

# **Encyclopedia of Information Science and Technology**

**Second Edition**

Mehdi Khosrow-Pour

*Information Resources Management Association, USA*

**Volume V  
Intero-Mo**

**Information Science  
REFERENCE**

**INFORMATION SCIENCE REFERENCE**

Hershey • New York

Director of Editorial Content: Kristin Klinger  
Director of Production: Jennifer Neidig  
Managing Editor: Jamie Snavely  
Assistant Managing Editor: Carole Coulson  
Cover Design: Lisa Tosheff  
Printed at: Yurchak Printing Inc.

Published in the United States of America by  
Information Science Reference (an imprint of IGI Global)  
701 E. Chocolate Avenue, Suite 200  
Hershey PA 17033  
Tel: 717-533-8845  
Fax: 717-533-8661  
E-mail: [cust@igi-global.com](mailto:cust@igi-global.com)  
Web site: <http://www.igi-global.com/reference>

and in the United Kingdom by  
Information Science Reference (an imprint of IGI Global)  
3 Henrietta Street  
Covent Garden  
London WC2E 8LU  
Tel: 44 20 7240 0856  
Fax: 44 20 7379 0609  
Web site: <http://www.eurospanbookstore.com>

Copyright © 2009 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Encyclopedia of information science and technology / Mehdi Khosrow-Pour, editor. -- 2nd ed.

p. cm.

Includes bibliographical references and index.

Summary: "This set of books represents a detailed compendium of authoritative, research-based entries that define the contemporary state of knowledge on technology"--Provided by publisher.

ISBN 978-1-60566-026-4 (hardcover) -- ISBN 978-1-60566-027-1 (ebook)

1. Information science--Encyclopedias. 2. Information technology--Encyclopedias. I. Khosrowpour, Mehdi, 1951-Z1006.E566 2008  
004'.03--dc22

2008029068

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this encyclopedia set is original material. The views expressed in this encyclopedia set are those of the authors, but not necessarily of the publisher.

*Note to Librarians: If your institution has purchased a print edition of this publication, please go to <http://www.igi-global.com/agreement> for information on activating the library's complimentary online access.*

# Mobile Ad Hoc Network Security Vulnerabilities

**M****Animesh K. Trivedi***Indian Institute of Information Technology, India***Rajan Arora***Indian Institute of Information Technology, India***Rishi Kapoor***Indian Institute of Information Technology, India***Sudip Sanyal***Indian Institute of Information Technology, India***Ajith Abraham***Norwegian University of Science and Technology, Norway***Sugata Sanyal***Tata Institute of Fundamental Research, India*

## INTRODUCTION

Mobile ad hoc networks inherently have very different properties from conventional networks. A mobile ad hoc network (MANET) is a collection of mobile nodes that are self configuring (network can be run solely by the operation of the end-users), capable of communicating with each other, establishing and maintaining connections as needed. Nodes in MANET are both routers and terminals. These networks are dynamic in the sense that each node is free to join and leave the network in a nondeterministic way. These networks do not have a clearly defined physical boundary, and therefore, have no specific entry or exit point. Although MANET is a very promising technology, challenges are slowing its development and deployment. Nodes in ad hoc networks are in general limited in battery power, CPU and capacity. Hence, the transmission ranges of these devices are also limited and nodes have to rely on the neighboring nodes in the network to route the packet to its destination node. Ad hoc networks are sometimes referred to as multi-hop networks, where a hop is a direct link between two nodes.

MANET has many important applications, including battlefield operations, emergency rescues, mobile conferencing, home and community networking, sensor dust and so forth.

