# 基于时间自动机的 Ad hoc 网络入侵检测

易 平[①②] 柳 宁[①] 吴 越[①]
[①](上海交通大学信息安全工程学院 上海 200030)
[②](东南大学儿童发展与学习科学教育部重点实验室 南京 210096)

**摘 要**：该文提出一种基于时间自动机分布式合作的入侵检测算法。首先，将整个网络分为子区域，每一区域随机选出簇头担任监视节点，负责本区域的入侵检测。其次，按照路由协议构筑节点正常行为和入侵行为的时间自动机，监视节点收集其邻居节点的行为信息，利用时间自动机分析节点的行为，识别入侵者。该算法不需要事先进行数据训练并能够实时检测入侵行为。最后，通过模拟实验证实了算法的有效性。

**关键词**：移动 Ad hoc 网络；路由协议；网络安全；入侵检测；时间自动机
**中图分类号**：TP393 **文献标识码**：A **文章编号**：1009-5896(2009)10-2310-06

# Intrusion Detection Based Timed Automata for Ad hoc Networks

Yi Ping[①②] Liu Ning[①] Wu Yue[①]
[①](*School of Information Security Engineering*, *Shanghai Jiao Tong University*, *Shanghai* 200030, *China*)
[②](*Key Laboratory of Child Development and Learning Science of Ministry of Education*, *Southeast University*, *Nanjing* 210096, *China*)

**Abstract**: In this paper, a distributed intrusion detection approach is proposed based on timed automata. A cluster-based detection scheme is presented, where periodically a node is elected as the monitor node for a cluster. These monitor nodes can not only make local intrusion detection decisions, but also cooperatively take part in global intrusion detection. And then the timed automata is constructed by the way of manually abstracting the correct behaviours of the node according to the routing protocol of Dynamic Source Routing (DSR). The monitor nodes can verify every node's behaviour by timed automata, and validly detect real-time attacks without signatures of intrusion or trained data. Compared with the architecture where each node is its own IDS agent, our approach is much more efficient while maintaining the same level of effectiveness. Finally, the intrusion detection method is evaluated through simulation experiments.

**Key words**: Mobile Ad hoc networks; Routing protocol; Security; Intrusion detection; Timed automata

## 1 引言

移动 Ad hoc 网络作为一种新型的移动多跳无线网络，与传统的无线网络有许多不同的特点。它不依赖于任何固定的基础设施和管理中心，而是通过移动节点间的相互协作和自我组织来保持网络的连接，同时实现数据的传递。移动 Ad hoc 网络无管理中心和不需要固定设施的特点，使其建网方式灵活、配置快捷方便，构造成本较低，它可广泛运用于商业和民用环境之中，如会议数据交换、紧急援救、偏远地区等一些需要临时组网的应用中。

与固定有线网络相比，移动 Ad hoc 网络面临更多的安全威胁。为了保障移动 Ad hoc 网络的安全，至今已经提出了许多安全解决方案[1]。但这些安全方案主要集中于密钥的分配与认证、路由安全算法两个方面。密钥的设置与认证和路由安全算法，这两种可以称为入侵阻止技术，所谓入侵阻止就是利用加密、认证、防火墙等技术来防止系统遭受外界的攻击。这些措施用于移动 Ad hoc 网络之中，能够发挥一定的安全防范作用。但是，由于移动 Ad hoc 网络中节点可任意移动，当网络处于敌对的环境时，节点可能被截获而泄露密钥，敌方节点可持密钥冒充合法节点加入网络进行攻击。此时，因为攻击者拥有合法的密钥，加密和认证技术都已经失效，只有通过入侵检测才能发现并清除入侵者。此外，网络安全的发展史告诉我们，任何入侵阻止方案都不可能完全阻挡外界的攻击，总有这样或那样的漏洞，因此，入侵检测就应该成为入侵阻止方案后的第 2 道防火墙。

本文提出基于时间自动机分布式合作的入侵检

2008-07-11 收到，2009-07-16 改回
国家 863 计划项目(2006AA01Z436，2007AA01Z452，2009AA01Z118)和上海市自然科学基金(09ZR1414900)资助课题

