抵抗 AODV 黑洞攻击的路由认证链机制

刘坤禹，周 亮*

(电子科技大学通信抗干扰技术国家级重点实验室 成都 611731)

【摘要】在移动自组网中，黑洞攻击是一种主要的针对 AODV 协议的攻击方式，黑洞攻击是指黑洞节点通过更改序列号或跳数等手段欺骗合法节点将路由导向它，从而将从源节点接收到的数据包丢弃的攻击，多个黑洞联合攻击的威胁更大。为此，该文提出一种基于安全递归函数的认证链机制，即一条路由的接续节点依赖递归函数的确定性状态转移关系实现安全的唯一关联，从而使得整条路由形成为一个认证链。该机制中，即使是采用简单递归函数类中的伪随机线性序列，只要其线性复杂度大于认证链上的节点数，则可以使得黑洞攻击者无法获取两倍于序列线性复杂度以上的连续状态值，从而可以保障路由的安全可认证性。最终证明，该文提出的路由认证链机制是一种新颖且有效的防御黑洞攻击的方法。

关 键 词 AODV； 黑洞攻击； 伪随机序列； 路由认证

中图分类号 TP393.08 **文献标志码** A doi:10.12178/1001-0548.2019235

Route Authentication Chain Mechanism Against AODV Black Hole Attack

LIU Kun-yu and ZHOU Liang*

(National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China Chengdu 611731)

Abstract The black hole attack is the main kind of attacks against AODV protocol in an Ad hoc network, black hole attack is a black hole node spoofing a legitimate node by changing the serial number or hop count, thereby drop the received packets, a much more threat by a joint attack of multiple black holes. This paper proposes an authentication chain mechanism based on the secure recursive function to overcome the black hole attack, by which the successive nodes of a route are unified only on the deterministic state transition relation of the recursive function to implement a unique association for security so that the whole route form an authentication chain. With the mechanism of this paper, even if the pseudo-random linear sequence as a kind of simple recursive function is adopted, as long as its linear complexity is greater than the number of nodes in the authenticating chain so that the attacker cannot obtain continuous state values of more than two times the linear complexity of the sequence, and then the secure authentication of the route can be guaranteed. Therefore, the mechanism and method presented in this paper is a novel and effective method to defend against the black hole attack.

Key words AODV; black hole attack; pseudo-random sequence; routing authentication

现代移动自组网 (mobile Ad-hoc networks, MANET) 的主要安全威胁之一是黑洞攻击。特别地，针对 MANET[1] 中的自组织按需距离矢量 (Ad hoc on-demand distance vector, AODV) 协议[2] 的黑洞攻击是对 MANET 的常见攻击。导致这类黑洞攻击成功的主要原因是 AODV 本身缺乏完善的路由认证机制。

路由传输中的安全认证通常分为两个层面：一是对路由中传输数据的安全认证；二是对传输数据的路由节点的身份认证。前者属于消息认证，后者称为路由认证。一般地，广义的路由认证包含 3 种情形：1) 源节点与目的节点之间的端到端节点认证[3-4]；2) 两连接节点之间的节点对认证或者链路认证[5]；3) 路由上全部节点序列的节点链认证，也可以称为狭义的路由认证[6]。

在不考虑节点间的链路信道风险时，通常默认非恶意节点传输的消息就是安全的，路由认证和消息认证的根本不同之处在于路由认证只对传输消息的节点及其节点链的可信身份进行确认，而不是对消息本身的完整性等进行确认。

收稿日期：2019－10－24；修回日期：2019－12－30

作者简介：刘坤禹 (1990－)，男，博士，主要从事无线自组织网路由协议安全方面的研究.

通信作者：周亮，Email：lzhou@uestc.edu.cn

1999 年，由公钥基础设施 PKI 支撑的认证技术开始用于网络以及路由安全保护。2002 年，文献 [7] 提出了散列链的概念来保护 DSDV[8]，SAODV[9] 也使用散列链和 RSA 密码体制来保护 AODV 消息中的跳数字段。2009 年，文献 [10] 使用 RSA 来保护 MANET 免受拜占庭攻击，其使用共享密钥的身份验证机制对消息进行端到端认证。