Due to limited memory and computational power, nodes in MANETs have limited services and security provision. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have characteristics such as dynamically changing topology, weak

physical protection of nodes, no established infrastructure or centralized administration and high dependence on inherent node cooperation. The routing protocols used in the current generation of mobile ad hoc networks, like Dynamic Source Routing (DSR), and Ad hoc On Demand Distance Vector Routing Protocol (AODV), are based on the principle that all nodes will cooperate, but dynamic and cooperative nature of MANETS presents substantial challenges to this assumption (Johnson, Maltz, & Broch, 2001; Perkins & Royer, 1999). Without node cooperation in a mobile ad hoc network, routes cannot be established, and packets cannot be forwarded. As a consequence, access control mechanisms, (similar to firewalls in wired networks) are not feasible. However, cooperative behavior, such as forwarding other node's messages, cannot be taken for granted because any node could misbehave. Misbehavior means deviation from regular routing and forwarding protocol assumption. It may arise for several reasons, non-intentionally when a node is faulty or intentionally when a node may want to save its resources. Cooperation in mobile ad hoc networks is a big issue of consideration. To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, the outcome is a nonfunctional network when multi-hop routes are needed, so all nodes are worse off. Without any counter policy, the effects of misbehavior have been shown to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their strategies, network throughput could decrease, and there could be packet losses, denial of

service or network portioning. These detrimental effects of misbehavior can endanger the entire network.

Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation, modification of packets and denial-of-service. Intrusion prevention measures, such as strong authentication and redundant transmission, can be used to tackle some of these attacks. However, these techniques can address only a subset of the threats, and moreover, are costly to implement due to the limited memory and computation power on nodes. We can identify two types of uncooperative nodes: faulty or malicious and selfish. Faulty or malicious behavior refers to the broad class of misbehavior in which nodes are either faulty and can therefore not follow a protocol, or are intentionally malicious and try to attack the system. Selfishness refers to no cooperation in certain network operations. In mobile ad hoc networks, the main threat from selfish nodes is dropping of packets (black hole), which may affect the performance of the network severely. Faulty, malicious and selfish nodes are misbehaved nodes.

## **ROUTING IN MANETs**

Dynamic Source Routing is a popular routing protocol for ad hoc networks and was proposed for MANET by Johnson, Maltz and Broch (2001). In DSR, nodes do not store route to different nodes but they are discovered as they are needed. This type of routing is called *Reactive* routing and protocols used in this are called *Reactive Protocols* (e.g., DSR, AODV, etc.). DSR works as follows: Nodes send out a ROUTE REQUEST (RREQ) message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY (RREP) message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. After receiving one or several routes, the source selects the best (by default the shortest) route, stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. Because route to the destination is put into the packet, it is called source routing.

## **Attacks on DSR**

There are a number of attacks possible on DSR protocol because there is no security measure and it assumes honest

coordination of nodes among them and to protocol. A few attacks are outlined in this section and others are discussed in detail in the cited references.

- Dropping of packets by a node takes into account the following scenarios-Drop all packets not destined to it or perform only partial dropping. Partial dropping can be restricted to specific types, such as only data packets, or route control packets that contain it or packets destined to specific nodes.
- Avoid sending a ROUTE ERROR when having detected an error, to prevent other nodes from looking for alternative routes.
- By sending forged routing packets, an attacker can create a so-called black hole, a node where all packets are discarded or all packets are lost.
- Attempt to make routes that go through one appear longer by adding some virtual nodes to the route. Thus, a shorter route will be chosen, avoiding this node.
- Modify the nodes list in the header of a ROUTE REQUEST or a ROUTE REPLY to misroute packets and to add incorrect routes in the route cache of other nodes.
- Decrease the hop count (TTL) when receiving a packet, so that the packet will never be received by the destination. This attack could be detected by the previous node in route by enhanced passive acknowledgment.
- Initiate frequent ROUTE REQUEST to consume bandwidth and energy and to cause congestion.
- Send route replies with a time not proportional to the length of the route. This can give more priority to long routes, thus attracting routes to the attacker, or less priority to short routes, thus avoiding the attacker.

Listed above are some frequent attacks possible on DSR operating without any security measurements.

