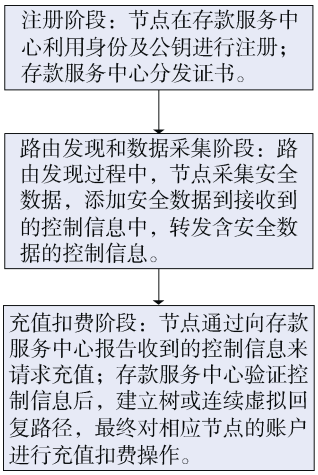

图 2　提出的数据采集激励机制流程图

Figure 2　Flow Diagram of Proposed Data Collection Incentive Mechanism

提出的 DSR 路由发现中基于微支付的安全数据采集激励机制包含三个阶段，即**注册阶段**、**路由发现和数据采集阶段**和**充值扣费阶段**。

注册阶段

注册阶段允许节点在可信的存款服务中心(例如银行)进行注册，并获得相关的证书。

路由发现和数据采集阶段

在发起路由寻找之前，源节点首先根据自己的预算，限制请求信息转发形成树的深度及每个深度上每个节点挑选的接收它请求信息的邻居节点个数，再将这些限制条件嵌入在请求信息中并对请求信息签名，最终根据限制条件将请求信息及签名转发给几个挑选的邻居节点。

在收到请求信息后，邻居节点确定它是指定的请求信息接收方，验证该请求信息，然后收集安全数据并将之放在请求信息里，生成签名，最终按照请求信息中的限制条件将请求信息及相应签名转发给它挑选的邻居节点。

如果目的节点或者拥有到目的节点路由路径的中间节点收到请求信息及签名，仍然先确认它为指定的请求信息接收方，然后验证请求信息。对于目的节点，它将生成回复信息，添加自己采集的安全数据到回复信息中，对回复信息签名，按照请求信息里的路由路径逆向转发回复信息及签名。对于拥有到目的节点路由路径的中间节点，它将生成回复信息，添加自己到目的节点的路由路径及采集的安全数据到回复信息中，对回复信息签名，再按照请求信息中的路由路径逆向转发。

若某节点收到回复信息及签名，确认其在回复信息中的路由路径里，对回复信息进行验证，然后添加自己采集的安全数据到回复信息中，对回复信息签名，最终将回复信息及签名按照回复信息中的路由路径逆向转发，直到源节点收到回复信息及签名。

充值扣费阶段

当节点和存款服务中心的连接为快速连接时，例如 WIFI、4G，节点利用接收到的控制信息(即请求信息和回复信息)及签名在存款服务中心处进行充值。

存款服务中心验证所有接收到的请求信息及签名，并利用报告者的身份及其报告的请求信息里的路由信息建立以源节点身份为根的树[54]。给除源节点的每个非叶子节点的账户充值 α 分，给每个叶子

节点的账户充值 β $(\alpha>\beta)$ 分, 并扣除源节点账户相应的金额; 对于树之外存在的每个报告者, 源节点需要向存款服务中心支付 $\alpha-\beta$ 分, 这是为了抵制中间节点与源节点合谋不向存款服务中心提供收据报告[54]。需要注意的是, 一个目的节点或者拥有到目的节点路由路径的中间节点报告一个不同的请求信息及签名, 就会获得 β 分, 这是由于 DSR 路由发现需要寻找所有可用路径。

对于所有接收到的回复信息和签名及报告者身份, 存款服务中心类似地建立从目的节点或拥有到目的节点路由路径的中间节点开始的连续虚拟回复路径[54]。对每条连续虚拟回复路径中的每个节点账户充值 α 分, 但对该路径最后一个节点账户充值 β 分。除了连续虚拟回复路径中的节点, 若回复信息里的 *route list* 还剩 *ln* 个节点, 为了防止中间节点与源节点合谋不报告回复信息及签名, 源节点将支付 $\ln\times(\alpha-\beta)$ 分给存款服务中心。

存款服务中心可以根据来自报告者的控制信息及身份实时更新树及连续虚拟回复路径, 并实行动态的充值扣费。

由于存款服务中心可能获得来自源节点的支付, 而这些支付是由防止源节点与中间节点合谋损害其他节点利益造成, 因此需要存款服务中心将获得的金额按照特定分布随机分发给所有注册过的节点。

4 DSR 路由发现中基于微支付的安全数据采集激励机制具体过程

相关符号如表 1 所示。

注册阶段

(1) 节点 N_i 首先产生密钥对 $\left(x_i, y_i=g^{x_i}\right)$, 其中 g 是间隙 Diffie-Hellman 群 G_1 的生成元。N_i 利用 $\left(N_i, y_i\right)$ 在存款服务中心 N_{DA} 注册。

(2) 拥有密钥对 $\left(x_{DA}, y_{DA}=g^{x_{DA}}\right)$ 的 N_{DA} 给 N_i 分发一个证书 $Cert_{N_i}=\{N_{DA}, N_i, y_i,\ \sigma_{DA_i}=H\left(N_{DA}, N_i, y_i\right)^{x_{DA}}\}$, 其中 σ_{DA_i} 为 N_{DA} 产生的数字签名。并且, N_{DA} 存储 $\{N_i, y_i\}$ 在其数据库以备后续的验证。