2011 年，文献 [11] 开发了 A-AODV，使用 HMAC 用于端到端身份验证，并通过哈希链验证控制包中的跳数值来验证控制消息的完整性，但是它存在着密钥建立的问题。同年，文献 [12] 则使用一种路由表更新的方式防止黑洞节点参与路由过程，来完成对黑洞攻击的抵抗，但是文献方案未考虑黑洞节点通过篡改 IP 地址进行伪装攻击带来的影响，这是该方案的缺陷所在。文献 [13] 在 ARAN[14] 协议上做出改进，将每个节点的身份标识加入认证包中，使得认证包通过的路径必须符合包中所有加入过节点身份的节点构成的路径，从而保证了路由路径的完整性和正确性，但是，认证传输数据会随着网络规模增大而增大。

2017 年，文献 [15] 使用 RSA 计算分组的数字签名用于节点的身份认证，并且将中间节点也加入认证，使得它完成了跳到跳认证以及端到端认证。2018 年，文献 [16] 使用 RSA、ECC 对 AODV 分组进行保护，完成了以节点身份为对象的节点认证。同年，文献 [17] 使用 ECC 加密 AODV 分组在车联网的环境下完成对 AODV 协议的保护。2019 年，文献 [18] 使用混沌映射来完成对 AODV 协议中单个黑洞攻击以及联合黑洞攻击的抵抗。

通过以上分析可以看出，所有基于 PKI 机理的网络安全措施都有计算复杂度高、密钥管理复杂等问题，因而在现实的网络安全工程中没有得到有效的实施。此外，这些方案有的是只进行节点认证，即对数据分组进行加密签名，对路径本身是否安全不作考虑；有的只使用链路认证，即端到端认证。目前，尚未有一种可以对所有参与路由的节点进行整体性认证的方案。

由于路由认证的对象是路由或节点序列，而一个路由所形成的序列由相互接续的节点构成，所以路由认证一定是一类链型结构的数据整体认证，或者是对一类数据向量或数据序列的认证。诸如伪随机序列类型的递归函数的状态值之间具有安全的关联关系，基于这个思路，本文在结合节点认证和链路认证的基础上提出一种基于认证链的路由认证方案，在减小计算开销的同时，使得认证传输数据不会随着网络规模增大而增大，并同时具备路由认证的能力。进一步地，本文修订了 AODV的路由发现机制，提出了一种用于 AODV 的路由认证链方法，实现了 MANET 中的路由保护，并证明可抵御黑洞攻击。

1　AODV 协议简介

1.1　AODV 分组类型

AODV 协议是 MANET 中的一种响应路由协议，主要由 UDP 或者 IP 协议传输的路由请求 (RREQ)、路由回复 (RREP) 和路由错误 (RERR) 这 3 种分组中各个数据段的定义和变化来实现路由发现和路由维护等功能。

RREQ 分组的结构为 $P_{\mathrm{REQ}}=(T,h(v),\mathrm{ID},\mathrm{IP}_D,\mathrm{Seq}_D,\mathrm{IP}_S,\mathrm{Seq}_S)$，$T=1$用于指示分组类型 RREQ；$h=h(v)$表示从源节点$S$开始跳转至本节点$v$的跳数 (hops)；ID是本次路由请求的标识，与源节点地址IP_S共同唯一确定一个路由请求；IP_D表示目的节点地址；Seq_D和Seq_S分别表示目的节点序列号以及源节点序列号。

RREP 分组的结构为$P_{\mathrm{REP}}=(T,h(v),\mathrm{IP}_D,\mathrm{Seq}_D,\mathrm{IP}_S,\mathrm{TTL})$，$T=2$表示分组类型；TTL表示本次路由回复分组的生存时间。

RERR 分组的结构为$P_{\mathrm{RER}}=(T,\mathrm{IP}_{\mathrm{UR}_1},\mathrm{Seq}_{\mathrm{UR}_1})$，$T=3$表示分组类型；$\mathrm{IP}_{\mathrm{UR}_1},\mathrm{Seq}_{\mathrm{UR}_1}$分别表示不可达节点的地址和序列号。

1.2　AODV 的工作过程

AODV 协议机制分为两个工作阶段。首先是路由发现阶段，源节点通过发送用于请求连接的 RREQ 分组和接收用于响应连接请求的 RREP 分组来确定路由连接链路；第二个阶段是路由维护阶段，这个阶段中通过发送 RERR 分组来广播失效或者堵塞的节点以避免之后的路由寻找、查询或者使用这些“坏”节点。

