无线自组网可信路由协议的研究

董文华
（湖北广播电视台　湖北省武汉市　430071）

摘　要：本文分析了无线自组网面临的安全风险，介绍了现有安全路由与不足之处，提出了一个以可信计算为基础、信任机制为辅助的可信路由方案，对其中涉及的具体问题进行了分析和研究。

关键词：无线自组网；网络安全；可信计算；路由协议

无线自组网（Ad Hoc Network）是由一组由自主的无线节点或终端相互合作而形成的，独立于固定的基础设施并采用分布式管理的网络。是一种自生成、自组织、自管理网络。无线自组网无需任何网络基础设备和管理支持就可以动态地创建无线网络，所有的节点分布式运行，当移动节点加入或离开网络时，网络拓扑结构会自动改变，每一个节点都可以承担路由器的工作。无线自组网非常适合通讯基础设施不存在或无法正常使用的环境，其潜在应用领域非常广泛。在无线自组网中，虽然其移动、多跳和自组织的特点可以提供随时随地的连接，但是，这些特点同时也带来了新的安全威胁。所以在无线自组网中，必须采用相应技术有效防范风险。

由于无线自组网在安全方面的种种弱点，所以国内外提出了众多的安全路由协议，主要有以下几种：

（1）ARAN，为自组网提供了身份鉴别、信息完整性和不可抵赖性等安全保证。

（2）“Watchdog”，监督节点行为，举报不可信的节点。

（3）Ad-mix，鼓励节点参与通讯。

（4）SAODV，利用数字签名保证路由信息完整性和不可抵赖性。

但是现有用于无线自组网的安全路由协议和提案没有很好地解决安全问题，主要表现在以下几个方面：

（1）一种安全路由协议一般只能够抵御一种或几种特定威胁，而对其他多数威胁则不能发挥作用。

（2）无线自组网具有网络拓扑变化快、无集中式的基础设施、节点资源有限等特点。而现有安全协议没有充分考虑无线自组网特定的环境。

（3）路由协议要么解决自私节点问题要么解决路由安全问题，但很少有同时解决这两个问题的协议。特别是，大多数防止自私节点的路由协议都是建立在假定在路由协议安全的前提基础之上的。

1 无线自组网可信路由协议

可信计算组织（Trusted Computing Group TCG）是近年来由 Intel、Microsoft、IBM 等公司发起的一个正式非赢利组织。它致力于加强彼此相互独立的计算平台上的计算环境的安全性。可信计算（Trusted Computing，TC）是 TCG 在计算和通信系统中广泛使用基于硬件安全模块（TPM Trusted Platform Module）支持下的可信计算平台，以提高系统整体的安全性。

可信计算技术的出现为解决无线自组网路由协议的安全性提供了一种新的切实可行的解决方案。将可信计算技术用于无线自组网可以在低附加数据传输、数据处理代价下提供高安全性能。

表 1：协议安全性对比
（√表示具备该属性 × 表示不具备该属性）

	1	2	3	4	5	6
TCAODV	√	√	√	√	√	√
ARAN	×	√	×	×	×	√
Watchdog	×	√	√	√	×	×
AD-MIX	√	×	√	×	√	×
SAODV	×	√	√	×	√	√

表 2：节点运动场景参数

参数	设定值
网络中节点数	50
移动范围	1000m×1000m
节点最大移动速度 (m/s)	0.01,5,10,15,20
停留时间	0s
仿真时间	300s

表 3：网络流量场景参数

参数	设定值
业务类型	cbr
最大连接数	10
节点数	50
发送速率	0.5 个 /s
随机种子数	1

可信无线自组网应具备以下特征：

（1）网络中的行为总是可以预知与可控的；

（2）网内的系统符合指定的安全策略，相对于安全策略是可信的、安全的；

（3）随着端点系统的动态接入，具备动态扩展性。

根据可信计算的原理提出可信无线自组网实现方法：

（1）在无线自组网中各个节点强制建立 TPM 可信平台模块。

（2）引入可信链模型，并据此来进行路由选择，实现带宽、系统资源重分配。

（3）在无线自组网中引入可信网络中的可信接入认证方法。

1.1 无线自组网可信路由实现

用可信计算技术对 AODV 协议进行扩展，使其能够抵御自私和恶意节点攻击，扩展后的路由协议被命名为 TCAODV（Trusted Computing Ad hoc On Demand Vector），该路由协议必须实现三个功能：

