Malicious nodes seriously affect the performance of mobile ad hoc networks

Fanzhi Li and Sabah Jassim

Packet delivery ratios in wireless ad hoc networks deteriorate significantly with the presence of malicious nodes.

Wireless ad hoc networks are rapidly gaining popularity as a mode of communication, especially among highly mobile sectors of society. A mobile ad hoc network (MANET) is formed with wireless mobile devices (nodes) without the need for existing network infrastructure. As a result, such networks are relatively easy to deploy and use for a very short time, for example, in both personal and business applications.

In addition to providing a convenient mode of communication for civilian and business purposes, wireless ad hoc networks are highly desirable for use in war zones, relief efforts in remote territories, and emergency situations in disaster-stricken areas. In such cases, where no network infrastructure exists, a mobile ad hoc network can provide a crucial mode of communication.

Mobile devices in ad hoc networks communicate with each other through a multi-hop route, using cooperating intermediary nodes. A high level of cooperation is essential for applications that require real-time data transmission, such as soldiers relaying information in a battlefield. However, the limited energy supply of mobile devices raises doubts about the ability of every node to be fully cooperative. As a result, packet delivery cannot be guaranteed even when malicious nodes are not present, and resending data packets does not provide a good solution.

If malicious nodes are present in a MANET, they may attempt to reduce network connectivity (and thereby undermine the network’s security) by pretending to be cooperative but in effect dropping any data they are meant to pass on. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance. We aim to evaluate the added effect of the presence of malicious nodes on ad hoc network performance, and determine appropriate measures to detect malicious nodes.

Instead of creating ad hoc networks with hundreds of physical mobile wireless devices and incurring significant costs, we used the Java in Simulation Time/Scalable Wireless Ad hoc Network Simulator (JiST/SWANS). The simulation experiments examined various network conditions, including node density, mobility speed, transmission power, and geographical distribution of devices. The simulation results demonstrate that the presence of only one malicious node in a MANET can cause an added packet loss of more than 25%. With multiple rogue dropers, nearly 60% of data packets could be lost. In such cases, the presence of malicious nodes have serious security implications.

Standard security solutions adopted for wired networks or structured wireless networks—networks with backbone nodes providing access via physical networks—do not extend naturally to ad hoc networks. Security methods such as public key infrastructure (PKI) and certification typically require a central infrastructure within the network, making them unusable in a MANET. However, the emergence of biometric-based user authentication for mobile devices motivates our investigation of the possible use of biometrics as a security measure for ad hoc networks. In some sensitive applications of MANETs—for example, in battlefields—biometrics could provide a crucial measure of security.

To test the viability of such a solution, we needed to assess the impact of packet dropping on biometric schemes. We tested the robustness of a face verification scheme, developed at Buckingham University, against packet dropping. Our experiments showed that there is no noticeable deterioration in the accuracy of the adopted face verification method, even when most of the biometric data is lost or dropped during transmission. This may initially appear to reflect only the robustness of the adopted biometric scheme, but it nevertheless demonstrates the viability of such schemes in securing sensitive ad hoc networks. These results also encourage the use of biometrics as part of the certification component for deployment in ad hoc wireless networks.

Continued on next page
In MANET applications where authentication is not essential, there is still a need for mechanisms whereby nodes can be assured that packets will be delivered to their intended destination. To address this need, we are currently investigating the use of ‘creditability-based’ routing tables to detect and isolate malicious nodes. In such a scheme, a node monitors its neighbors and assigns ‘credit scores’ to them according to their observed behavior and ‘credit history.’ Maintaining such a table at each node facilitates the choice of trusted routes rather than the shortest ones, potentially mitigating the packet losses caused by malicious nodes, even when authentication is not used. We are currently implementing this mechanism within the simulation system.

This work was supported in part by the EU FP6 IST contract 001930 (BROADWAN).

Author Information

Fanzhi Li and Sabah Jassim
Department of Applied Computing
University of Buckingham
Buckingham, UK

Fanzhi Li received his first degree, in thermal engineering, from Xi’an Jiaotong University in China, and an MSc in computing from the University of Buckingham in 2004. He is presently a PhD candidate at the University of Buckingham, investigating how to detect and isolate malicious nodes in wireless networks.

References