## **INTRUSION DETECTION SYSTEMS**

Intrusion detection systems (IDS), especially those which are reputation-based, are a new paradigm and are being used for enhancing security in different areas. These systems are lightweight, easy to use and are capable to face a wide variety of attacks as long as they are observable. Among these mechanisms, some of the popular ones are CORE, CONFIDANT, OCEAN and SAFE.

## **Reputation-Based IDS**

Reputation-based IDS do not rely on the conventional use of a common secret to establish confidential and secure communication between two parties. Instead, they are simply based on each other's observations (Buchegger & Le Boudec, 2005). To be more precise, every node in the network moni-

tors the packet emission of its neighboring nodes and derives a reputation value for them. If any misbehavior is detected, this information is broadcasted to the neighboring nodes in order to help them to protect themselves against this fraud (Buchegger & Le Boudec, 2003). Different architectures using the reputation concept for securing packet forwarding have been proposed so far (Resnick & Zeckhauser, 2002). The reputation herein is simply bound to how “good routers” the nodes are. Monitoring the packet loss carried out by the neighborhood is one of the main tasks of these reputation-based systems (Marti, Giuli, & Baker, 2000). The monitoring operation was implemented in CORE and CONFIDANT using a packet overhearing technique based on the promiscuous mode.

## Issues Being Addressed

There are few basic problems in MANET that need to be kept in mind while designing any security solution. First, it is often very hard to differentiate intrusions and normal operations or conditions in MANET because of the dynamically changing topology and volatile physical environment. Second, mobile nodes are autonomous units that are capable of roaming independently in unrestricted geographical topology. This means that nodes with inadequate physical protection can be captured, compromised, or hijacked. Third, decision-making in ad hoc networks is usually decentralized and many ad hoc network algorithms rely on the cooperative participation of all nodes. Most ad hoc routing protocols are also cooperative in nature and hence can be easily misguided by false routing information (Yau & Mitchell, 2003).

It is observed that without countermeasure the effect of misbehavior dramatically decreases network performance. Intrusion prevention measures, such as authentication and encryption, can be used as the first line of defense against attacks in MANETs. However, even if these prevention schemes can be implemented perfectly, they still cannot eliminate all attacks, especially the internal or insider attacks. Also, they are costly to implement on mobile nodes from the point of view of limited computation power and energy needed. Another possible solution to this problem is similar to the concept of economic incentives, but the problem with them is that they need a centralized banking system and tamper proof hardware, and a more basic question is who will pay and how much ?

## Architecture and Working Principle of Reputation-Based IDS

*Reputation-based* systems are used for enhancing security in ad hoc networks as they model cooperation between the nodes which is inspired from our social behavior. As in our daily life, when we meet somebody for the first time, we build

a reputation about him or her from our personal (firsthand) and some body else's (secondhand) experience. Reputation-based systems are built on this principle. Such systems are used to decide who to trust, and to encourage trustworthy behavior. Resnick and Zeckhauser identify three goals for reputation systems (Resnick & Zeckhauser, 2002):

- To provide information to distinguish between a trustworthy principal and an untrustworthy principal,
- To encourage principals to act in a trustworthy manner, and
- To discourage untrustworthy principals from participating in the service the reputation mechanism is present to protect.

*Watchdog* and *Path-rater* are some essential components of any Reputation-based Intrusion detection System (Buchegger & Le Boudec, 2004). Complementing DSR with a watchdog increases throughput of mobile ad hoc networks. Misbehavior Detection and Reputation Systems may or may not be distributed. Here, fully distributed means whether information regarding one's reputation is immediately propagated in the whole network or not. In the latter case, nodes are fully dependent on their own personal view about other nodes reputation and behavior.