测系统。整个入侵检测系统由两部分组成，其一是分布式合作的入侵检测架构。移动 Ad hoc 网络具有自组织无管理中心的特点，因此必须采用分布式入侵检测的方法，即入侵检测点分布于整个网络。但为了节省网络资源，又不能所有节点都为入侵检测执行节点，所以，提出一种基于簇头的分布式合作的入侵检测，在每一个区域内选出一个簇头节点作为入侵响应的监视节点，负责整个区域节点行为的监视，同时各个监视节点又相互合作检测整个网络节点。所有监视节点形成了对整个网络的入侵检测。其二是基于时间自动机的入侵检测算法，我们将按需路由协议 DSR 的规范形成时间自动机，节点的行为使用时间自动机进行分析，如果不符合时间自动机的行为则认为是攻击行为。该检测算法不需要事先知道入侵行为的特征，也不需要事先进行数据训练，就可直接进行入侵检测。

## 2　相关工作

现阶段在移动 Ad hoc 网络安全方面研究主要分为 3 个方面：密钥的分配与认证、路由安全算法、入侵检测算法。本文主要介绍入侵检测方面的研究进展。

在入侵检测算法方面， Zhang 和 Lee 提出了一个基于 agent 的分布式协作入侵检测方案[2]。在该方案中 IDS agent 运行于网络中每一个节点上，执行本地数据收集和入侵检测，一旦发现有异常行为则触发整个网络的入侵检测和响应。该方案的优点是提出了使用异常检测技术的分布式合作的入侵检测和响应的框架，其不足之处是没有描述具体实现算法和进行实验评估。Zhang 在后续文献[3]中对上述方案进行了详细的论述，建立了一个 IDS 模型并用网络模拟器进行了模拟实验。Kachirski 和 Guha 提出了基于移动 agent 的入侵检测方案[4]。他们认为 Zhang 的方案每个节点都有 agent，过于占用网络资源，为了节省资源，其算法只是在某些节点上驻留有监视网络的 agent，并且 agent 的数量可按要求进行增减。Puttini 等人设计了一种分布式的入侵检测架构[5]，该架构使用基于特征的入侵检测技术。Huang 和 Lee 提出合作检测的系统[6]，该系统通过一些简单的规则来识别入侵者。Sun、Wu、和 Pooch 设计一种入侵检测 agent[7]，该 agent 利用马尔可夫链来进行入侵行为识别。Albers 提出一种利用简单网络管理协议(SNMP)所使用的管理信息库(MIB)作为入侵检测源数据的架构[8]。Bhargava 和 Agrawal 提出一种入侵检测和响应的模型[9]。Wang 提出一种鉴别 AODV 协议中序列号伪造的方法[10]。Subhadrabandhu 提出一种误用检测架构，包含两种近似算法并证明其算法取得最好的优化效果[11]。Chinyang Henry Tseng 提出了一种基于规范的入侵检测模型[12]。

表 1 对几种入侵检测方案进行了比较，它们具有以下特点。因为移动 Ad hoc 网络没有全网统一的信息监测点，任何节点收集的信息都是不完全的，所以上述方案都采用分布式邻居监测，协同检测的方法。前 3 类算法都是采用异常检测的算法，需要事先进行数据数据训练，检测率和误报率与算法和训练数据有关。基于时间自动机的入侵检测，是基于规范的入侵检测，直接将路由协议规范形成时间自动机，对节点行为按路由协议规范进行匹配，如果不符合则认为是异常行为。具有较高的检测率和较低的误报率，也不需要事先进行数据训练的特点。

## 3　入侵检测算法

### 3.1 监视节点选举算法

在移动 Ad hoc 网络中，节点的资源是有限的，如果将每个节点都作为入侵检测节点，是非常耗费网络节点资源的。为了节省节点资源，本文提出基于簇头的监视模式，整个网络划分为一个个区域，每个区域选出一个簇头作为监视节点负责整个区域入侵检测。该簇头收集整个区域内的节点的行为信息，并按路由规范进行分析，确定入侵行为。

选举算法由两部分组成，选举阶段和维持阶段。

**表 1 几种典型的入侵检测方案的比较**

| 协议名称 | 基于 agent 的分布式协作入侵检测[2] | 基于移动 agent 的入侵检测[4] | 基于 HMM 的入侵检测[7] | 基于时间自动机的入侵检测 |
|---|---|---|---|---|
| 执行者 | 驻留节点上的 agent | 移动 agent | 每个节点 | 每个节点 |
| 检测模式 | 异常检测 | 异常检测 | 异常检测 | 基于规范的检测 |
| 检测方法 | 分布式监测、邻居监视 | 分布式监测、邻居监视 | 马尔可夫链 | 分布式协作，时间自动机 |
| 优点 | 各 agent 合作监测与响应 | 可动态调整 agent 数量，降低对资源的消耗 | 较高的检测率 | 不需要数据进行训练，较高的检测率 |
| 缺点 | 事先需要数据训练 | 协议比较复杂 | 事先需要数据训练 | 需要事先按路由协议形成时间自动机 |

