TENABLE ROUTE ENCOUNTER MODUS OPERANDI IN MANETS

Dr. SIVAKUMAR K

Abstract - A M**obile Ad-hoc Network** (**MANET**), consists of mobile platforms herein simply referred to as "nodes". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. It is a collection of wireless mobile devices with restricted broadcast range and resources, and no fixed infrastructure. Communication is achieved by relaying data along appropriate routes that are dynamically discovered and maintained through collaboration between the nodes. Discovery of such routes is a major task, both from efficiency and security points of view. Among the novel characteristics of this security mode, A novel route discovery algorithm called endairA was also proposed, together with a claimed security proof within the same model. In this paper, we show that the security proof for the route discovery algorithm endairA 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 composability is an essential feature for ubiquitous applications.

Keywords — MANET, Communication , security proof , endairA, etc.

I. INTRODUCTION

Mobile hosts and wireless networking hardware are becoming widely available, and extensive work has been done recently in integrating these elements into traditional networks such as the Internet. Oftentimes, however, mobile users will want to communicate in situations in which no fixed wired infrastructure such as this is available, either because it may not be economically practical or physically possible to provide the necessary infrastructure or because the expediency of the situation does not permit its installation.

For example, a class of students may need to interact during a lecture, friends or business associates may run into each other in an airport terminal and wish to share files, or a group of emergency rescue workers may need to be quickly deployed after an earthquake or flood. In such situations, a collection of mobile hosts with wireless network interfaces may form a temporary network without the aid of any established infrastructure or centralized administration. This type of wireless network is known as an ad hoc network.

Efficient communication through networking has become the order of the day. Networking, till a few decades back was confined to the wires that imposed a limitation on the positioning of users. With the advancement of technology in strides, networking has evolved into the wireless mode, wherein it is not required for the users to be stationary. An ad hoc network is a group of wireless mobile computers (or nodes); in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range.

The main aim of the project is to design a more secure routing protocol for ad hoc networks. The design of routing protocol based on On-demand source routing. The function of the routing protocol in ad hoc network is to establish route between nodes. Several 'secure' routing protocols have been proposed for ad hoc networks such as AODV, DSR, ZRP, TORA, DSDV, TBRPF, Ariadne and others. These secure routing protocols still have security vulnerabilities, and can be attacked. In this project it implements a more secure routing protocol for ad hoc networks. The protocol is implemented using GloMoSim network simulator.

II. ROUTING ALGORITHM

Route discovery can be proactive or reactive (on-demand). Proactive routing is usually table driven with reactive algorithms; routes are discovered only when needed. Proactive routing protocols maintain routes to all destinations, regardless of whether or not these routes are needed. In order to maintain correct route information, a node must periodically send control messages. Therefore, proactive routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no data traffic. The main advantage of this category of protocols is that hosts can quickly obtain route information and quickly establish a session. Reactive routing protocols can dramatically reduce routing overhead because they do not need to search for and maintain the routes on which there is no data traffic. This property is very appealing in the resource-limited environment.

Dr. Sivakumar K , Ph.D., MIEEE., Assistant Professor , College of Computer Science , King Khalid University - Kingdom of Saudi Arabia .(Email: rksivakumar@gmail.com)

Routing is a basic network functionality that supports communication. In MANETs, each node acts as a router forwarding data to other nodes.

It distinguishes three basic phases in routing:

1) Route discovery in which one or more routes (of adjacent nodes) that link a source S to a target T are sought,

2) Route maintenance in which broken links of established routes are fixed, and

3) Packet forwarding in which communication is achieved via established routes.

Route discovery can be proactive or reactive (on-demand). Proactive routing is usually table driven with reactive algorithms; routes are discovered only when needed.

1) The Source Routing Protocol (SRP)

The Source Routing Protocol algorithm is an on-demand algorithm, which enables dynamic, self-starting, multihop routing to be established when a source sensor node wishes to send a data packet. All the routing messages in SRP are small and have fixed length. This way less transmission energy is needed for the routing overhead, which is especially important at the source initiated request flooding. The SRP algorithm have three phrases: Route Setup, Route Maintenance and Route Re-establishment.

