IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Securing Route Discovery in MANETs: Analysis and Improvement

Surya Kiran Suhag[1], Dr. Paramjit Singh[2]

[1]M.Tech Scholar, P.D.M. College of Engineering, M.D.U, Rohtak, India

[2]Director and Professor, P.D.M. College of Engineering, M.D.U, Rohtak, India

Abstract
In this paper, we show that the security proof for the route discovery algorithm end air A is flawed, and moreover, this algorithm is vulnerable to a hidden channel attack. We also analyze the security framework that was used for route discovery and argue that compos ability is an essential feature for ubiquitous applications. We conclude by discussing some of the major security challenges for route discovery in MANETs.

Keywords: *MANET, Route Discovery, Data discovery.*

I. INTRODUCTION

In a multihop wireless ad hoc network, mobile nodes cooperate to form a network without using any infrastructure such as access points or base stations. Instead, the mobile nodes forward packets for each other, allowing communication among nodes outside wireless transmission range. The nodes' mobility and the fundamentally limited capacity of the wireless medium, together with wireless transmission effects such as attenuation, multipath propagation, and interference, combine to create significant challenges for routing protocols operating in an ad hoc network.

Mobile ad hoc networks (MANETs) are dynamic collections of autonomous mobile nodes with links that are changing in an unpredictable way. They are characterized by a dynamic topology and the lack of any fixed infrastructure. The communication medium is broadcast. The nodes can be regarded as wireless mobile hosts with limited power (operating off batteries), constrained bandwidth and transmission range (typically 250–1000 meters in an open field). The recent rise in popularity of mobile wireless devices and technological developments has made possible the deployment of such networks for several applications. Indeed, because ad hoc networks do not have any fixed infrastructure such as stations or routers, they are highly applicable for emergency deployments, disasters, search and rescue missions and military operations. Finding and maintaining routes in a MANET is a major challenge. So far, most of the research has focused on functionality issues and efficiency with security being given a lower priority, and in many cases, regarded as an add-on afterthought technology rather than a design feature. Although such an approach may be suitable for networks with predictable faults, it not suitable for MANETs in which we have unpredictable or malicious faults. Of particular concern is the possibility that an established route is under the control of a malicious adversary, and will be disconnected at a critical time when damage is maximized, and when there is not sufficient time to fix the route or to find alternative routes. In such cases multipath routing is of benefit. Multipath routing involves the establishment of multiple paths between source and destination pairs. These paths are used for replicated (or redundant) communication to prevent Byzantine attacks. Routing is a basic functionality for multihop mobile ad hoc networks (MANETs). These networks are decentralized, with nodes acting both as hosts and as routers, forwarding packets for nodes that are not in transmission range of each other. Several route discovery algorithms have been proposed in the literature. These focus mainly on efficiency issues such as scalability with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements. Some of the proposed routing algorithms also address security issues but their security is restricted to rather weak adversary models. There are several reasons for this, the most important one being that it is hard to model a formal security framework that captures all the basic security aspects of a MANET.

2. SCOPE OF STUDY

PROPOSED SYSTEM:

Our main contribution in this paper is to show that the security proof for endairA is flawed and that this routing algorithm is similarly subject to a hidden channel attack.

Revisiting the ABV model, we present several reasons why we think that concurrent security for MANET route discovery is essential. The ABV model's security standard is insufficient in practice, because it requires the absence of channels that are always present in any real world MANET application. We then argue that a higher security standard namely composability is a fundamental requirement for ubiquitous applications. Subsequently, we make some observations about issues that have to be addressed by any routing protocol that achieves security in a composable model.

MODULES:

1. Secure Route Discovery
2. Route Activation
3. Multicast Tree Maintenance
4. Data Forwarding

MODULES DESCRIPTION:

SECURE ROUTE DISCOVERY

The protocol follows the RREQ/RREP procedure used by on-demand routing protocols, with several differences. To prevent outsiders from interfering, all route discovery messages are authenticated. Only authenticated nodes can initiate RREQs, and the group authenticated is required in each request. Tree nodes use the tree token to prove their tree status.