路由发现和数据采集阶段

(1) 为方便起见, 假设 N_0 为源节点, 它试图发现目的节点 N_d. N_0 首先根据自己的预算确定合适的 TTL 和 $k=\{k_h: h=0,1,\cdots,TTL-1\}$, 该过程将在**转发规模限制**中讨论。

表 1 相关符号

Table 1 Notations

符号	描述
N_i	第 i 个节点的身份(地址)
x_i	N_i 的私钥
y_i	N_i 的公钥
N_{DA}	存款服务中心的身份(地址)
$Cert_{N_i}$	N_{DA} 分发给 N_i 的数字证书
N_d	目的节点的身份(地址)
h	距离源节点的跳数
k_h	h 跳上每个节点挑选的接收它 *RREQ* 的邻居节点数目
k_h'	h 跳上每个节点挑选的接收它 *RREQ* 的邻居节点真实数目
TTL	允许请求信息 *RREQ* 传播的最大跳数
n_h	转发 *RREQ* 形成的树中从 0 跳到 h 跳的节点期望总数
m_h	转发 *RREQ* 形成的树中 h 跳上的节点期望数目
ID	*RREQ* 的标识
srd	安全数据, 例如时间戳、位置信息等
N	估计的移动自组织网节点总数
n_{sr}	源节点收到的 *RREP* 个数
n_{fr}	转发节点收到的 *RREP* 个数
n_{dr}	目的节点或拥有到目的节点路由路径的中间节点收到的 *RREQ* 个数

(2) 源节点 N_0 随机挑选 k_0' $\left(k_0'\leqslant k_0\right)$ 个邻居节点 $N_{0_1}, N_{0_2}, \cdots, N_{0_{k_0'}}$, 并生成 $RREQ_0=\{N_0, N_d, Cert_{N_0}, route\ list, h=0, ID, TTL, k, H\left(ID, TTL, k\right)^{x_0}, srd, N_{0_1}, N_{0_2}, \cdots, N_{0_{k_0'}}\}, \sigma_0=H\left(RREQ_0\right)^{x_0}$, 其中 srd 为空。然后, N_0 广播 $RREQ_0$ 及 σ_0。

(3) 在首次收到来自 N_i 的 $RREQ_i=\{N_0, N_d, Cert_{N_i}, route\ list, h, ID, TTL, k, H\left(ID, TTL, k\right)^{x_0}, srd, N_{i_1}, N_{i_2}, \cdots, N_{i_{k_i'}}\}, \sigma_i=H\left(RREQ_i\right)^{x_i}$, 节点 N_j 首先验证它是不是在列表 $\left\{N_{i_1}, N_{i_2}, \cdots, N_{i_{k_i'}}\right\}$ 里, 验证 $h<TTL$, 最终验证 $e\left(\sigma_{DA_i}, g\right)=e\left(H\left(N_{DA}, N_i, y_i\right), y_{DA}\right), e\left(H\left(ID, TTL, k\right)^{x_0}, g\right)=e\left(H\left(ID, TTL, k\right), y_0\right), e\left(\sigma_i, g\right)=e\left(H\left(RREQ_i\right), y_i\right)$。

为了加速验证[62], N_j 可挑选三个随机数 $\mu_1,\mu_2,\mu_3\in Z_q^*$, 然后进行如下验证:

$$e\left(\sigma_{DA_i}{}^{\mu_1}\sigma_i^{\mu_2}H\left(ID,TTL,k\right)^{x_0\mu_3},g\right)$$
$$=e\left(H\left(N_{DA},N_i,y_i\right)^{\mu_1},y_{DA}\right)e\left(H\left(RREQ_i\right)^{\mu_2},y_i\right)$$
$$e\left(H\left(ID,TTL,k\right)^{\mu_3},y_0\right).$$

若所有验证都成立, N_j 将其地址及采集的安全参数分别加入到 *route list* 和 *srd*, 将 *h* 增加1. 最终, N_j 产生并广播 $RREQ_j=\{N_0,N_d,Cert_{N_j},$ *route list*, h, *ID*, *TTL*, k, $H\left(ID,TTL,k\right)^{x_0}$, *srd*, N_{j_1}, $N_{j_2},\cdots,N_{j_{k_j'}}\}$, $\sigma_j=H\left(RREQ_j\right)^{x_j}$, 其中 $N_{j_1},N_{j_2},\cdots,N_{j_{k_j'}}$ 为 N_j 随机挑选的 k_j' 个邻居节点。

(4) 当目的节点或者拥有到目的节点路由路径的中间节点收到 *RREQ* 及相应签名时, 同样地, 它首先验证它是不是指定的 *RREQ* 接收方, 验证 *RREQ* 是否超出了传播范围(即 *TTL*), 并且通过签名验证 *RREQ*。若验证都成立, 目的节点 N_d 生成 $RREP_d=\{N_0,N_d,Cert_d,$ *route list*, *srd*$\}$ 及签名 $\delta_d=H\left(RREP_d\right)^{x_d}$, 或者拥有到目的节点路由路径的中间节点 N_w 生成 $RREP_w=\{N_0,N_w,Cert_w,$ *route list*, *srd*$\}$ 及签名 $\delta_w=H\left(RREP_w\right)^{x_w}$。需要注意的是, *RREP* 里的 *route list* 包含 N_0 到 N_d 的完整路由路径, *srd* 包含 *RREQ* 的 *srd*. 最终, 该目的节点或者中间节点将 *RREP* 及签名按照 *route list* 中路由路径的逆方向转发。