在选举阶段，随机而竞争性地选出监视节点。起始时，整个网络没有一个监视节点，在一段时间内如果没有任何监视节点的信息，任一节点可以广播一份告示报文宣称自己是监视节点，任何收到此告示报文节点就成为被监视节点，不能再发告示报文。告示报文只能在一跳范围内传播，不能被转发。因为通信是双向的，某个节点能收到告示报文，那么它所发出的报文也能被监视节点收到，所以监视节点能够监视告示报文传播范围内的节点行为。在选举阶段中，不同节点存在竞争性，在没有监视节点的区域内谁先广播一份告示报文，谁成为监视节点。

当区域内选举出一个监视节点后，就进入了维持阶段，监视节点周期性地广播告示报文，以维持其监视节点的地位。监视节点服务时间到了后，就重新启动一个新的选举过程，为了保证公平和随机性，上一届的监视节点将不能参加下一届监视节点的选举，除非整个区域只有它一个节点存在。图 1 显示 3 个监视节点及其监视区域分布。

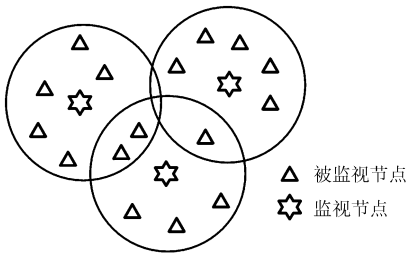


图 1 监视节点及监视区域

监视节点的选举是公平而又随机的。所谓公平性，即每个节点都能够有公平的机会选为监视节点，同时每个节点有相同的服务时间。公平性意味着选举的随机性。每个监视节点相同的服务时间要求周期性地重新选举新的监视节点。随机地选举和周期性地更换监视节点，保证了检测的安全性。如果有某个节点是入侵者，又被选举为监视节点，那么在其作为监视节点的期间可以攻击网络而不被发现，因为它是这个区域内的唯一入侵检测点。但它的监视服务时间结束后，又会选出新的监视节点，此时就会发现入侵者。

移动 Ad hoc 网络中节点可任意移动，监视节点和被监视节点都可能移动而离开原来的区域，如果一个节点在一时间内收不到告示报文，它就可以启动一个选举过程，发出告示报文，宣称自己是监视节点。如果两个监视节点靠近相互收到了告示报文，就比较它们的 ID，那个 ID 较小的节点继续保持为监视节点，另外一个就转变为被监视节点。

因为节点的移动性，被监视节点可能会移动到另一个监视节点区域内，对监视节点的信息监测就不完全，因此需要相邻簇头监视节点进行协作，才能实现对同一节点连续的监测。其具体方法为，当簇头监视节点通过 MAC 层的邻居列表，发现被监视节点不在其监视的一跳范围内时，将向周围邻居监视节点广播发出询问报文，查询该节点的行为信息，如果邻居节点有其监视节点的信息则回答相应报文。邻居监视节点协作机制可以通过广播应答的方式来实现，查询报文和回答报文按正常的路由协议形成、发送和接收报文。

### 3.2 时间自动机

每个监视节点使用时间自动机来分析监视区域内被监视节点的行为是否符合路由规范并与其他监视节点交换监视信息，以保证节点移动过程中监视的连续性。在监视过程中，它对所监视的每个节点建立时间自动机进行分析。在 DSR 路由协议中，节点可能收到并处理 4 种类型的报文：路由查询报文、路由回答报文、路由出错报文和数据报文。我们首先对路由查询报文按 DSR 路由规范形成时间自动机如图 2。