（1）该路由协议必须遵守所有无线自组网路由协议的规范，不得尝试模仿其他节点，不能伪造虚假路由报告，不能发布非法错误，传送数据的速率不能超过规定的上限，不能忽略正当的路由请求。

（2）该路由协议必须能验证无线设备驱动程序。如果不能证明驱动可信性，将拒绝驱动参与到无线自组网中。

（3）该路由协议必须监测从驱动层发送来的报告，如果物理设备超出预设的极限，将拒绝进一步参与网络。

协议实现过程如下：

可信平台要对 TCAODV 协议进行可信度量并验证，当验证通过后，将该协议纳入可信边界，并允许其运行。同时可信平台向通过验证的路由颁发经可信平台签名的证书。每一节点都在其可信存储根保护范围内存储路由私钥，证书无需存储保护。路由证书在节点发送 Hello 消息时广播，邻节点收到该证书后校验证书发布者签名，如果验证证书合法就将证书存储在节点内，否则直接丢弃该数据包而不做任何处理。

假定 A 节点希望建立一条由 A 到 B 的数据链路，具体步骤如下：

（1）A 广播路由请求消息 RREQ，该过程和普通的 AODV 协议类似，不过 RREQ 消息被附加 A 节点完整性报告并使用 A 的私钥签名。

（2）某一节点（这里假定为 X 节点）接收到 A 节点的 RREQ 消息后，使用接收的 A 节点在 Hello 消息中传送的公钥来验证 A 节点的 RREQ 消息是否可信。如果 X 节点没有接收到 A 节点的公钥证书，或者验证 RREQ 完整性报告时失败，则 X 节点直接丢弃 A 节点的 RREQ 消息。若 X 节点验证 RREQ 消息成功则对 A 节点发送的 RREQ 消息处理。如果 RREQ 消息的目的地址不是节点 X 并且在 X 节点的路由缓存表中没有保存到目的节点 B 的路由，则节点 X 将向前传送 RREQ。节点 X 首先将 A 节点的签名剔除，取而代之的是其自身完整性报告和签名，并且节点 X 增加一项向前的路由表指向 A。如果节点 X 就是目的节点或者在节点 X 的路由缓存表中保存有到目的节点的路由，它将生成一个