ROUTE ACTIVATION

The requester signs and unicasts on the selected route a multicast activation (MACT) message that includes its identifier, the group identifier, and the sequence number used in the RREQ phase. The MACT message also includes a one-way function applied on the tree token extracted from RREP which will be checked by the tree node that sent the RREP message to verify that the node that activated the route is the same as the initial requester. An intermediate node on the route checks if the signature on MACT is valid and if MACT contains the same sequence number as the one in the original RREQ. The node then adds to its list of tree neighbors the previous node and the next node on the route as downstream and upstream neighbors, respectively, and sends MACT along the forward route.

MULTICAST TREE MAINTENANCE

The network periodically broadcasts in the entire network a signed GroupHello message that contains the current group sequence number, the tree token authenticator, and the hop count anchor. A signed GroupHello message containing a special flag also ensures that when two disconnected trees are merging, one of the group leaders is suppressed.

DATA FORWARDING

The source periodically sends in the tree a request message that contains its data transmission rate. As this message propagates in the multicast tree, nodes may add their perceived transmission rate to it. Each tree node keeps a copy of the last heard packet. The information in the message allows nodes to detect if tree ancestors perform selective data forwarding attacks. Depending on whether their perceived rate is within acceptable limits of the rate in the message, nodes alternate between two states. The initial state of a node is disconnected; after it joins the multicast group and becomes aware of its expected receiving data rate, the node switches to the connected state. Upon detecting a selective data forwarding attack, the node switches back to the disconnected state.

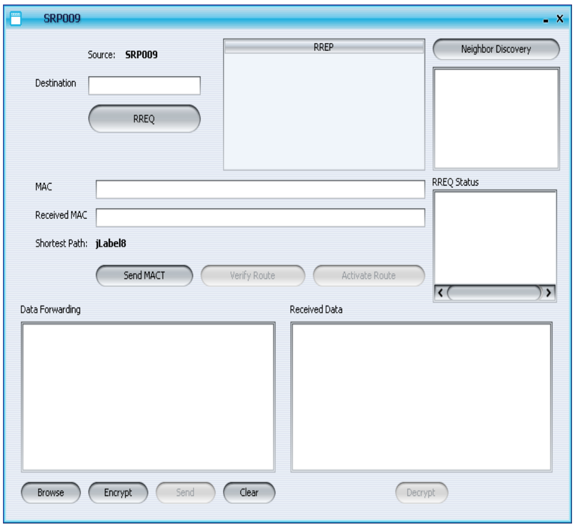
3. EXISTING SYSTEM

These focus mainly on efficiency issues such as scalability with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements. Some of the proposed routing algorithms also address security issues for a survey, but their security is restricted to rather weak adversary models. There are several reasons for this, the most important one being that it is hard to model a formal security framework that captures all the basic security aspects of a MANET.

4. EXPERIMENTAL RESULTS

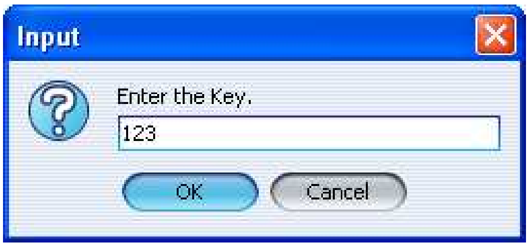
Snapshots Shown on next Page

IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com



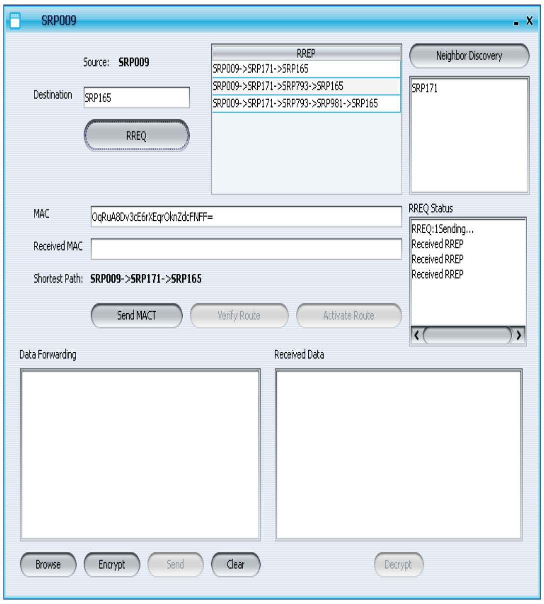
Source: SRP009

Shortest Path: jLabel8



Enter the Key.