(5) 当某节点收到 *RREP* 及签名时, 首先确定它在 *RREP* 中的路由路径中, 对 *RREP* 进行验证, 添加采集的安全数据到 *srd*, 生成并按照 *route list* 逆方向转发新的 *RREP* 及签名, 直到源节点收到 *RREP* 及签名。

充值扣费阶段

(1) 任意转发节点利用收到的控制信息和相应签名及其身份向存款服务中心发起充值请求。具体地说, 当转发节点能够快速地连接到存款服务中心时, 例如 WIFI 或者 4G, 它向存款服务中心发送收到的控制信息和相应签名及其身份。

(2) 存款服务中心首先对接收到的所有 *RREQ* 及签名进行验证。假设接收到的所有 *RREQ* 及签名都是由节点 $N_i,i=0,1,\cdots,s$ 生成并转发的 $\{RREQ_i,\sigma_i\},i=0,1,\cdots,s$, 存款服务中心验证 $e\left(H\left(ID,TTL,k\right)^{x_0},g\right)=e\left(H\left(ID,TTL,k\right),y_0\right),e\left(\sigma_i,g\right)$ $=e\left(H\left(RREQ_i\right),y_i\right),i=0,1,\cdots,s.$

并且, 存款服务中心可以加速验证[62]。具体地, 存款服务中心首先选择 $s+1$ 个随机数 $r_0,r_1,\cdots,r_s\in Z_q^*$ 然后验证:

$$e\left(\prod_{i=0}^{s}\sigma_i^{r_i},g\right)=\prod_{i=0}^{s}e\left(H\left(RREQ_i\right)^{r_i},y_i\right).$$

若验证都通过, 存款服务中心利用接收到的所有 *RREQ* 中的路由信息和报告者的身份建立以源节点身份为根的树[54]。存款服务中心给除源节点的每个非叶子节点账户充值 α 分, 给每个叶子节点的账户充值 β $(\alpha>\beta)$ 分, 并扣除源节点账户相应的金额。对于树之外的每个报告者, 源节点需要向存款服务中心支付 $\alpha-\beta$ 分, 这是为了抵制中间节点与源节点合谋不向存款服务中心提供收据报告。需要注意的是, 一个目的节点或者拥有到目的节点路由路径的中间节点报告一个不同的请求信息及签名, 就会获得 β 分, 这是由于DSR路由发现是寻找所有可用路径。

(3) 存款服务中心同样地对所有收到的 *RREP* 和签名进行验证。若验证都通过, 存款服务中心根据所有收到的 *RREP* 中的路由信息及报告者身份建立从目的节点或拥有到目的节点路由路径的中间节点开始的连续虚拟回复路径。对每条连续虚拟回复路径中的每个节点充值 α 分, 但对路径最后一个节点充值 β 分。除了连续虚拟路径中的节点, 若 *RREP* 里的 *route list* 还剩 ln 个节点, 为了防止中间节点与源节点合谋不报告回复信息及签名, 源节点将支付 $\ln\times(\alpha-\beta)$ 分给存款服务中心。

(4) 存款服务中心可以根据来自报告者的控制信息和身份更新树及连续虚拟回复路径, 然后实行动态的充值扣费。

(5) 由于存款服务中心可能获得来自源节点的支付, 其需要按照特定随机分布将这些获得的存款分发给所有注册过的节点。

转发规模限制

在源节点广播请求信息之前, 它应该根据假设的请求信息转发形成树的最大深度及每个深度上每个节点挑选的接收它 *RREQ* 的邻居节点数目预算其花费。反过来, 源节点可以通过自己的预算限制请求

信息转发形成树的最大深度及每个深度上每个节点挑选的接收它 *RREQ* 的邻居节点数目。直观上地, 深度及每个深度上每个节点挑选的接收它 *RREQ* 的邻居节点数目越大, 找到目的节点的几率就越大, 源节点的花费也越大。

假设移动自组织网中的节点是异构的, 即当源节点决定发起路由发现时, 每个节点成为目的节点的概率相同。当转发控制信息时, 每个节点不会转发给偏向的某个邻居节点, 而是转发给随机挑选的邻居节点。为了让源节点根据自己的花费限制请求信息转发形成树的深度以及每个深度上每个节点挑选的接收它 *RREQ* 的邻居节点数目, 假设每个节点都具有相同数目的邻居节点。

源节点可以根据以下命题[53]估计其最大花费:

(1) 假设预估的移动自组织网节点总数为 N, 由 *RREQ* 转发形成树的 $h+1$ 跳上的节点期望数目为:

$$m_{h+1}=\left(N-n_{h-1}-m_h\right)\left[1-\left(1-\frac{k_h}{N-1}\right)^{m_h}\right].$$

(2) 树中从 0 跳到 $h+1$ 跳的节点期望数目为:

$$n_{h+1}=n_h+m_h d_h.$$

给定 TTL, k_h, $h=0,1,\cdots,TTL-1$, 及初始值 $n_0=m_0=1$, 源节点能够通过迭代计算出 m_{TTL} 和 n_{TTL}. 因此, 源节点的花费可以看成 TTL 和 k_h 的函数。当在 TTL 跳上的所有节点都有到目的节点的路由路径(TTL 跳上可能存在目的节点), 源节点的支付将是最大的。因此, 其最大支付为:

$$\begin{aligned}Cost&=\left(n_{TTL-1}-1\right)\alpha+m_{TTL}m_{TTL-1}\beta\\&\quad+m_{TTL}m_{TTL-1}TTL\alpha\\&=\left(n_{TTL-1}-1\right)\alpha+m_{TTL}m_{TTL-1}\left(TTL\alpha+\beta\right).\end{aligned}$$

反过来, 给定最大的预算, 源节点可以确定合适的 TTL 和 k_h.