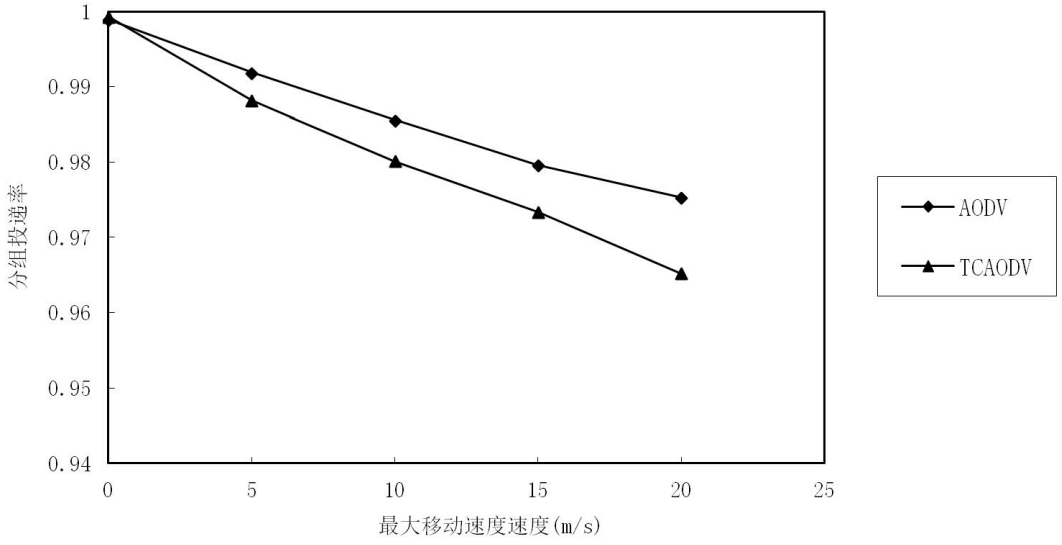

图 1：无恶意节点分组投递率

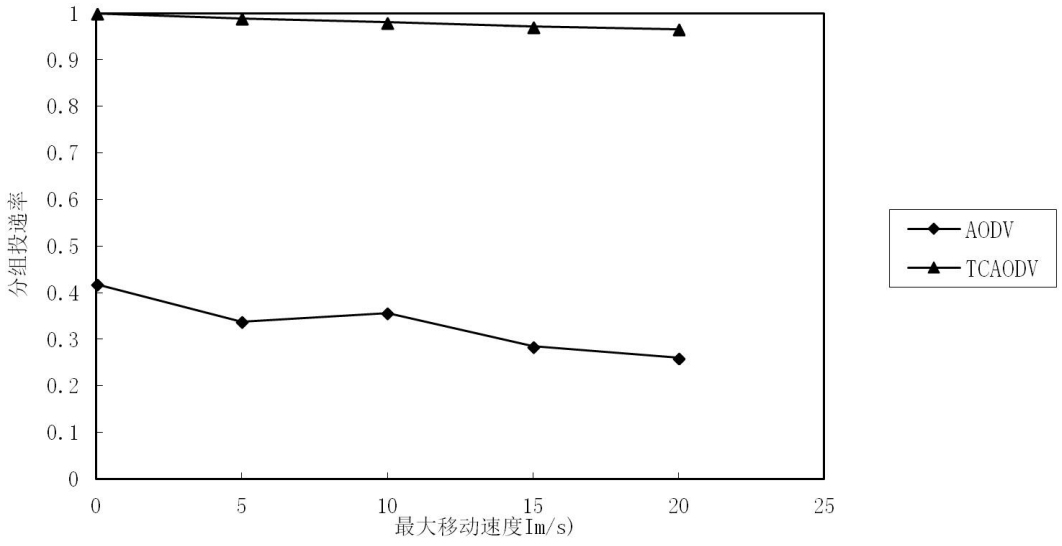

图 2：包含 1 个黑洞节点分组投递率

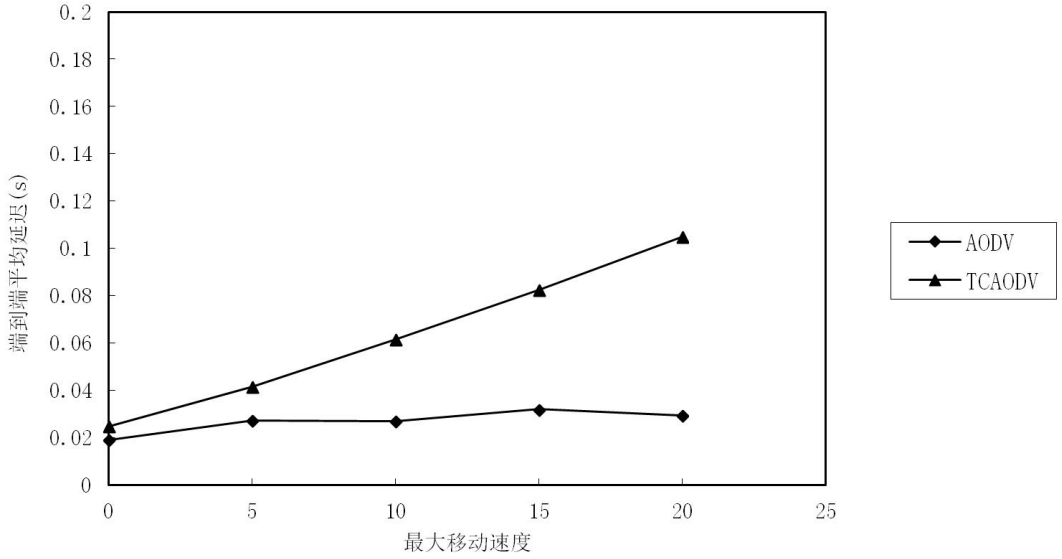

图 3：无恶意节点端到端平均延迟

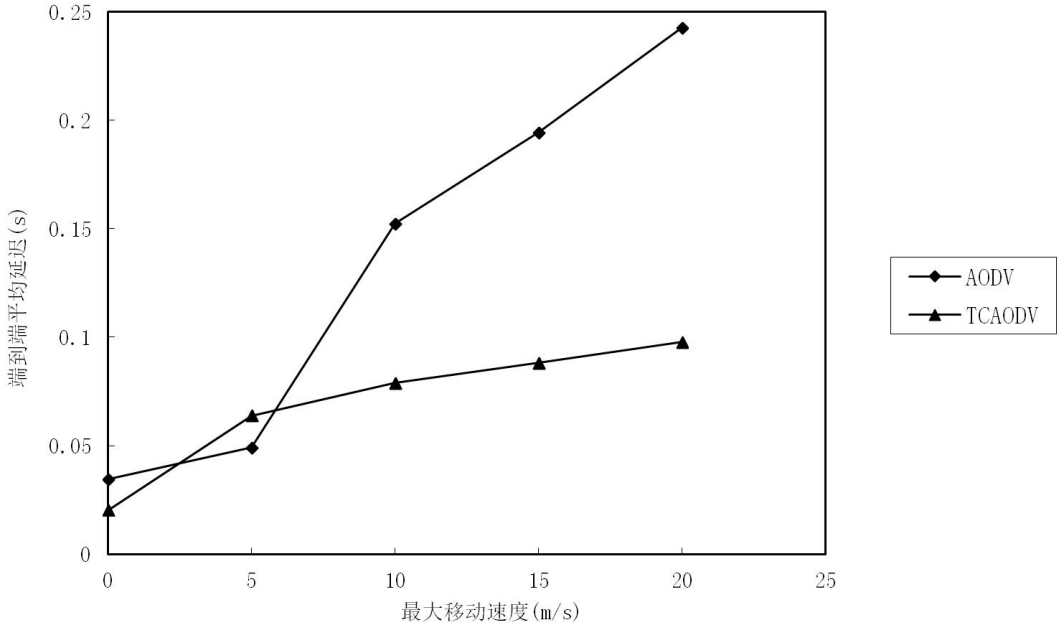

图 4：包含 1 个黑洞节点端到端平均延迟

RREP 消息，并沿着已建立的路由反方向单播传递给节点 A。这个过程同标准 AODV 协议类似，所不同的是 RREP 消息也被签名。这样在建立路由中的每一节点都要校验上一节点的完整性签名，这样就保证路由中每一节点都是可信的。每一合法的 RREP 消息被接受后都说明了建立了一条由可信节点组成的由源节点到目的节点的路由。

然而这还不能保证这些在路由建立状态下可信的节点在接下来参与通讯的过程中仍然保持正常的行为。一个不可信的设备能够在路由一旦建立后广播消息使得通讯阻塞，不可信的节点也能很容易模拟其他节点的参与通讯。为了防止这种情况的产生，一个对称的路由密钥 RK（Route Key）将在节点通讯时使用，保证只有可信的且在路由链上节点才能参与通讯。这个处理过程的也就是要让一个路由节点被其他路由节点信任（也就是说一个路由节点中的签名校验信息能被其他节点验证）其将 RK 进行了保护，使得该路由节点的 RK 不被其他进程读取不暴露在其他任意外部代码中。