123



Source: SRP009

Destination: SRP165

RREP:
SRP009->SRP171->SRP165
SRP009->SRP171->SRP793->SRP165
SRP009->SRP171->SRP793->SRP981->SRP165

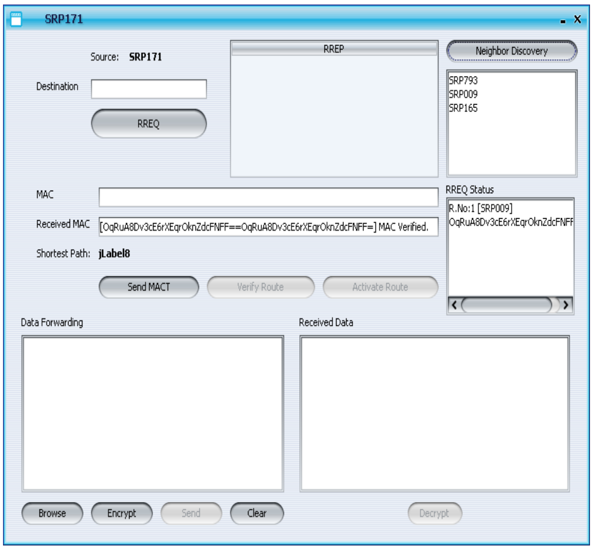
Neighbor Discovery: SRP171

MAC: OqRuA8Dv3cE6rXEqrOknZdcFNFF=

Shortest Path: SRP009->SRP171->SRP165

RREQ Status:
RREQ:1Sending...
Received RREP
Received RREP
Received RREP

In Neighbor Node:



Source: SRP171

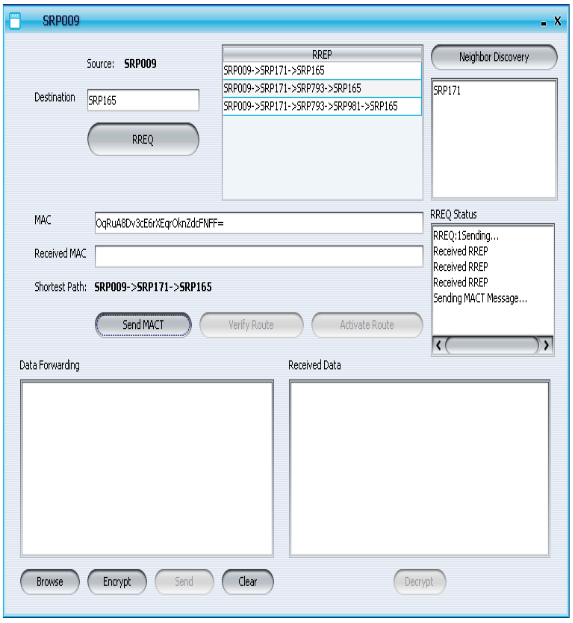
Neighbor Discovery:
SRP793
SRP009
SRP165

Received MAC: [OqRuA8Dv3cE6rXEqrOknZdcFNFF==OqRuA8Dv3cE6rXEqrOknZdcFNFF=] MAC Verified.

Shortest Path: jLabel8

RREQ Status:
R.No:1 [SRP009]
OqRuA8Dv3cE6rXEqrOknZdcFNFF

In Destination:



Source: SRP009

Destination: SRP165

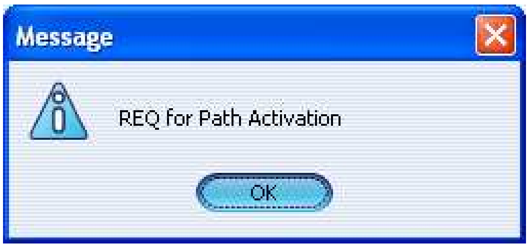
RREP:
SRP009->SRP171->SRP165
SRP009->SRP171->SRP793->SRP165
SRP009->SRP171->SRP793->SRP981->SRP165