Distributed IDS protocols either rely only on firsthand information or on positive secondhand information. CONFIDANT and CORE fall into this category. Some basic problems with this approach of global reputation systems are:

- Every node has to maintain  $O(n)$  reputation information where  $n$  is number of nodes in network.
- Extra traffic generation in reputation exchange.
- Extra computation in accepting indirect reputation information (secondhand information), especially Bayesian Estimation.
- Security issues in reputation exchange such as reputation data packets can be modified.

**CONFIDANT**, proposed by Buchegger and Le Boudec, detects misbehaving nodes by means of observation or by ALARM signals from neighborhood (Buchegger & Le Boudec, 2002). CONFIDANT aggressively informs nodes in neighborhood about misbehavior of the malicious node. The weight-age of ALARM warning signal depends upon the level of trust that is believed by receiving node. CONFIDANT uses Bayesian Estimation for various measures and calculation of trust and reputation and thus IDS become complex. Each ad hoc running a CONFIDANT system comprises of a:

- *Monitor*, for observation purpose,
- *Reputation Manager*, for calculating reputation of other nodes,

- *Trust Manager*, for calculating level of trust to a particular node, which is used in calculating weightage of ALARM from that node, and
- *Path Manager*, for update path information in route cache as the reputation of neighborhood nodes changes. For example, Deletion of paths containing malicious node, selection of path from various available path option on particular situation and so forth.

CONFIDANT is vulnerable to false accusation if trusted nodes lie or if several liars collude.

Michiardi and Molva (2002) proposed a mechanism called CORE, to enforce node cooperation in mobile ad hoc network. In this mechanism, reputation is a measure of someone's contribution to network operations. Members that have a good reputation can use available resources while members with a bad reputation, because they refused to cooperate, are gradually excluded from the community. CORE defines three types of reputation:

1. Subjective reputation is a reputation value which is locally calculated based on direct observation.
2. Indirect reputation is secondhand reputation information which is established by other nodes.
3. Functional reputation is related to a certain function, where each function is given a weight as to its importance. For example, data packet forwarding may be deemed to be more important than forwarding packets with route information, so data packet forwarding will be given greater weight in the reputation calculations.

CORE reputation values range from positive (+1), through null (0), to negative (-1). CORE suffers from the problem of unwanted consequence of good reputation, where a good node may even wish to decrease its reputation by behaving badly to prevent its resources from being overused. The CORE mechanism assumes that every node will use the same reputation calculations and will also assign the same weights to the same functions. This is a potentially inappropriate assumption in heterogeneous ad hoc networks, where devices with different capabilities and roles are likely to place different levels of importance on different functions depending upon CPU usage, battery usage and so forth. One can take advantage of this situation and may perform only those functions which have higher preferences in calculating reputation.

A second type of IDS is one that solely depends upon the firsthand observation for reputation maintenance. Nodes make routing decision based on only the direct observation of its neighbor's node. This eliminates most of the trust manager complexity but in highly mobile ad hoc network it might not be appropriate to only depend solely upon personal observation. But also using secondhand information can sig-

nificantly accelerate the detection and subsequent isolation of malicious nodes in mobile ad hoc networks.

**OCEAN** by Bansal and Baker relies exclusively on firsthand observations for ratings and avoids indirect (secondhand) reputation information. In OCEAN, the rating of each node is initialized to Neutral (0), with every positive action resulting in an increment (+1) of the rating, and every negative action resulting in a decrement (-2) of the rating (Bansal & Baker, 2003). Once the rating of a node falls below a certain faulty threshold (-40), the node is added to a faulty list. The faulty list represents a list of misbehaving nodes. If the rating is below the faulty threshold, the node is added to the faulty list. This faulty list is appended to the route request by each node broadcasting it to be used as an avoid list. A route is rated good or bad depending on whether the next hop is on the faulty list. In addition to the rating, nodes keep track of the forwarding balance with their neighbors by maintaining a chip count for each node.

OCEAN's approach is to disallow any secondhand reputation exchanges. Routing decisions are made based solely on direct observations of neighboring nodes behavior. This eliminates most trust management complexity. The basic problem with OCEAN is that it does not take secondhand information that can significantly improve detection of malicious nodes. Also, authors only consider individual bad behavior, not collusion of nodes.