（3）为了实现这一点，当节点 A 接收到 RREP 消息后或者在由 A 到 B 节点路由发生改变后，A 节点都要沿路由方向发送 RK。首先，A 随机产生一个对称密钥加上路由身份信息和时间戳，并用下一跳的公钥进行加密。路由表上的下一跳使用私钥对发来的消息解密，并将得到的对称密钥 RK 保护存储在对应的路由表中。然后使用下一跳的公钥重新加密收到的消息，沿着路由方向一步步的传送至节点 B。当节点 B 接收到由 A 传送而来的 RK 后，一条受到 RK 保护的路由最终完成。

所有在该路由上传送的数据都被该路由的 RK 加密，这些信息包括所有数据链路层数据但不包含路由 ID。每当一个节点接收到向前传送的数据，它首先查找路由 ID，如果

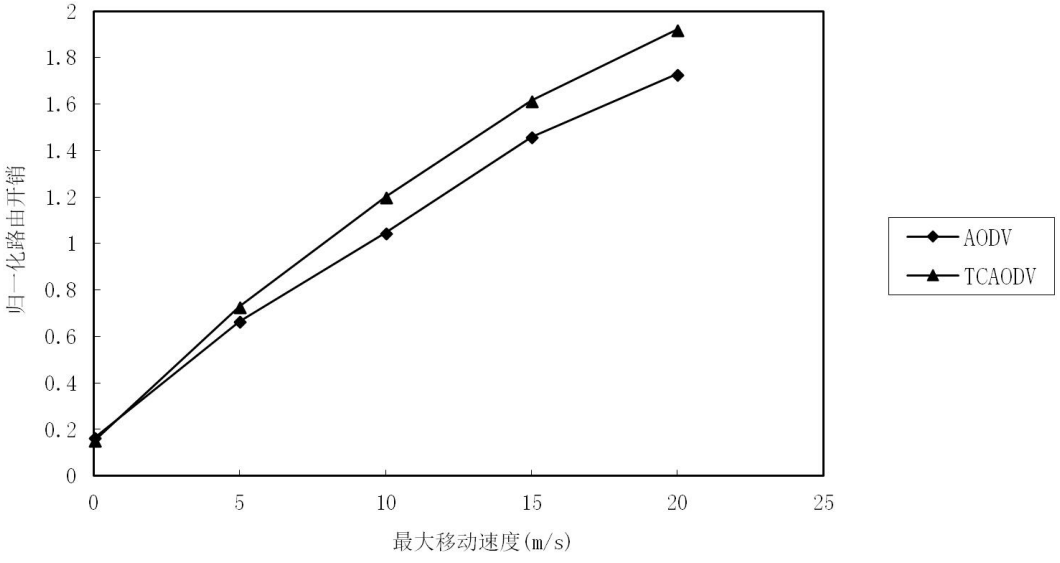

图 5：无恶意节点归一化路由开销

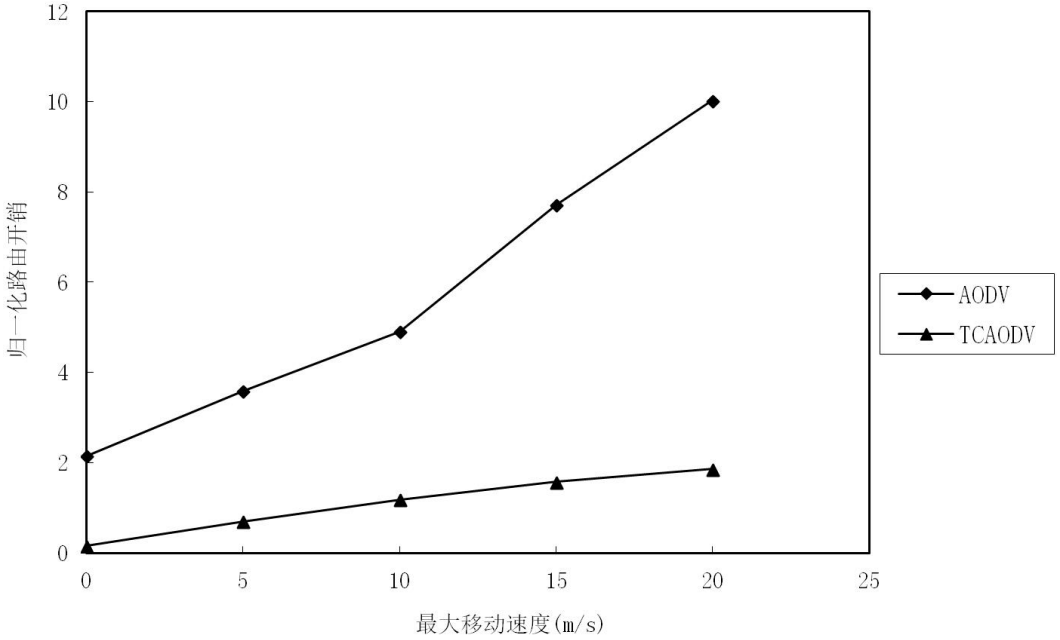

图 6：包含 1 个黑洞节点归一化路由开销

存在该 ID 的 RK，使用 RK 对该消息解密并校验消息头。如果消息头合法，则该消息被继续向前传送。如果校验消息头失败，或者路由 ID 不在该节点路由表中，则该消息被丢弃。

路由错误仍然由路由消息 RERR 标明，并且 RRER 消息也被 RK 进行加密后在整个路由上传送。如果某一节点接收到了合法 RERR 消息后将按上面所述的过程重新发现路由，但是在可能的条件下它将尝试重新使用 RK 和路由 ID。如果重新使用 RK，节点仍然需要沿着路由方向重新传送 RK，使得新加入的节点能够知道 RK 和路由 ID。

由于 RK 被保护存储在链路的各节点上，除路由协议外其他任何程序或进程无法读取 RK，保证了在整个通讯过程中只有可信的节点才能参与。

1.2 TCAODV路由协议安全性