Neighbor Discovery: SRP171

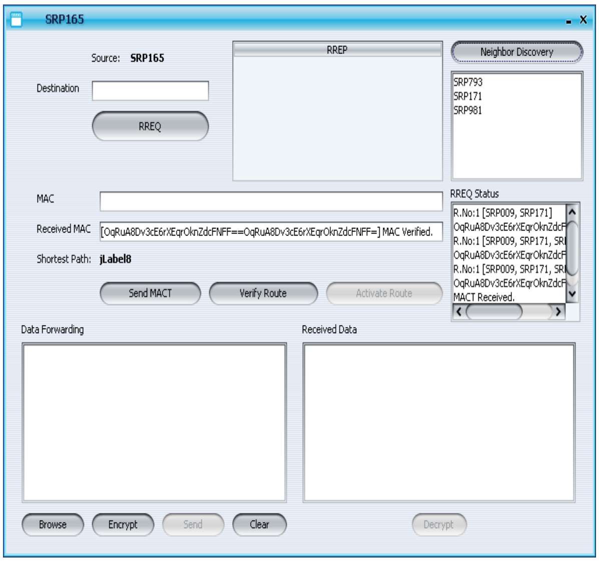
MAC: OqRuA8Dv3cE6rXEqrOknZdcFNFF=

Shortest Path: SRP009->SRP171->SRP165

RREQ Status:
RREQ:1Sending...
Received RREP
Received RREP
Received RREP
Sending MACT Message...



REQ for Path Activation



Source: SRP165

Destination

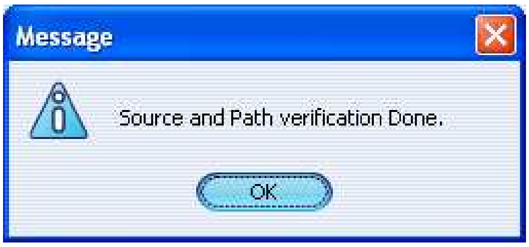
SRP793
SRP171
SRP981

MAC

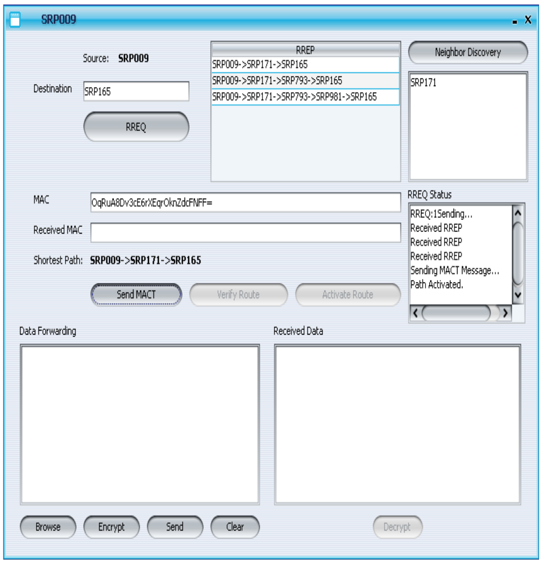
Received MAC [OqRuA8Dv3cE6rXEqrOknZdcFNFF==OqRuA8Dv3cE6rXEqrOknZdcFNFF=] MAC Verified.

Shortest Path: jLabel8

R.No:1 [SRP009, SRP171]
OqRuA8Dv3cE6rXEqrOknZdcF
R.No:1 [SRP009, SRP171, SR
OqRuA8Dv3cE6rXEqrOknZdcF
R.No:1 [SRP009, SRP171, SR
OqRuA8Dv3cE6rXEqrOknZdcF
MACT Received.



Source and Path verification Done.