## CONCLUSION

Mobile ad hoc networks have a number of significant security issues which cannot be solved alone by Intrusion detection systems. Physical security of nodes is another very important issue. Reputation systems are used to establish trust and encourage trustworthy behavior and cooperation among nodes. In this article, we have critically examined the existing systems and outlined their strength and shortcomings.

## REFERENCES

- Bansal, S., & Baker, M. (2003). *Observation-based cooperation enforcement in ad hoc networks*. Retrieved December 10, 2007, from <http://arxiv.org/pdf/cs.NI/0307012>
- Buchegger, S., & Le Boudec, J.Y. (2002). Performance analysis of the CONFIDANT Protocol: Cooperation of nodes—fairness in dynamic ad hoc networks. In *Proceedings of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, (pp. 226-236).
- Buchegger, S., & Le Boudec, J.Y. (2003). The effect of rumor spreading in reputation systems for mobile ad hoc

nets. In *Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Sophia-Antipolis, France.

Buchegger, C.T., & Le Boudec, J.Y. (2004). A test-bed for misbehavior detection in mobile ad hoc networks—how much can watchdogs really do? In *WMCSA: Proceedings of the Sixth IEEE Workshop on Mobile Computing Systems and Applications*.

Buchegger, S., & Le Boudec, J.Y. (2005). Self-policing mobile ad hoc networks by reputation systems. *IEEE Communications Magazine*.

Johnson, D.B., Maltz, D.A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In C.E. Perkins (Ed.), *Ad Hoc Networking* (pp. 139-172). Addison-Wesley.

Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking Table of Contents*, (pp. 255–265).

Michiardi, P., & Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP Communication and Multimedia Security Conference*.

Perkins, C.E., & Royer, E.M. (1999). Ad hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, (pp. 90-100).

Resnick, P., & Zeckhauser, R. (2002). Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In M. R. Baye (Ed.), *The economics of the Internet and e-commerce: Advances in applied microeconomics* (Vol. 11, pp. 127-157). Amsterdam, Elsevier Science.

Yau, P., & Mitchell, C.J. (2003). Reputation methods for routing security for mobile ad hoc networks. In *Proceedings of SympoTIC '03, Joint IST Workshop on Mobile Future and Symposium on Trends in Communications*, Bratislava, Slovakia.

## KEY TERMS

**Ad Hoc Network:** A mobile ad hoc network (MANET) is a kind of wireless ad hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology.

**Bandwidth:** Bandwidth is a measure of frequency range and is typically measured in hertz. Bandwidth is related to channel capacity for information transmission.

**Denial of Service (DoS):** Is an attempt to make a computer resource unavailable to its intended users. Typically, the targets are high-profile Web servers where the attack is aiming to cause the hosted Web pages to be unavailable on the Internet. It is a computer crime that violates the Internet proper use policy as indicated by the Internet Architecture Board (IAB).

**Firewalls:** A logical barrier designed to prevent unauthorized or unwanted communications between sections of a computer network.

**Gateway:** A computer or a network that allows or controls access to another computer or network.

**Intrusion Detection System (IDS):** Is used to detect many types of malicious network traffic and computer usage that can't be detected by a conventional firewall.

**Promiscuous Mode:** Refers to a configuration of a network interface wherein a setting is enabled so that the interface passes all traffic it receives to the CPU rather than just packets addressed to it, a feature normally used for packet sniffing.

**Routers:** A router acts as a junction between two or more networks to transfer data packets among them.

**Reputation:** As a socially transmitted belief (i.e., belief about belief) concerns properties of agents, namely their attitudes toward some socially desirable behavior, be it cooperation, reciprocity, or norm-compliance.

**Terminal:** In the context of telecommunications, a terminal is a device which is capable of communicating over a line.