TCAODV 路由协议和其他安全协议的对比：下面将列出几种常见的路由应具备的属性。

（1）路由参与，节点必须积极的参与路由过程。

（2）路由忠诚，节点必须能报告自己的可信性，提供正确的身份标识，如实的报告链接错误。

（3）传送职责：节点必须按路由协议的要求转发其他节点的数据。

（4）带宽控制：节点不容许超过预设带宽的传送数据。

（5）加密传送：节点必须保护传送内容和数据包头不被偷听。

（6）身份认证：节点不能假装成网络中的其他节点。TCAODV 路由协议与其他安全协议安全性对比如表 1 所示。

1.3 TCAODV协议的附加开销

1.3.1 TCAODV 协议数据处理额外开销

在发现路由阶段，TCAODV 路由协议在每次发送或转发 RREQ 和 RREP 消息时必须进行签名操作，而在接收到 RREQ 和 RREP 消息后必须进行验证操作。要让路由共享 RK，则必须在沿路由方向上的每一节点进行一次基于公钥体系的加密、解密操作。

在路由建立后，要使用路由传送数据时，路由中的源节点要使用对称密钥 RK 发送的数据加密，在目的节点使用 RK 对接收的数据解密。路由中的其他节点也要使用 RK 对接收数据解密，并验证数据包的合法性，然后用 RK 加密数据继续传送。

考虑到在基于无线自组网体系结构中，要保证路由和传送数据的安全性，必定要使用加密、解密操作，而且在可信计算架构中使用 TPM 来对数据进行加密、解密（签名、认证）操作。因为使用硬件来进行该类操作，所以造成的处理延迟较低。

1.3.2 TCAODV 协议数据传送额外开销

在发现路由阶段，因为每一 RREQ 和 RREP 消息都被签名，所以传送的数据包将会增大。考虑到 TCG 建议使用不少于 1024bit 的密钥，TCAODV 使用 1028bit 密钥，完整性报告 512 比特，附加的数据为 1536bit。