示例

图 3 介绍了路由发现示例。源节点 N_0 设置 *RREQ* 传播的最大深度为 $TTL=4$, 每个深度上每个节点挑选的接收它 *RREQ* 的邻居节点个数分别为 $k_0=k_1=2, k_2=k_3=1$。其中虚线箭头表示接收方不是发送方挑选的邻居节点, 或者接收方因重复收到而拒绝接受来自同一个源节点的请求信息。N_0 广播 $RREQ_0\left(N_1,N_2\right),\sigma_0$, 其中 N_1,N_2 表示 N_0 挑选的接收者。N_1,N_2 对收到的 $RREQ_0\left(N_1,N_2\right),\sigma_0$ 进行验证。如果验证通过, N_1 生成并广播 $RREQ_1\left(N_3,N_4\right),\sigma_1$, N_2 生成并广播 $RREQ_2\left(N_4,N_5\right),\sigma_2$。在跳数 $TTL=4$ 上, 当目的节点 N_d 以及拥有到 N_d 路由路径的 N_8 收到 *RREQ*, 并对收到的 *RREQ* 验证通过, 它们分别生成 $RREP_d,\delta_d$ 和 $RREP_8,\delta_8$, 并按照 *RREQ* 中的路由路径逆向转发。最终, N_0 收到 $RREP_1,\delta_1$ 和 $RREP_2,\delta_2$, 从而确定两条有效路由路径 $N_0\to N_1\to N_3\to N_6\to N_8\to\cdots\to N_d$, $N_0\to N_2\to N_4\to N_7\to N_d$。在充值扣费阶段, 假设每个节点将收到的控制信息及签名发送给存款服务中心。存款服务中心建立图 3 中以 *RREQ* 传播方向的实线箭头组成的树, 以及两条虚拟回复路径, $N_8\to N_6\to N_3\to N_1\to N_0, N_d\to N_7\to N_4\to N_2\to N_0$。然后, 存款服务中心给 N_1,N_2,N_3,N_4,N_6, N_7 的账户分别充值 2α 分, 给 N_d,N_8 的账户分别充值 $\alpha+\beta$ 分, 给 N_5 的账户充值 β 分, 并扣除 N_0 账户 $14\alpha+3\beta$ 分。

5 分析

本节将对提出的 DSR 路由发现中基于微支付的安全数据采集激励机制进行性质分析, 主要包括: 激励性、抗合谋攻击、抗欺骗攻击、抗滥转发性、公平性和执行评估。表 2 展示了提出的数据采集激励机制和相关工作的性质对比。最终对提出的数据采集激励机制进行执行评估。

性质分析

激励性

在 DSR 路由发现过程中, 每个转发节点采集安全数据, 将之添加到控制信息中, 然后转发控制信息。每个转发节点可以用收到的控制信息作为收据在存款服务中心处请求充值, 存款服务中心将扣除源节点相应费用。因此, 提出的机制不仅鼓励了转发节点转发控制信息, 而且鼓励了转发节点采集安全数据。

抗合谋攻击

考虑 *RREQ* 的一条传播路径。根据文献[54], 若路径最后一个节点收到 *RREQ*, 并与源节点合谋不向存款服务中心报告收到的 *RREQ*. 具体地, 源节点承诺向这个节点支付一定金额, 即 $\beta+\varepsilon\ (\varepsilon>0)$ 分, 这个节点也承诺不会向存款服务中心报告收到的 *RREQ*. 从而, 源节点将少支付 $\alpha-(\beta+\varepsilon)$ 分。为抵抗这种合谋攻击, 对于树之外的每个报告者, 源节点需要向存款 ss 服务中心支付 $\alpha-\beta$ 分。类似地, 对于