AODV 协议的路由发现过程是：源节点广播 RREQ 分组，中间节点接收此分组之后查询到达目的节点的下一跳路由链路；若中间节点也没有到下一跳节点的路由链路则将 RREQ 分组中的跳数加一并继续广播该分组；若中间节点存在到达目的节点的路由，则将 RREQ 分组转发至能够到达目的节点的下一跳路由节点；所有网络节点如此接续，寻求从源节点到目的节点的路由；参与路由的全体中间节点同时更新自己的路由表条目，该条目将用

于建立反向路径并通过这条反向路径重播 RREQ 分组；目标节点在接收到 RREQ 分组之后，使用反向路径将自身序列号加一，然后建立 RREP 分组，返回至源节点。

当源节点同时收到多个 RREP 分组时，它会选择目的序列号最高的分组来更新自己的路由表。

1.3 针对 AODV 的黑洞攻击

常规 AODV 协议既不存在对发送分组的保护机制，也不存在对传输与接收分组的节点身份的安全保护机制。如果网络中间节点被劫持或者网络被渗入攻击性的中间节点，则所有这些恶意节点可以以窃听、欺骗、修改数据分组等方式来实现对 AODV 协议以致对网络的攻击。

黑洞攻击是指恶意节点通过使用具有更高序列号的路由回复分组对源节点进行欺骗，可将整条路由导向自己，并将路由连接之后的数据分组实施丢弃处理，它是一种欺骗攻击，造成的后果是丢弃所有接收到的传输数据。

采取丢弃策略的黑洞攻击过程细节可描述如下。

1) 源节点S广播 RREQ，即：$S \to *: P_{\mathrm{REQ}} = (T, h(V), \mathrm{ID}, \mathrm{IP}_D, \mathrm{Seq}_D, \mathrm{IP}_S, \mathrm{Seq}_S)$。

2) 恶意节点M收到 RREQ 并通过更改 RREP 分组中的序列号字段，回复一个更高目的序列号的 RREP 至源节点，即：

$$M \to S: P_{\mathrm{REP}} = (T, h(V), \mathrm{ID}, \mathrm{IP}_D, \mathrm{HigherSeq}_D, \mathrm{IP}_M, \mathrm{Seq}_M)$$

3) 源节点S忽略接收到的其它 RREP，建立起与恶意节点的连接并进行载荷消息P的传输，即：$S \to M: P = \mathrm{Message}$。

4) 恶意节点M丢弃所有接收到的载荷消息P，即$M: \mathrm{drop}P$。

由此过程可知，针对 AODV 协议的黑洞攻击能够成功的前提是 AODV 协议没有有效的节点认证机制。即源 (或发送) 节点在广播机制下无法指证目的 (或某个接收) 节点的合法性，或者在获得一个 RREP 分组时没有机制去认证此 RREP 分组的来源合法性。

2 递归函数与线性移位寄存器序列

2.1 递归函数

递归函数F是一个二元组$F = (f, \sigma)$，记$\sigma(n)$为递归函数f在第n时刻 (或者时序或者计数序) 的状态或者递归输出，则：

$$\sigma(n) = f^d[\sigma(n-d)] = f\left[f^{d-1}[\sigma(n-d+1)]\right] \quad n, d \in \mathbb{N} \tag{1}$$

递归函数f可逆，是指$\sigma(n) = f^{-d}[\sigma(n+d)]$，$n, d \in \mathbb{N}$。

2.2 伪随机线性移位寄存器序列与线性复杂度

线性反馈移位寄存器 (linear feedback shift register, LFSR) 是一类简单的递归函数，由一个n级移位寄存器和一组线性组合逻辑电路构成，电路结构如图 1 所示。