在数据传输阶段，由于使用对称密钥加密，不会增加数据传送量。

2 TCAODV协议仿真测试

2.1 仿真场景设置

为有效评估 TCAODV 性能，使用 ns2 仿真软件进行测试。仿真场景的设置主要包括节点运动场景设置和网络流量场景设置。

在本次仿真实验中参数设置如表 2 和表 3 所示。

为了对比 ADOV 协议和经过改进的 TCAODV 协议之间的性能区别，特别是在包含恶意节点时的区别，在仿真场景设置上定义如下两个场景：

（1）无恶意节点：网络全部由可信节点组成（50 个节点全部可信）。

（2）包含 1 个黑洞节点：网络由 49 个可信节点，1 个黑洞节点组成。

2.2 仿真测试及分析

仿真测试从分组投递率、端到端平均延迟、归一化路由开销几个方面对 AODV 和 TCAODV 协议性能进行对比。

由图 1 可知在无恶意节点场景中，在低速情况下 TCAODV 同 AODV 协议分组投递率类似，但是随着移动速度加快 TCAODV 分组投递率下降比 AODV 协议的要严重。

由图 2 可知在包含一个黑洞节点场景中，不论是在低速还是高速情况下 TCAODV 协议分组投递率都比 AODV 协议的要高很多。

由图 3 可知在无恶意节点场景中，在低速情况下 TCAODV 同 AODV 协议端到端平均延迟类似，但是随着移动速度加快 TCAODV 端到端平均延迟增加比 AODV 协议的要快。

由图 4 可知在包含一个黑洞节点场景中，在低速情况下 TCAODV 和 AODV 协议端到端平均延迟类似，在高速环境下 TCAODV 比 AODV 协议端到端平均延迟要小得多。

由图 5 可知在无恶意节点场景中，在低速情况下 TCAODV 同 AODV 协议归一化路由开销类似，但是随着移动速度加快 TCAODV 路由发起频率增高比 AODV 协议的要稍严重。

由图 6 可知在有一个黑洞节点的场景中，无论是低速还是高速情况 TCAODV 都比 AODV 协议的归一化路由开销要小很多。

3 结论

随着便携产品的不断发展，移动无线设备迅速流行，通过自组网网连接这些设备的需求也随之增长，自组网本身的安全问题也更加突出。可信计算技术的发展为无线自组网安全保护提供了新的途径。利用可信计算保护无线自组网路由的安全，可以在较低的代价下提供各种安全挑战的防护。通过对 AODV 协议进行扩展，加入身份认证、状态报告及密钥存储保护，实现了 TCAODV 协议。该路由协议不仅能防止恶意节点的攻击，而且能防止自私节点拒绝参与路由。通过仿真测试，说明在有恶意节点环境中 TCAODV 能提供比 AODV 更高的性能与可靠性。

参考文献

[1] 郑相全等 . 无线自组网技术实用教程 [M]. 清华大学出版社 , 2004: 7-10.
[2] Ad hoc On-Demand Distance Vector (AODV) Routing [M]. IETF RFC3651, 2003.
[3] S. Yi, P. Naldurg, R. Kravets. Security-aware ad-hoc routing for wireless networks[c]. In proc 2nd ACM Intl Symp on Mobile ad hoc networking &computing. 2001.
[4] Davide Cerri, Alessandro Ghioni, Francesco Dolcini. The A-SAODV adaptive secure routing protocol prototype. [R] MobiHoc 2006.
[5] S. Buchegger, J. Y. L. Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in dynamic ad-hoc networks[C]. In proc. 3rd IEEE/ACM Intl. Symp. Mobile Ad hoc Networking&Computing(MobiHoc). IEEE 2002
[6] S. Sundaramurthy, E. M. Belding-Royer. The ad-mix protocol for encouraging participating in mobile ad hoc networks[c]. 11th IEEE Intl. Conf. Network Protocols. 2003.
[7] Trusted Platform Module Library. Trusted Computing Group [C], Aug 2019.

作者简介

董文华，男，硕士学位，高级工程师，现为湖北广播电视台播控中心动力部高级主管。研究方向为供电安全，网络安全。