In SRP, route requests generated by a source S are protected by Message Authentication Codes (MACs) computed using a key shared with the target T. Requests are broadcast to all the neighbors of S. Each neighbor that receives a request for the first time appends its identifier to the request and rebroadcasts it. Intermediate nodes do the same. The MAC in the request is not checked because only S and T know the key used to compute it. When this request reaches the target T, its MAC is checked by T. If it is valid, then it is assumed by the target that all adjacent pairs of nodes on the path of the route request are neighbors. Such paths are called valid or plausible routes. The target T replaces the MAC of a valid route request with an MAC computed with the same key that authenticates the route. This is then sent back (upstream) to S using the reverse route. For example, a route request that reaches an intermediate node Xj is of the form

$\mathbf{msg}_{S,T,rreq}\mathbf{=(rreq,S,T,id,sn,X_1,....X_j,mac_S)}$

with id a randomly generated route identifier, sn a session number, and macS an MAC on (rreq, S,T, id, sn) computed by S using a key shared with T. If S,X1, . . .,Xp; T is a discovered route, then the route reply of the target T has the following fixed form for all intermediate nodes Xj, 1 ≤ j ≤ p:

$\mathbf{msg}_{S,T,rrep}\mathbf{=(rrep,S,T,id,sn,X_1,...Xp,mac_T)}$

where mac_T is an MAC computed by T with the key shared with S on the message fields preceding it.

2) Ariadne

Ariadne is an on-demand routing algorithm based on the Dynamic Source Routing (DSR) protocol. There are several variants of Ariadne, depending on which mode of authentication is used to protect route requests: one uses digital signatures, one TESLA, and one uses MACs. The MAC version has an optimized variant that uses iterated MAC computations instead of several independent MACs. In addition to being more efficient, the iterated MAC version has superior security characteristics when compared to the no optimized version. A typical route request that reaches an intermediate node Xj, 1 ≤ j ≤ p, on the route S =X_0,X_1, . . .,Xp, Xp_{+1} = T is of the form

$\mathbf{msg}_{S,\ T,rreq}\mathbf{=(rreq,S,T,id,X_1,..Xj,\ macsxi...}_{Xj}\mathbf{)}$

where $mac_{SX1...Xj}$ is the MAC computed by Xj with a key it shares with T on the route request received from X_{j-1}.The route reply of T is

$\mathbf{msg}_{S,\ T,rrep}\mathbf{=(rrep,S,T,id,X_1,..Xp,mac_T)}$

where mac_T is an MAC computed by T with a key shared with S on the message field that precedes it (rrep, S, T, id,X1, . . .,Xp).

3) EndairA

EndairA is one of the most secure on-demand ad hoc network source routing protocols which provides several defense mechanisms against so many types of attacks. In this paper, we prove the vulnerability of endairA to the tunneling attack by presenting an attack scenario against it. We also propose a new security mechanism to defend it against the tunneling attack by the utilization of the delay between receiving and sending its control packets computed locally by all intermediate nodes. Our proposed security mechanism can detect probable tunnels in the route as well as approximate locations of the adversarial nodes. It needs no time synchronization between mobile nodes of the network. It also does not change the number of control packets involved in endairA and only modifies the RREP messages slightly. Fundamentally, endairA (and the ABV model) was developed to deal with a class of hidden channels, the intrinsic hidden channels of a wireless broadcast medium in a neighborhood. However, security is not achieved because other hidden channels remain present.

III. ANALYSIS OF ARIADNE

This framework was used to analyze SRP and Ariadne, finding them insecure against hidden-channel attacks, and led to the design of endairA, an on-demand route discovery protocol that the authors claim to be provably secure. Later, the ABV model. In this section, It first outline the ABV framework and the attending attack on Ariadne. It then describes endairA. This discussion is not original and closely parallels arguments. However, it is directly cogent to the novel arguments which show that the security proof for endairA provided is flawed, and moreover, this route discovery protocol is not secure even in the (somewhat restricted) ABV security model.

The real-world and ideal-world models described in [15] are similar to those used in the generic secure reactive system approach [17], [21], but there are some crucial differences. In the ABV framework:

1. The adversary does not have full control of message delivery schedule, in the sense that the broadcast channel enforces the concept of communication rounds—in particular, the ABV framework does not capture rushing attacks (synchrony);
2. The adversary may prompt honest parties to initiate new route discoveries but not dishonest ones, in other words, the ABV security framework does not capture concurrent security in the presence of route discovery sessions that is initiated by adversarial nodes;
3. The adversary is no adaptive, i.e., cannot initiate new route discoveries as a function of previously observed messages
4. The link configuration of an MANET is enforced in the security framework by the communication medium functionality (Machine C in the real-world model of ABV [15]).