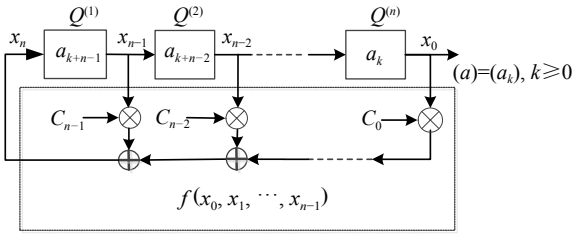

图 1 LFSR 结构

由图 1 结构产生的 LFSR 序列为$(a_k) = \left(Q^{(n)}\right) = (x_0(k)), k \geqslant 0$；LFSR 由当前状态 (或者第$k$状态) $(x_0, x_1, \cdots, x_{n-1}) = (x_0(k), x_1(k), \cdots, x_{n-1}(k))$转移至下一个状态 (或者第$k+1$状态) $(x'_0, x'_1, \cdots, x'_{n-1}) = (x_0(k+1), x_1(k+1), \cdots, x_{n-1}(k+1))$的状态转移关系为：

$$(x'_0, x'_1, \cdots, x'_{n-1}) = (x_0(k+1), x_1(k+1), \cdots, x_{n-1}(k+1)) = (x_1(k), x_2(k), \cdots, x_{n-1}(k), x_n(k))$$

$$x_n(k) = \sum_{j=0}^{n-1} c_j x_j(k) \tag{2}$$

式中，$x_n = f(x_0, x_1, \cdots, x_{n-1}) = \sum_{j=0}^{n-1} c_j x_j$称为 LFSR 的连接反馈函数；$g(x) = \sum_{j=0}^{n-1} c_j x^j$称为 LFSR 的连接反馈多项式。

当n级 LFSR 序列具有最大周期$2^n - 1$时，称该序列为 m 序列。

线性复杂度是任意序列安全性的最基本度量指标，表示采用线性移位寄存器结构的序列发生器去重构或者复现一个给定序列所需要的最小级数或连接反馈多项式的最小阶数[19]。例如，一个n级 m 序列的线性复杂度恰为n。

如果一个序列的线性复杂度为L，则只需知道该序列的任意$2L$个连续元素，即可通过解线性方程组或借助 B-M 算法找到该序列所满足的连接反馈多项式，进而可确定整个序列[19]。

通常无线网络节点 (即路由中的节点总数) 跳

数不超过 16，所以即使采用 m 序列，只要其反映状态转移关系安全性的线性复杂度大于认证链上的节点数的两倍，就可以保障有相应序列确立的路由节点之间的关联关系，从而提供可信赖的安全可认证性。

3　基于认证链的路由认证

3.1　路由模型

在节点集合V和链 (边) 集合E确定的网络(V,E)中，一条N长的路由R是一个可连接N个网络节点v(或者$v(n)$)，或者$N-1$个接续的节点串$(v(n),v(n+1))$所构成的序列，即：

$$R=(v(0),v(1),\cdots,v(n),v(n+1),\cdots,v(N-1))$$

节点标识$\mathrm{ID}=\mathrm{ID}(v)$是赋予节点$v$的某种特定属性或者赋予节点$v$的某种唯一性标识。例如，由互联网 IP 地址确定的节点标识为$\mathrm{ID}=\mathrm{ID}(v)=\mathrm{IP}(v)$。

若节点标识由某种递归函数F生成，则称此节点为链标识节点，描述为$v=(F,\mathrm{ID}(v))=((f,\sigma),\mathrm{ID}(v))$，递归函数状态$\sigma=\sigma(v)$称为节点状态。

安全链标识节点是指链标识节点的递归函数结构f保密且在节点标识和节点状态即$(\mathrm{ID},\sigma)=(\mathrm{ID}(v),\sigma(v))$均公开的条件下难以解析其结构$f$。

3.2　采用递归函数进行路由认证的机理

路由认证的主体可以是网络服务提供者、也可以是用户自己。路由认证的客体 (对象) 是整个路由的节点串R，而非单个节点$v(n)$，也非节点链路$(v(n),v(n+1))$。由于路由R是序列数据结构，所以路由认证一定是一类链型结构的数据认证，或者是对一类数据向量或者数据序列的认证。

根据路由建立的过程，构建认证链是逐个可信节点的认证过程。因而，一种直觉的采用对称密码体制的认证链构建思路是节点链路间认证的级联。但是使用该体制的缺陷在于完成路由认证必然伴随着庞大的传输数据的扩展。

由于递归函数可以建立前后状态之间的唯一关联关系，所以采用安全递归函数结构 (由有限个状态值难以重构函数结构) 的节点认证所传递的认证数据可以不存在数据扩展。

4　采用 AODV 协议的路由认证方案

4.1　AODV 认证数据分组

具有认证功能的分组P_S仍然是链上传输数据的最小数据单元，设计为：

$$P_S=(T,\mathrm{ID},\mathrm{IP}_S,\mathrm{Seq}_S,\mathrm{IP}_D,\mathrm{Seq}_D,r(v),A(v),h(v))$$