起始状态是 $S_1$，当节点收到报文后，时间自动机转向状态 $S_2$。接下来，时间自动机对接收的报文进行判断，分为两类进行处理，一类是路由查询报文，另一类是路由回答、路由出错和数据报。如果收到的报文是路由回答、路由出错和数据报，进入状态 $S_9$，同时将时钟 $t_1$ 设置为 0。如果收到的报文是路由查询报文，进入状态 $S_3$，同时将时钟 $t_1$ 设置为 0。我们设置一个有限的时间长度 $T_1$，当节点在 $T_1$ 时间内不回答或转发该报文时，就认为该节点抛弃了报文。如果该节点在 $T_1$ 时间内产生了路由回答报文，则进入状态 $S_4$，接下来对路由回答报文按 DSR 路由规范进行检查，如果是正常的，则达到状态 $S_7$，时间自动机正常结束。如果报文有些字段被非法修改了，则发出非法修改告警。在状态 $S_3$ 时，如果收到的是以前收到过的路由查询报文，则直接抛弃报文进入终止状态 $S_7$。如果节点在 $T_1$ 时间内转发路由查询报文则进入状态 $S_5$，接下来对转发的路由查询报文按 DSR 路由规范进行检查，如果修改了一些不能变化的字段，则发出非法修改告警，否则进入终止状态 $S_7$。如果在状态 $S_3$ 超过 $T_1$ 时间没有动作，这时有可能是节点移动离开了监视区域，监视节点不能收到节点所转发的路由报文，所以向周围监视节点发出询问，是否收到该节点的转发报文，同时将时间 $t_2$ 设置为 0。这里设置另外一个时间长度 $T_2$，用于等待邻居节点的回答。如果邻居监视节点收到

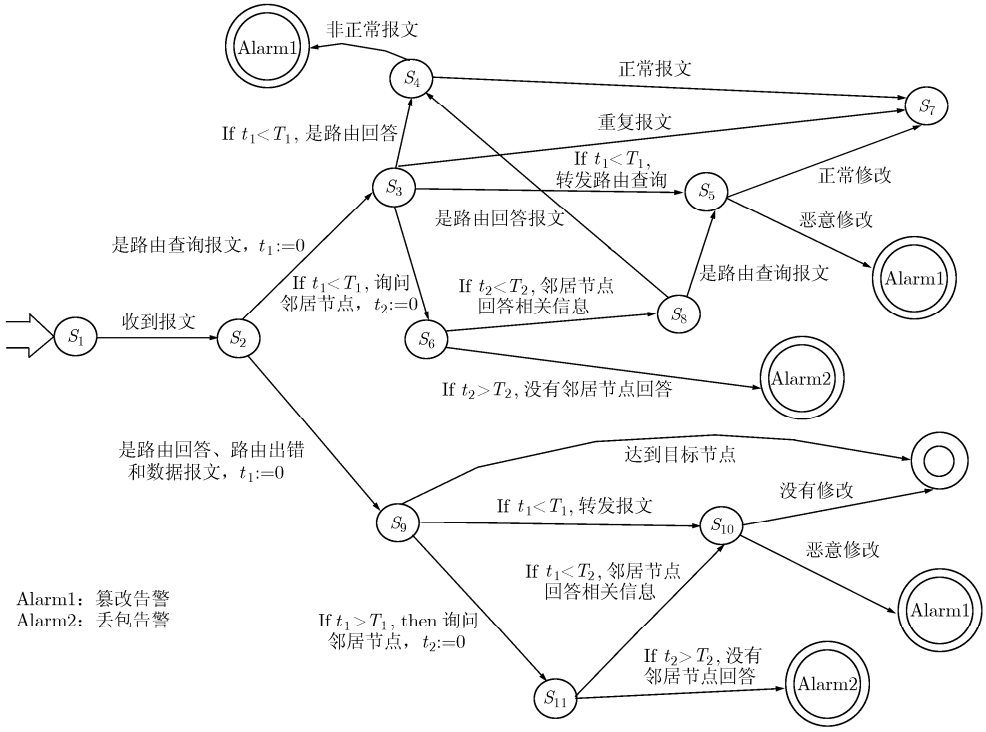


图 2　节点收到报文后处理过程的时间自动机

并在 $T_2$ 时间内将报文信息发回，则状态转向 $S_8$，是路由查询报文将报文信息发到监视节点，转到状态 $S_5$ 进行比较，是路由回答报文将报文信息发到监视节点，转到状态 $S_4$ 进行比较。如果在 $T_2$ 时间内未收到邻居节点报文，说明该节点不参与路由转发，则发出抛弃报文告警。

在 DSR 路由协议中，对于路由回答报文、路由出错、数据报文 3 种报文的处理过程是同样的，可以采用相同的时间自动机进行分析处理。如图 2，起始状态是 $S_1$，当节点收到报文转向状态 $S_2$。如果收到的报文是路由回答、路由出错、数据报文 3 种报文之一，则进入状态 $S_9$，同时将时间 $t_1$ 设置为 0。以下可转入 3 个状态，如果本节点已经是报文目标节点，则进入终止状态 $S_{12}$。如果在 $T_1$ 期限内转发报文，则进入状态 $S_{10}$，在 DSR 路由协议中对这 3 种报文是只能原样转发不能进行修改的，接下来只要对照一下转发前后的报文，如果有不同则发出非法修改告警，如果相同则进入终止状态。在状态 $S_9$ 时，如果超过 $T_1$ 没有收到转发报文，则向邻居监视节点查询该报文信息，同时将 $t_2$ 设为 0。进入状态 $S_{11}$，如果邻居监视节点在 $T_2$ 周期内收到其发出报文，则将信息发来，进入状态 $S_{10}$，如果邻居没有收到则发出抛弃报文告警。