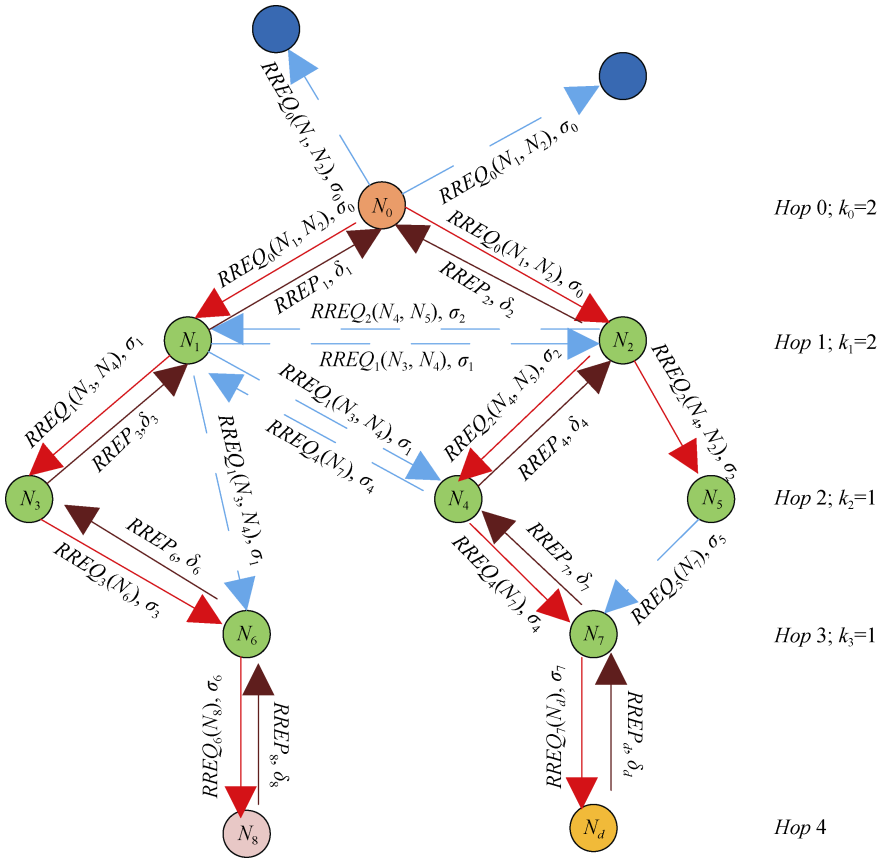

图 3　DSR 路由发现示例

Figure 3　Route Discovery Illustration of DSR Protocol

表 2　提出的数据采集激励机制与相关工作对比

Table 2　The Comparison of Proposed Data Collection Incentive Mechanism and Related Works

	激励性	抗合谋攻击	抗欺骗攻击	抗滥转发	公平性
文献[51]	*N*	*NC*	*NC*	*NC*	*NC*
文献[52]	*Y*	*NC*	*N*	*NC*	*Y*
文献[53]	*Y*	*NC*	*N*	*Y*	*N*
文献[54]	*Y*	*Y*	*Y*	*N*	*Y*
本文	*Y*	*Y*	*Y*	*Y*	*Y*

(注: *Y* 指支持; *N* 指不支持; *NC* 指不适于考虑)

RREP 的一条传播路径, 除了从目的节点或拥有到目的节点路由路径的中间节点开始的连续虚拟路径中的节点, 若 *RREP* 里的 *route list* 还剩 ln 个节点, 为了防止中间节点与源节点合谋不报告回复信息, 源节点将支付 $\ln\times(\alpha-\beta)$ 分给存款服务中心。所以, 提出的激励机制能够抵抗合谋攻击[54]。

抗欺骗攻击

任意攻击者不能伪造来自发送方的控制信息及签名, 然后利用伪造的收据(即控制信息及签名)去存款服务中心进行充值。假设 N_i 广播 $\{RREQ_i, \sigma_i\}$, 某个邻居节点接收到了这个信息, 但该邻居节点不是 N_i 指定的接收方, 并且该邻居节点试图伪造一个使得存款服务中心接受的收据, 这里主要有两种方法: 第一, 它试图获得 N_i 的私钥, 然后产生一个新的收据, 但为实现这一目的, 它需要首先解决离散对数难题, 即根据 $y_i=g^{x_i}$ 获取 x_i; 第二, 给定一个伪造的 $RREQ_i'$, 邻居节点试图通过 $e\left(\sigma_i', g\right)=e\left(H\left(RREQ_i'\right), y_i\right)$ 得到一个伪造的签名 σ_i', 但是它不能获得 σ_i', 这是因为 G_1 是一个 GDH 群。

抗滥转发

由于源节点根据预算限制了请求信息转发形成的树的深度及每个深度上每个节点挑选的接收它请求信息的邻居节点数目, 对这些限制条件进行签名, 将这些限制条件及签名放在请求信息中, 再对请求信息进行签名, 最终广播请求信息及签名。每个转发节点在收到请求信息后, 都会遵守其中的限制条件, 采集安全数据, 转发请求信息, 否则将不能获得奖励。具体地, 若节点不是请求信息发送方指定的接收方, 即使该节点采集安全数据, 转发了请求信息, 并用接收到的来自发送方的收据在存款服务中心处充值, 它的收据将不会通过验证, 从而不能获得奖励。若在 *TTL* 之外的节点采集安全数据, 并转发了请求信息, 它存储的收据仍然不能通过存款服务中心的验证, 因此不能获得奖励。

公平性

只要节点按照请求信息中的限制条件提供数据采集及转发服务, 在充值扣费阶段, 它只需要向存款服务中心报告收据, 就极有可能获取奖励, 从而尽可能保证提供数据采集及转发服务的节点能获得奖励, 实现了公平性。