式中，$r=r(v)$表示在本节点v处生成的一个随机数；$A=A(v)$表示在本节点v处生成的节点认证值，它由节点状态$\sigma(v)$与分组的消息摘要$\mathrm{MD}(v)$模二加生成，$A(v)=\sigma(v)\oplus\mathrm{MD}(v)$；$h=h(v)$为从源节点$S$开始跳转至本节点$v$的跳数，即从源节点开始计算的链长。

本文将$(r(v),A(v))$定义为认证数据分组的认证扩展字段，与标准的 AODV 协议分组的异同点在于在使用 AODV 协议分组的基础上，将认证扩展字段扩展到 AODV 协议分组后面，形成安全路由请求消息分组，即$P_S=(P_{\mathrm{REQ}},r(v),A(v))$。本文使用的安全路由请求消息分组如图 2 所示，其中认证字段类型 0xFFFF 表示该分组为认证数据分组。安全路由回复和安全路由错误分组格式同理可得。

图 2　安全路由请求消息分组格式

4.2　采用 m 序列的节点参数预配置方案

每个节点之间通过线下分配或者其他安全方式共享两个能够生成 m 序列的参数α和β，由有限域上迹函数描述的 m 序列a为：

$$a=(a_i)=\left(\mathrm{Tr}\left(\beta\alpha^i\right)\right)\quad i=0,1,\cdots,2^n-2 \tag{3}$$

式中，级数为n的 m 序列的周期为2^n-1；生成 m 序列的本原元$\alpha\in\mathrm{GF}(2^n)$；确定 m 序列初始状态的任意非零元素$\beta\in\mathrm{GF}(2^n)$，$\beta\notin 0$。

4.3　源节点操作

源节点$v(0)$建立安全路由请求消息分组$P_S^{(0)}=(P_{\mathrm{REQ}}^{(0)},r(v(0)),A(v(0)))$，分组中，$P_{\mathrm{REQ}}^{(0)}$是源节点$v(0)$建立的 RREQ 分组，格式如 4.1 小节定义；$r(v(0))$表示节点$v(0)$产生的随机数；跳数字段初始化为$h(v(0))=0$；$A(v(0))=\sigma(v(0))\oplus\mathrm{MD}(v(0))=f^r(0)\oplus\mathrm{MD}(v(0))$为节点$v(0)$计算的节点认证值；本方案中

节点状态值$\sigma(v)$由链生成函数$f^r(x)$生成，而链生成函数$f^r(x)$由式 (3) 表示，即$\sigma(v)=f^r(h)=(\mathrm{Tr}(\beta\alpha^{r+h}),\mathrm{Tr}(\beta\alpha^{r+h+1}),\cdots,\mathrm{Tr}(\beta\alpha^{r+h+31}))$，是一个 32 位的二元序列；$\alpha,\beta$是在 4.2 小节提前共享的；$\mathrm{MD}(v(0))=\mathrm{Hash}(P_{\mathrm{REQ}}^{(0)})$为 RREQ 分组的消息摘要值，用来保证 RREQ 分组的完整性。

本文将源节点生成的随机数$r(v(0))$和节点认证值$A(v(0))$一起填入安全路由回复消息分组的认证扩展字段中，然后将建立好的安全路由请求消息分组$P_S{}^{(0)}$广播出去。

4.4 中间节点转发认证操作

中间节点在接收到安全路由请求消息分组和安全路由回复分组之后分别做出如下操作。

4.4.1 RREQ 分组接收

中间节点$v^{(*)}$接收到安全路由请求分组$P_S{}^{(*)}=(P_{\mathrm{REQ}}^{(*)},r^{(*)},A^{(*)})$后，进行如下动作：

1) 查找路由表，判断是否存在到目的节点D的路由，若不存在，则将 RREQ 分组中的跳数加一，并继续广播安全路由请求消息分组$P_S{}^{(*)}$；否则，进行步骤 2)。

2) 获取并验证安全路由请求分组$P_S{}^{(*)}$，由提前共享的参数计算节点认证值A'，判断与分组中的节点认证值$A^{(*)}$是否相同，若不相同则丢弃该分组；否则，进行步骤 3)。