Source: SRP009

Destination SRP165

SRP009->SRP171->SRP165
SRP009->SRP171->SRP793->SRP165
SRP009->SRP171->SRP793->SRP981->SRP165

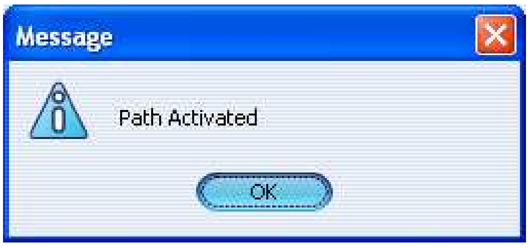
SRP171

MAC OqRuA8Dv3cE6rXEqrOknZdcFNFF=

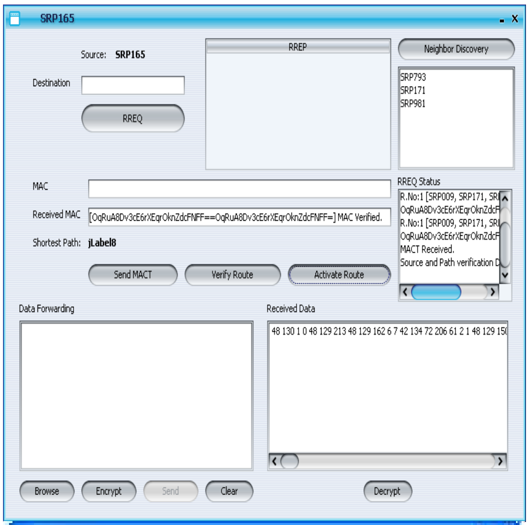
Received MAC

Shortest Path: SRP009->SRP171->SRP165

RREQ:1Sending...
Received RREP
Received RREP
Received RREP
Sending MACT Message...
Path Activated.



Path Activated



Source: SRP165

Destination

SRP793
SRP171
SRP981

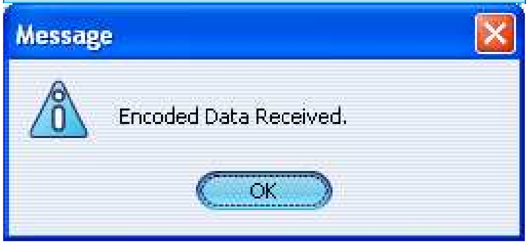
MAC

Received MAC [OqRuA8Dv3cE6rXEqrOknZdcFNFF==OqRuA8Dv3cE6rXEqrOknZdcFNFF=] MAC Verified.

Shortest Path: jLabel8

R.No:1 [SRP009, SRP171, SR
OqRuA8Dv3cE6rXEqrOknZdcF
R.No:1 [SRP009, SRP171, SR
OqRuA8Dv3cE6rXEqrOknZdcF
MACT Received.
Source and Path verification D

48 130 1 0 48 129 213 48 129 162 6 7 42 134 72 206 61 2 1 48 129 15



Encoded Data Received.

5. CONCLUSION AND FUTURE SCOPE

In our project a new security framework tailored for on-demand route discovery protocols in MANETs was proposed. This represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. However, as we observed above, there are a plethora of other hidden channels that become available through concurrent execution of route discovery protocols. Additionally, in the context of mobility, which requires that route discovery take place simultaneously with data communication, large additional bandwidth is naturally generated and available to adversarial nodes. Consequently, in the proposed formal model, it is impossible to prevent that adversarial nodes break up routes by inserting non existing links. To address this shortcoming, either more flexible definitions of routes must be employed (e.g., redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil, wormhole, and more generally, man-in-the-middle attacks.

REFERENCES

[1] Mike Burmester and Breno de Medeiros ,“ On the Security of Route Discovery in MANETs “IEEE Transactions on mobile computing, vol. 8, no. 9, september 2009.

[2] Y.-C. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Security and Privacy, vol. 2, no. 3, pp. 28-39, Mar.2004.

[3] M. Burmester and T. van Le, “Secure Multipath Communication in Mobile Ad Hoc Networks,” Proc. Int’l Conf. Information Technology: Coding and Computing (ITCC ’04), vol. 2, pp. 399-405, 2004.

[4] M. Burmester, T. van Le, and M. Weir, “Tracing Byzantine Faults in Ad Hoc Networks,” Proc. Conf. Computer, Network and Information Security 2003, pp. 43-46, 2003

[5] L. Buttya´n and I. Vajda, “Towards Provable Security for Ad Hoc Routing Protocols,” Proc. ACM Workshop Ad Hoc and Sensor Networks (SASN ’04), 2004.