IV. ANALYSIS OF ENDAIRA

This implies that the route can be uniquely partitioned as follows: each partition consists of a single on compromised identifier (label) or a sequence of consecutive compromised identifiers. A plausible route is one whose partitions correspond to that of a real route that physically exists in the network. The security statement of endairA is that it only accepts plausible routes. Note that this statement also does not consider an adversarial lengthening of a route by assignment of multiple labels to a single compromised network node as an attack. Again, this is a strong restriction on the security guarantees that the ABV model can provide, but we also follow this paradigm because we wish to show that endairA fails in the exact model in [15].

1) An Attack on endairA

This is a hidden channel attack that does not require out-of-band resources. Consider an instance of endairA with source node S and let (S; A; X; B; Y; D; T)
be a sequence of identifiers of pair wise neighbor nodes in which only X; Y are faulty. In the attack, when the second faulty node Y receives

$\mathbf{msg_{S,T,rreq}=(rreq,S,T,id,A,X,B)}$

it drops node B from the listing and transmits

$\mathbf{msg_{S,T,rrep}=(rrep,S,T,id,A,X,Y,D,sig_T, sig_D\,)}$

Eventually, the route request will reach the target T, which will compute and send back a route reply. Node Y will then receive from D

$\mathbf{msg\ _{D,A,,rreq}=(rreq,D,A,id)}$

Now, Y can obviously attach its label and signature to this reply and transmit to B the extended reply, but B will not retransmit it because B is not included in the listing. Eventually, X will be able to reconstruct these signatures and can then generate the route reply

$\mathbf{msg_{S,T,rrep}=(rrep,S,T,id,A,X,Y,D,sig_T, sig_D, sig_Y, sig_X)}$

this is sent back to the source S and validated.

2) Hidden Channel and Concurrency Attacks

In all the attacks described above, including the attacks adversarial nodes succeed in shortening plausible routes by removing intermediate nodes. The adversarial nodes use hidden channels to communicate and transfer the necessary data (signatures, etc.). The hidden channels that we considered above do not use out-of-band resources; although this is an obvious alternative. Let us now pursue our earlier discussion on interleaving protocol instances. In a networking environment, one should expect that several instantiations of a routing protocol are executed. Some may involve route discovery, while others route maintenance, data communication, or general network applications. It makes no sense to require that route communication can only start when all the other route discovery instantiations (and network applications) have been completed.

V. SECURE ROUTE DISCOVERY CHALLENGES

Our argument about the impossibility of secure discovery of routes is simple and has been articulated throughout the paper. We base it on the fact that every route discovery algorithm is, in practice, vulnerable to attacks that exploit alternative communication channels to articulate distributed attacks by "encapsulating" and tunneling routing requests. Therefore, it does not seem possible to capture or "model out" Sybil and wormhole attacks from pure-protocol-based security models. The purpose of routing being to establish a communication infrastructure, it is always reasonable to assume the existence of alternative communication channels, namely those that route discovery will establish. Even though it is not possible to discover secure routes in general MANETs, there are several other approaches that could be used to establish secure communication channels. In the following, we consider two such approaches: multipath routes and route discovery with traceability.

VI. PROPOSED RESULT AND COMPARATIVE STUDY

At the end of the project, we expect to have a network which provides more security for route discovery in Mobile Adhoc network. Different types of protocols and algorithms are analyzed. Also some papers are surveyed .we are going to implement a secure system for Ad-Hoc networks using endairA protocol. The protocol uses blow fish algorithm.

1) PROPOSED RESULT

A new security framework tailored for on-demand route discovery protocols in MANETs. 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.

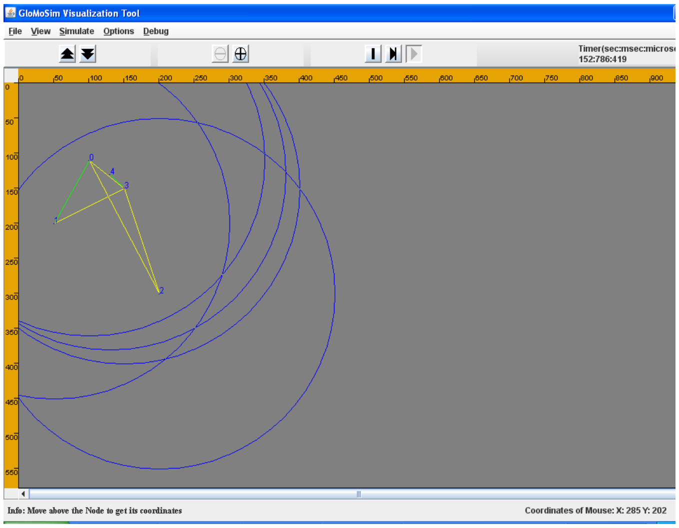
SRP is a secure variant of DSR. Route discovery is used to discover a route from a given source to a given destination. The neighbor discovery process is performed after the route request from source node. SRP is simple but it does not prevent the manipulation of mutable information added by intermediate nodes. The message authentication code is used for the authentication. The system uses authenticate the route by Message authentication codes (MACs) and Digital Signatures.