3) 生成新的字段值，计算$h=h^{(*)}+1$；生成新的随机数$r=r(v)$；计算本节点认证值 A，即：

$$A=A(v)=\sigma(v)\oplus\mathrm{MD}(v)=f^r(h)\oplus\mathrm{MD}(v)=(\mathrm{Tr}(\beta\alpha^{r+h}),\mathrm{Tr}(\beta\alpha^{r+h+1}),\cdots,\mathrm{Tr}(\beta\alpha^{r+h+31}))\oplus\mathrm{Hash}(P_{\mathrm{REQ}}^{(v)}) \tag{4}$$

4) 节点认证值A生成完毕之后，将其和新生成的随机数r填入安全路由请求消息的认证扩展字段中，形成新的安全路由请求消息分组$P_S{}^{(*)}$继续向目的地址转发。

4.4.2 RREP 分组接收

当节点$v^{(*)}$接收到安全路由请求消息分组$P_S{}^{(*)}=(P_{\mathrm{REP}}^{(*)},r^{(*)},A^{(*)})$后，进行如下动作：

1) 节点$v^{(*)}$根据提前共享的参数计算节点认证值A'，判断与分组中的节点认证值$A^{(*)}$是否相同，若不相同则丢弃该分组；否则，进行步骤 2)。

2) 认证成功之后，将 RREP 分组中的跳数加一并计算新的随机数和节点认证值，生成新的安全路由回复消息分组，沿反向路径转发至源节点。

4.5 目的节点接收认证操作

目的节点D收到目的节点地址为IP_D的安全路由请求消息分组$P_S{}^{(*)}=(P_{\mathrm{REQ}}^{(*)},r^{(*)},A^{(*)})$，则获取该分组$P_S{}^{(*)}$，进行如下动作：

1) 根据提前共享的参数计算节点认证值A'，判断与分组中的节点认证值$A^{(*)}$是否相同，若不相同则丢弃该分组；否则，进行步骤 2)。

2) 认证成功之后，目的节点D将自身序列号加一，构建新的安全路由回复消息分组$P_S^{(D)}=(P_{\mathrm{REP}}^{(D)},r(v(D)),A(v(D)))$，其中新的节点认证值为$A(v(D))=\sigma(v(D))\oplus\mathrm{MD}(v(D))=f^r(0)\oplus\mathrm{MD}(v(D))$。

4.6 安全性分析

攻击者主要有两种攻击方式：1) 修改分组中的某些字段试图获取发送方信任；2) 窃听分组中的节点认证值A，试图反推出递归函数结构f。

对于攻击方式 1)，本文设计的安全认证分组由消息摘要来保护消息的完整性，一旦攻击者更改数据分组，则无法通过消息摘要的验证，另一方面，若攻击者将修改后的分组生成消息摘要，但是由于攻击者不具备生成节点状态值的共享参数，无法获得正确的节点认证值，则无法通过合法节点的认证，从而无法实施黑洞攻击。

对于攻击方式 2)，假设攻击者通过窃听获取了所有节点的节点认证值，并通过计算消息摘要得到了所有的节点状态值，但是，本文在方案中加入了随机数，使得在路由中传输的节点认证值所包含的节点状态值不会是连续的，根据 2.2 小节的描述，只要攻击者无法获取线性复杂度两倍以上的序列的连续状态值，则无法解构递归函数结构f，从而无法得到合理的节点状态值从而欺骗合法节点。

综上所述，本文的方案能够抵御 AODV 路由协议中的黑洞攻击。

5 结 束 语

本文提出了基于认证链机制的路由认证来完成对 AODV 路由协议中黑洞攻击的抵抗，在分析了 AODV 协议的基础上，建立了路由认证的数学模型并实现了路由认证的目标。进一步地，本文修订了 AODV 的路由发现机制，提出了一种用于 AODV 的路由认证链方法，实现了 MANET 中的路由保护，本路由认证方案使得黑洞节点无法得到安全链标识节点的信任，从而无法实施攻击。由于黑洞攻击节点无法获取线性复杂度两倍以上的伪随机序列的连续状态值，因而不能实现依赖状态转移的欺骗。所以，本文方案在路由发现和数据传输阶段都能够很好地抵抗黑洞攻击，同时，认证传输数据量

没有随着路由节点的增多而增加，对协议本身只做出小的扩展，所以更容易部署。

参 考 文 献

[1] SANZGIRI K, LAFLAMME D, DAHILL B, et al. Authenticated routing for Ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(3): 598-610.