执行评估

提出的数据采集激励机制在计算上的开销集中在签名的产生及验证。我们假设存款服务中心的计算能力很强, 所以我们只讨论单个节点在路由发现和数据采集阶段的计算时间耗费。一个节点的计算时间耗费主要是对收到的控制信息的签名验证时间耗费, 和对新的控制信息的签名时间耗费。在 Fan 等人[63]提出的数据聚合方案中, 作者利用 3-GHz 的奔腾 4 系统评估每个密码计算操作的时间耗费。根据文献[65-67]及 Java 双线性对密码库(jPBC),各种计算操作的时间耗费如表 3 所示。源节点需要产生 *RREQ*, 并且假若源节点收到 n_{sr} 个 *RREP*, 它需要对这些 *RREP* 进行验证, 则源节点在未使用快速验证时的时间耗费为 $2T_e+4n_{sr}T_p$, 而在使用快速验证时的时间耗费为 $2(2n_{sr}-1)T_m+4n_{sr}T_e+(2n_{sr}+1)\ T_p$。转发节点除了验证收到的 *RREQ* 外还需要制造新的 *RREQ*, 并且若该转发节点收到 n_{fr} 个 *RREP*, 它除了验证这 n_{fr} 个 *RREP*, 还需要产生 n_{fr} 个新的 *RREP*, 则其在未使用快速验证时的时间耗费为 $(n_{fr}+1)T_e+(4n_{fr}+6)T_p$, 而在使用快速验证时的时间耗费为 $2(2n_{fr}+1)T_m+4(n_{fr}+2)T_e+(2n_{fr}+5)T_p$. 当目的节点或拥有到目的节点路由路径的中间节点收到 n_{dr} 个 *RREQ*, 它需要对其进行验证, 然后生成 n_{dr} 个 *RREP*, 因此其在未使用快速验证时的时间耗费为 $n_{dr}T_e+6n_{dr}T_p$, 当使用快速验证时的时间耗费为 $2(3n_{dr}-1)T_m+7n_{dr}T_e+(3n_{dr}+1)T_p$。

表 3 密码计算时间耗费

Table 3 Time Cost of Cryptographic Computation

符号	描述	时间耗费(ms)
T_m	模乘运算	0.19
T_e	模幂运算	1.57
T_p	双线性对运算	49.25

6 结论

本文提出一种 DSR 路由发现中基于微支付的安全数据采集激励机制, 旨在激励各节点采集安全数据, 避免请求信息滥转发给源节点造成的巨额支付, 在支付方面实现对各节点的公平。通过分析, 提出的数据采集激励机制还能够抗合谋攻击和抗欺骗攻击, 适用于移动自组织网络。

致 谢 本课题得到科技部重点研发计划(课题编号 2016YFB0800704)和信息网络安全公安部重点实验室开放课题项目(项目编号 C18614)资助。

参考文献

[1] A. Nadeem and M.P. Howarth, "A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2027-2045, 2013.

[2] N. Deb, M. Chakraborty and N. Chaki, "A State-of-The-Art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks," *Advances in Parallel Distributed Computing*, pp. 169-179, 2011.

[3] C. Rajabhushanam and A. Kathirvel, "Survey of Wireless MANET Application in Battlefield Operations," *International Journal of Advanced Computer Science and Applications*, vol. 2, no. 1, 2011.

[4] M. Rath, B.K. Pattanayak and B. Pati, "Energy Efficient MANET Protocol Using Cross Layer Design for Military Applications," *Defence Science Journal*, vol. 66, no. 2, 2016.

[5] Y.N. Lien, H.C. Jang and T.C. Tsai, "A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters," in Proc. *IEEE International Conference on Distributed Computing Systems (ICDCS) Workshops*, pp. 412-417, 2009.

[6] H.C. Jang, Y.N. Lien and T.C. Tsai, "Rescue Information System for Earthquake Disasters Based on MANET Emergency Communication Platform," in Proc. *International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (WiCOM)*, pp. 623-627, 2009.

[7] C.T. Li, M.S. Hwang and C.Y. Liu, "An Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks," *Computer Communications*, vol. 31, no. 10, pp. 2534-2540, 2008.

[8] K.N.E.A. Siddiquee, K. Andersson, F.F. Khan, et al., "A Scalable and Secure MANET for an i-Voting System," *Journal of Wireless Mobile Networks*, Ubiquitous Computing, and Dependable Applications, vol. 8, no. 3, pp. 1-17, 2017.

[9] G. Liu, Z. Yan and W. Pedrycz, "Data Collection for Attack Detection and Security Measurement in Mobile Ad Hoc Networks: A survey," *Journal of Network and Computer Applications*, vol. 105, 2018.

[10] M. Strasser, B. Danev and S. Apkun, "Detection of Reactive Jamming in Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 2, pp. 16, 2010.

[11] W. Xu, K. Ma, W. Trappe, et al., "Jamming Sensor Networks: Attack and Defense Strategies," *IEEE Network*, vol. 20, no. 3, pp. 41-47, 2006.

[12] W. Xu, W. Trappe, Y. Zhang, et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proc. *International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pp. 46-57, 2005.

[13] P. Kyasanur and N.H. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 5, pp. 502-516, 2005.

[14] E. Sasikala and N. Rengarajan, "An Intelligent Technique to Detect Jamming Attack in Wireless Sensor Networks (WSNs)," *International Journal of Fuzzy Systems*, vol. 17, no. 1, pp. 76-83, 2015.

[15] Y.C. Hu, A. Perrig and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," in Proc. *IEEE International Conference on Computer Communications (INFOCOM)*, vol. 3, pp. 1976-1986, 2003.