图 2 是处理当一个节点接收报文后的处理流程。图 3 显示的是当节点发送报文后的时间自动机处理流程图。当监视节点监视某个节点 $A$ 发出报文时，状态是由 $S_1$ 到 $S_2$，下面可能是下列两种情况之一：其一，以 $A$ 节点为源节点的报文，即 $A$ 节点发出了这个报文，状态是由 $S_2$ 到 $S_4$，然后比较一下发出报文源地址与节点的地址，如果相符的话则转入终止状态，如果不相符，则发出假冒报警。其二，$A$ 节点是中间节点，它只是转发报文，进入状态 $S_3$。同时设置时间 $t_3$ 为 0。可能节点 $A$ 接收报文时，不在监视节点的区域内，转发时节点移动进入监视节点的范围内，所以只看到节点 $A$ 发出了报文，此时监视节点等待邻居监视节点查询，如果在 $T_3$ 时间内有邻居监视节点查询，则将报文信息发来邻居监视节点，时间自动机进入终止状态。如果在 $T_3$ 时间内没有邻居监视节点查询，那么监视节点主动向周围监视节点发出查询，询问有节点收到过该报文，同时将 $t_2$ 设为 0。如果在 $T_2$ 时间内没有回答，说明没有节点发送过此报文，是节点 $A$ 编造了此报文，时间自动机发出编造告警。

## 4　模拟实验

### 4.1 实验设置

实验平台为 Pentium4 1.8 GHz， 512 MB RAM，使用的操作系统是 Red Hat Linux 7.12 ，仿真平台是 ns-2 2.26 (Network Simulator Version 2.26)。仿真中，节点总数设置为 50 个，节点运动

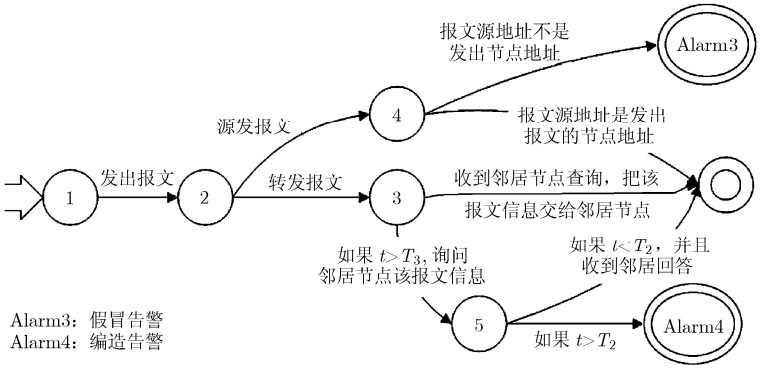


图 3 节点发送报文后处理过程的时间自动机

范围 1500 m×300 m，运动速度 0–20 m/s，网络中节点的运动采用随机运动模型，即每个节点在该区域内从一点向另一点运动，运动速度在[0,20 m/s ]内均匀分布，到达目标点后,停留一段时间，然后选择一个新的目标点，同时再选择一个新的速度，向新的目标点运动，依次类推，直至仿真结束。MAC 层使用的 802.11，传输半径为 250 m，链路带宽为 2 Mbps。模拟时间为 900 s。

### 4.2 实验结果

我们将选举算法和时间自动机在 NS-2 中进行了编码实现。为了检验入侵检测效果，按上节的分析，我们设计了 4 种对 DSR 路由协议的攻击方式。攻击方式 1 是非法修改攻击，即入侵者转发报文时，非法插入、删除和修改报文中的信息。攻击方式 2 是抛弃攻击，即入侵者只收报文，不转发任何报文。攻击方式 3 是假冒攻击，即入侵者假冒其它节点发送各种报文，如路由查询报文、数据报文等。攻击方式 4 是编造攻击，入侵者编造一些由它转发的报文，但实际上源节点并未发出此报文。