[2] DAS S R, BELDINGROYER E M, PERKINS C E. Ad hoc on-demand distance vector (AODV) routing[EB/OL]. [2003-06-20]. https://tools.ietf.org/html/rfc3561.

[3] OTHMEN S, ARAI F, BELGHITH A, et al. Secure routing protocol based on Weil paring for multi-hop cellular network (SRPMCN)[J]. International Journal of Computer Science and Network Security, 2016, 16(6): 117-124.

[4] HU Y, PERRIG A, JOHNSON D B, et al. Ariadne: A secure on-demand routing protocol for Ad hoc networks[J]. Wireless Networks, 2005, 11(1): 21-38.

[5] OTHMEN S, ZARAI F, OBAIDAT M S, et al. Secure and optimal routing protocol for multi-hop cellular networks[C]// IEEE Global Communications Conference. [S.l.]: IEEE, 2014: 1-8.

[6] 范静雯, 周亮. 基于 SEND 协议的安全路由认证机理与方法[J]. 北京信息科技大学学报 (自然科学版), 2015(2): 14-19.
FAN Jing-wen, ZHOU Liang. Mechanism and method of secure routing authentication based on SEND[J]. Journal of Beijing Information Science & Technology University, 2015(2): 14-19.

[7] HU Y, JOHNSON D B, PERRIG A, et al. SEAD: Secure efficient distance vector routing for mobile wireless Ad hoc networks[J]. Ad Hoc Networks, 2003, 1(1): 175-192.

[8] ZAPATA M G, ASOKAN N. Securing Ad hoc routing protocols[C]//Workshop on Wireless Security. [S.l.]: ACM, 2002: 1-10.

[9] PERKINS C E, BHAGWAT P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers[C]//ACM Special Interest Group on Data Communication. [S.l.]: ACM, 1994, 24(4): 234-244

[10] YU M, ZHOU M, SU W. A secure routing protocol against byzantine attacks for MANETs in adversarial environments[J]. IEEE Transactions on Vehicular Technology, 2009, 58(1): 449-460.

[11] SACHAN P, KHILAR P M. Securing AODV routing protocol in MANET based on cryptographic authentication mechanism[J]. International Journal of Network Security & Its Applications, 2011, 3(5): 229-241.

[12] JALIL K A, AHMAD Z, MANAN J A, et al. Securing routing table update in AODV routing protocol[C]//IEEE Conference on Open Systems. [S.l.]: IEEE, 2011: 116-121.

[13] 闫丽丽, 彭代渊, 高悦翔. Ad hoc 网络中认证路由协议的改进及其安全性分析[J]. 电子科技大学学报, 2011, 40(4): 577-581.
YAN Li-li, PENG Dai-yuan, GAO Yue-xiang. Security analysis of extensible authenticated routing for Ad hoc networks[J]. Journal of University of Electronic Science and Technology of China, 2011, 40(4): 577-581.

[14] SANZGIRI K, DAHILL B, LEVINE B N, et al. A secure routing protocol for Ad hoc networks[C]//International Conference on Network Protocols. [S.l.]: IEEE, 2002: 78-89.

[15] NISSAR N, NAJA N, JAMALI A, et al. Lightweight authentication-based scheme for AODV in Ad-hoc networks[C]//International Conference Wireless Technologies Embedded and Intelligent Systems. [S.l.]: IEEE, 2017: 1-6.

[16] KUMAR R, TRIPATHI S, AGRAWAL R, et al. A secure handshaking AODV routing protocol (SHS-AODV)[C]//International Conference on Recent Advances in Information Technology. [S.l.]: ACM, 2018: 1-5.

[17] TYAGI P, DEMBLA D. Advanced secured routing algorithm of vehicular Ad-hoc network[J]. Wireless Personal Communications, 2018, 102(1): 41-60.

[18] ELSEMARY A M, DIAB H. BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map[J]. IEEE Access, 2019: 95197-95211.

[19] 万哲先. 代数和编码[M]. 北京: 高等教育出版社, 2007.
WANG Zhe-xian. Algebra and coding[M]. Beijing: Higher Education Press, 2007.

编　辑　刘飞阳