[16] Y.C. Hu, A. Perrig and D.B. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, 2006.

[17] R. Maheshwari, J. Gao and S.R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," in Proc. *IEEE International Conference on Computer Communications (INFOCOM)*, pp. 107-115, 2007.

[18] S. Hazra and S.K. Setua, "Rushing Attack Defending Context Aware Trusted AODV in Ad-Hoc Network," *International Journal of Security, Privacy and Trust Management*, vol. 1, no. 3, pp. 176, 2012.

[19] Y.C. Hu, A. Perrig and D.B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in Proc. *ACM Workshop on Wireless Security (WiSec)*, pp. 30-40, 2004.

[20] M.Y. Su, "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems," *Computer Communications*, vol. 34, no. 1, pp. 107-117, 2011.

[21] C.W. Yu, T.K. Wu, R.H. Cheng, et al., "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks," in Proc. *Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD)*, pp. 538-549, 2007.

[22] J. Sen, M.G. Chandra, S.G. Harihara, et al., "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks," in Proc. *IEEE International Conference on Information, Communications and Signal Processing (ICICS)*, pp. 1-5, 2007.

[23] X. Gao and W. Chen, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks," in Proc. *International Conference on Network and Parallel Computing (NPC) Workshops*, pp. 209-214, 2007.

[24] K. Balakrishnan, J. Deng and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," in Proc. *Wireless Communications and Networking Conference (WCNC)*, pp. 2137-2142, 2005.

[25] C. Pu and S. Lim, "A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation," *IEEE Systems Journal*, pp. 1-9, 2016.

[26] A. Chaudhary, V.N. Tiwari and A. Kumar, "A Cooperative Intrusion Detection System for Sleep Deprivation Attack Using Neuro-Fuzzy Classifier in Mobile Ad Hoc Networks," *Computational Intelligence in Data Mining*, vol. 2, pp. 345-353, 2015.

[27] T. Martin, M. Hsiao, D. Ha, et al., "Denial-of-Service Attacks on Battery-Powered Mobile Computers," in Proc. *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 309-318, 2004.

[28] C. Piro, C. Shields and B. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," in Proc. *International Conference on Security and Privacy in Communication Networks (SecureComm)*, pp. 1-11, 2006.

[29] S. Abbas, M. Merabti, D. Llewellyn-Jones, et al., "Lightweight Sybil Attack Detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236-248, 2013.

[30] S. Wang, Q. Sun, H. Zou, et al., "Detecting SYN Flooding Attacks Based on Traffic Prediction," *Security and Communication Networks*, vol. 5, no. 10, pp. 1131-1140, 2012.

[31] M. Bellaiche and J.C. Gregoire, "SYN Flooding Attack Detection Based on Entropy Computing," in Proc. *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1-6, 2009.

[32] M. Korczynski, L. Janowski and A. Duda, "An Accurate Sampling Scheme for Detecting SYN Flooding Attacks and Portscans," in Proc. *IEEE International Conference on Communications (ICC)*, pp. 1-5, 2011.

[33] X. Long and B. Sikdar, "A Mechanism for Detecting Session Hijacks in Wireless Networks," IEEE Transactions on *Wireless Communications*, vol. 9, no. 4, pp. 1380-1389, 2010.

[34] B. Aziz and G. Hamilton, "Detecting Man-in-the-Middle Attacks by Precise Timing," in Proc. *International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, pp. 81-86, 2009.

[35] J. Newsome, B. Karp and D. Song, "Polygraph: Automatically Generating Signatures for Polymorphic Worms," in Proc. *IEEE Symposium on Security and Privacy (S&P)*, pp. 226-241, 2005.

[36] S.A. Aljawarneh, R.A. Moftah and A.M. Maatuk, "Investigations of Automatic Methods for Detecting the Polymorphic Worms Signatures," *Future Generation Computer Systems*, vol. 60, pp. 67-77, 2016.

[37] Y. Tang, B. Xiao and X. Lu, "Signature Tree Generation for Poly-

morphic Worms," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 565-579, 2011.

[38] A. Tuteja, R. Gujral and S. Thalia, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2," in Proc. *International Conference on Advances in Computer Engineering*, pp. 330-333, 2010.

[39] D.B. Johnson, D.A. Maltz and J Broch, "DSR: The Dynamic Source Routing Protocol for Multi Hop Wireless Ad Hoc Networks," *Ad Hoc Networking*, vol. 5, pp. 139-172, 2001.

[40] Y. Liu and J. Yan, "A Lightweight Micropayment Scheme Based on Lagrange Interpolation Formula," *Security and Communication Networks*, vol. 6, no. 8, pp. 955-960, 2013.

[41] Y. Liu, Q. Zhao, G. Liu, et al., "A Fairness-Enhanced Micropayment Scheme," *Wireless Personal Communications*, pp. 1-12, 2016.

[42] M. Mohanapriya and I. Krishnamurthi, "Modified DSR Protocol for Detection and Removal of Selective Black Hole Attack in MANET," *Computers and Electrical Engineering*, vol. 40, no. 2, pp. 530-538, 2014.

[43] Y.Q. Liu, Y.I. Ping, X.H. Jiang, et al., "Design and Simulation of Intrusion Detection Based on DSR Protocol," *Computer Simulation*, 2008.