The Blowfish algorithm is used to provide confidentiality for the routing packets. Authentication and confidentiality operations are used to protect active attacks on route discovery. The passive attacks are handled by the neighbor verification method.

2) COMPARATIVE STUDY

S. No.	ALGORITHM/ PROTOCOL	Accuracy	Speed	Cost
1.	Secure Routing Protocol	Medium	High	High
2.	Symmetric-key authentication (MACs)	Low	Low	Medium
3.	Routing disruption attacks	High	High	High
4.	Ariadne Routing Protocol	Medium	Low	High
5.	Per-hop hash mechanism	Medium	Low	Medium
6.	Digital signatures	Medium	Medium	High
7.	Symmetric-key broadcast authentication with TESLA	High	Low	Medium
8.	EndairA Routing Protocol	High	High	Medium
9.	Route Discovery	High	Medium	Medium
10.	Route Maintenance	Medium	High	Low
11.	Symmetric Block Cipher	High	High	Medium
12.	Cryptographic hash function	Low	Medium	Low

VII. SAMPLE SNAPSHOTS:

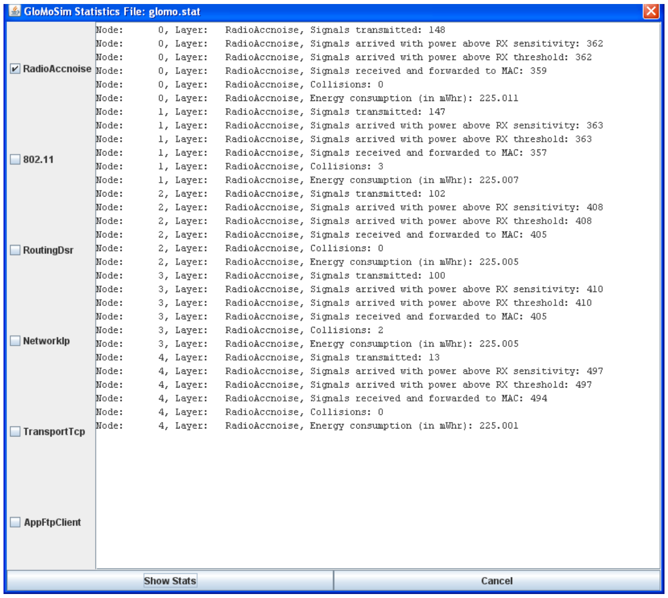


Timer(sec:msec:micros
152:786:419

Info: Move above the Node to get its coordinates

Coordinates of Mouse: X: 285 Y: 202

Figure 1



```
Node:      0, Layer:   RadioAccnoise, Signals transmitted: 148
Node:      0, Layer:   RadioAccnoise, Signals arrived with power above RX sensitivity: 362
Node:      0, Layer:   RadioAccnoise, Signals arrived with power above RX threshold: 362
Node:      0, Layer:   RadioAccnoise, Signals received and forwarded to MAC: 359
Node:      0, Layer:   RadioAccnoise, Collisions: 0
Node:      0, Layer:   RadioAccnoise, Energy consumption (in mWhr): 225.011
Node:      1, Layer:   RadioAccnoise, Signals transmitted: 147
Node:      1, Layer:   RadioAccnoise, Signals arrived with power above RX sensitivity: 363
Node:      1, Layer:   RadioAccnoise, Signals arrived with power above RX threshold: 363
Node:      1, Layer:   RadioAccnoise, Signals received and forwarded to MAC: 357
Node:      1, Layer:   RadioAccnoise, Collisions: 3
Node:      1, Layer:   RadioAccnoise, Energy consumption (in mWhr): 225.007
Node:      2, Layer:   RadioAccnoise, Signals transmitted: 102
Node:      2, Layer:   RadioAccnoise, Signals arrived with power above RX sensitivity: 408
Node:      2, Layer:   RadioAccnoise, Signals arrived with power above RX threshold: 408
Node:      2, Layer:   RadioAccnoise, Signals received and forwarded to MAC: 405
Node:      2, Layer:   RadioAccnoise, Collisions: 0
Node:      2, Layer:   RadioAccnoise, Energy consumption (in mWhr): 225.005
Node:      3, Layer:   RadioAccnoise, Signals transmitted: 100
Node:      3, Layer:   RadioAccnoise, Signals arrived with power above RX sensitivity: 410
Node:      3, Layer:   RadioAccnoise, Signals arrived with power above RX threshold: 410
Node:      3, Layer:   RadioAccnoise, Signals received and forwarded to MAC: 405
Node:      3, Layer:   RadioAccnoise, Collisions: 2
Node:      3, Layer:   RadioAccnoise, Energy consumption (in mWhr): 225.005
Node:      4, Layer:   RadioAccnoise, Signals transmitted: 13