表 2 显示时间自动机对 4 种攻击方式的入侵检测率和误报率。从表中可以看出，对 4 种攻击类型都有比较高的检测率和比较低的误报率，其中对假冒攻击的检测率最高，主要原因是监视节点只需要将发出报文节点地址与报文中地址列表对照一下，如果没有就是假冒攻击，最为简单。抛弃攻击检测率最低，主要原因是监视节点不能直接做出判断，要到邻居节点去查询才能得出结果。编造攻击也是需要邻居监视节点查询才能判断，检测率也较低。但是总的来说，检测率在 80%以上，说明该算法还是十分有效的。

**表 2 4 种攻击方式的入侵检测率(%)**

| 攻击方式 | 检测率 | 误报率 |
|---|---|---|
| 修改攻击 | 91.3 | 2.9 |
| 抛弃攻击 | 83.7 | 5.7 |
| 假冒攻击 | 97.4 | 1.3 |
| 编造攻击 | 88.5 | 7.2 |

## 5 结论

在本文中，提出了基于簇头的分布式合作的入侵检测架构，整个网络分成一个个区域，每个区域内的监视节点既负责本地入侵检测又合作检测整个网络节点，通过随机选举簇头作为监视节点，并周期性地重新选举簇头，既节省网络资源又保证了入侵检测系统的安全性。在入侵检测架构的基础上，设计了基于时间自动机的入侵检测算法，通过 DSR 路由协议规范形成节点处理过程的时间自动机，对节点的每个报文的处理过程按时间自动机进行分析，实时地发现入侵行为。最后通过模拟实验检测了该算法的有效性。

## 参 考 文 献

[1] 易平, 蒋嶷川, 钟亦平, 等. 移动 Ad hoc 网络安全综述[J]. 电子学报, 2005, 33(5): 893–899.
Yi P, Jiang Y C, and Zhong Y P, *et al*.. A survey of security for mobile ad hoc networks [J]. *Acta Electronica Sinica*, 2005, 33(5): 893–899.

[2] Zhang Yong-guang and Lee Wenke. Intrusion detection in wireless Ad-hoc networks[C]. Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, August, 2000: 275–283.

[3] Zhang Yong-guang and Lee Wenke. Intrusion Detection Techniques for Mobile Wireless Networks. *Mobile Networks and Applications*, 2003, 9(5): 545–556.

[4] Kachirski O and Guha R. Intrusion detection using mobile agents in wireless ad hoc networks. IEEE Workshop on Knowledge Media Networking (KMN'02), Kyoto, Japan, 2002: 153–158.

[5] Puttini R S, Percher J M, and Mé L, *et al*.. A modular architecture for distributed IDS in MANET[C]. Proceedings

of the 2003 International Conference on Computational Science and Its Applications (ICCSA 2003), Springer Verlag, LNCS 2668, San Diego, USA, 2003: 984–990.

[6] Huang Yi-an and Lee Wenke. A cooperative intrusion detection system for ad hoc networks[C]. 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), Fairfax, VA, USA, October 31, 2003: 135–147.

[7] Sun B, Wu K, and Pooch U W. Routing anomaly detection in mobile ad hoc networks[C]. Proceedings of 12th International Conference on Computer Communications and Networks (ICCCN 03), Dallas, Texas, October 2003: 25–31.

[8] Albers P, Camp O, Percher J M, and Jouga B, *et al.*. Security in ad hoc Networks: a general intrusion detection architecture enhancing trust based approaches. Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002), Ciudad Real, Spain, Apr. 2002: 1–12.

[9] Bhargava S and Agrawal D P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks[C]. Vehicular Technology Conference, 2001: 2143–2147.

[10] Wang Wei-chao, Lu Yi, and Bhargava B K. On vulnerability and protection of ad hoc on-demand distance vector protocol[C]. Proceedings of 10th IEEE International Conference on Telecommunication (ICT), Papeete, French Polynesia, 2003: 375–382.

[11] Subhadrabandhu D, Sarkar S, and Anjum F. A framework for misuse detection in ad hoc networks—Part I[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 274–289.

[12] Chinyang Henry Tseng, Tao Song, Poornima Balasubramanyam, Calvin Ko, and Karl Levitt. A Specification-Based Intrusion Detection Model for OLSR[C]. RAID 2005, LNCS 3858, 2006: 330–350.

易　平：男，1969 年生，副研究员，研究方向为无线网络、信息安全.

柳　宁：男，1979 年生，博士生，研究方向为移动通信、信息安全.

吴　越：男，1968 年生，副教授，研究方向为无线网络、QoS.