[44] A. Malathi and N. Sreenath, "Black Hole Attack Prevention and Detection in VANET Using Modified DSR Protocol," *International Journal of Computer Applications*, vol. 168, no. 7, pp. 27-30, 2017.

[45] R. Vidhyalakshmi and P. Srinivasaragavan, "Public Key Based Incentive Strategies for Cooperation in MANETs," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1, 2013.

[46] R. Lu, X. Lin, H. Zhu, et al., "A Novel Fair Incentive Protocol for Mobile Ad Hoc Networks," in Proc. *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 3237-3242, 2008.

[47] D. Feng, Y. Zhu and X. Luo, "Cooperative Incentive Mechanism Based on Game Theory in MANET," in Proc. *IEEE International Conference on Networking and Digital Society (ICNDS)*, pp. 201-204, 2009.

[48] S. Choi, D.Y. Kim, D.H. Lee, et al., "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," in Proc. *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC)*, pp. 43–348, 2008.

[49] S. Xu and R.V. Boppana, "On Mitigating In-Band Wormhole Attacks in Mobile Ad Hoc Networks," in Proc. *IEEE International Conference on Communications (ICC)*, pp. 1136–1141, 2007.

[50] S. Sun, K. Wu and U.W. Pooch, "Routing Anomaly Detection in Mobile Ad Hoc Networks," in Proc. *IEEE International Conference on Computer Communications and Networks (ICCCN)*, pp. 25–31, 2003.

[51] S. Qazi, R. Raad, Y. Mu, et al., "Securing DSR against Wormhole Attacks in Multirate Ad Hoc Networks," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 582-592, 2013.

[52] N. Marchang and R. Datta, "Light-Weight Trust-Based Routing Protocol for Mobile Ad Hoc Networks," *IET Information Security*, vol. 6, no. 2, pp. 77-83, 2012.

[53] C. Li, B. Yu and K. Sycara, "An Incentive Mechanism for Message Relaying in Unstructured Peer-to-Peer Systems," *Electronic Commerce Research and Applications*, vol. 8, no. 6, pp. 582-592, 2009.

[54] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," in Proc. *IEEE International Conference on Computer Communications (INFOCOM)*, vol. 3, pp. 1987-1997, 2003.

[55] J. Shao, "Efficient Verifiable Multi-Secret Sharing Scheme Based on Hash Function," *Information Sciences*, vol. 278, pp. 104-109, 2014.

[56] G. Avoine and P. Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol," in Proc. *IEEE International Conference on Pervasive Computing and Communications (PERCOM) Workshops*, pp. 110-114, 2005.

[57] C. Meshram, "An Efficient ID-Based Cryptographic Encryption Based on Discrete Logarithm Problem and Integer Factorization Problem," *Information Processing Letters*, vol. 115, pp. 351-358, 2015.

[58] N.P. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One," *Journal of Cryptology*, vol. 12, no. 3, pp. 193-196, 1999.

[59] K.A. Shim, "An Efficient Ring Signature Scheme from Pairings," *Information Sciences*, vol. 300, pp.63-69, 2015.

[60] Y. Liu, W. Guo, C.I. Fan, et al., "A Practical Privacy-Preserving Data Aggregation (3PDA) Scheme for Smart Grid," *IEEE Transactions on Industrial Informatics*, no. 99, pp.1, 2018.

[61] D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing," in Proc. *International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (EUROCRYPT)*, pp. 514-532, 2001.

[62] Y. Liu, G. Liu, C. Cheng, et al., "A Privacy-Preserving Health Data Aggregation Scheme," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 8, pp. 3852-3863, 2016.

[63] C.I. Fan, S.Y. Huang and Y.L. Lai, "Privacy-Enhanced Data Aggregation Scheme against Internal Attackers in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666-675, 2014.

[64] M. Tamilarasi, V.R.S. Sunder, U.M. Haputhanthri, et al., "Scalability Improved DSR Protocol for MANETs," in Proc. *IEEE International Conference on Computational Intelligence and Multimedia Applications (ICCIA)*, pp. 283-287, 2007.

[65] P. Failla, "Privacy-Preserving Processing of Biometric Templates by Homomorphic Encryption," Ph. D. dissertation, School in Information Engineering, University of Siena, Italy, 2010.

[66] E.J. Goh, "Encryption Schemes from Bilinear Maps," Stanford University, 2007.

[67] M. Scott, "Implementing Cryptographic Pairings," *Lecture Notes in Computer Science*, vol. 4575, pp. 177, 2007.

刘高 于 2016 年在桂林电子科技大学数学专业获得硕士学位。现在西安电子科技大学信息安全专业攻读博士学位。研究领域为网络空间安全。研究兴趣包括: 数据采集、攻击检测和网络安全度量。Email: gaoliu9865@gmail.com

闫峥 于 2007 年在赫尔辛基工业大学电子工程专业获得博士学位。现任西安电子科技大学网络与信息安全学院教授。研究领域为网络空间安全。研究兴趣包括: 信任管理、隐私保护和网络安全度量。Email: zyan@xidian.edu.cn

付玉龙 在波城大学计算机专业获得博士学位。现就职于西安电子科技大学网络与信息安全学院。研究领域为网络空间安全。研究兴趣包括: 5G 网络安全、异构网络数据采集与处理和逻辑代数理论及应用。