Node:      4, Layer:   RadioAccnoise, Signals arrived with power above RX sensitivity: 497
Node:      4, Layer:   RadioAccnoise, Signals arrived with power above RX threshold: 497
Node:      4, Layer:   RadioAccnoise, Signals received and forwarded to MAC: 494
Node:      4, Layer:   RadioAccnoise, Collisions: 0
Node:      4, Layer:   RadioAccnoise, Energy consumption (in mWhr): 225.001
```

Figure 2

VIII. FUTURE WORKS AND CONCLUSION

A new security framework tailored for on-demand route discovery protocols in MANETs.This is successful in mitigating a class of hidden channel attacks—the attacks that are intrinsic to the wireless broadcast medium in a neighborhood.

As future work, 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 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] Acs, G., Buttya´n.L. and Vajda, I. (2004) Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks', Technical Report 159, Int'l Assoc. for Crypto logic Research.

[2] Acs, G., Buttya´n.L. and Vajda, I. (2005) 'Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks',Proc. European Workshop Security and Privacy in Ad Hoc and Sensor Networks (ESAS '05), pp. 113-127.

[3] Acs, G., Buttya´n.L. and Vajda, I. (2006) 'Modeling Adversaries and Security Objectives for Routing Protocols in Wireless Sensor Networks', Proc. Workshop Security in Ad Hoc and Sensor Networks (SASN '06).

[4] Beaver, D. and Haber, S. (1992) 'Cryptographic Protocols Provably Secure against Dynamic Adversaries', Proc. Conf. Advances in Cryptology (EUROCRYPT '92), pp. 307-323.

[5] Burmester, M., van Le, T., and Weir, M. (2003). 'Tracing Byzantine Faults in Ad Hoc Networks', Proc. Conf. Computer, Network and Information Security 2003, pp. 43-46,

[6] Burmester, M., van Le, T., and Yasinsac, A. (2007) 'Adaptive Gossip Protocols: Managing Security and Redundancy in Dense Ad Hoc Networks', J. Ad Hoc Networks, vol. 5, no. 3, pp. 286-297.

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

[8] Douceur.J.R. (2002) 'The Sybil Attack', Proc. First Int'l Workshop Peer-to- Peer Systems (IPTPS '02), pp. 252-260.

[9] Hall,J., Barbeau,M., and Kranakis,E. (2004) 'Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting', Proc. IASTED Int'l Conf. Comm., Internet, and Information Technology.

[10] Hu.Y.C., Johnson, D.B., and Perrig, A. (2003) 'SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks', Ad Hoc Networks, vol. 1, no. 1, pp. 175-192.

[11] Hu.Y.C., Perrig, A., and Johnson, D. (2002) 'Ariadne: A Secure on-Demand Routing Protocol for Ad Hoc Networks', Proc. ACM MobiCom.

[12] Hu.Y.C., Perrig, A., and Johnson, D. (2003) 'Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks', Proc. IEEE INFOCOM, pp. 1976-1986.

[13] Johnson, D. and Maltz D. (1996) 'Dynamic Source Routing in Ad Hoc Wireless Networks', Mobile Computing, Kluwer Academic Publishers.

[14] Mike Burmester, Breno de Medeiros (2009) 'On the Security of Route Discovery in MANETs', IEEE Transactions on Mobile Computing, vol. 8, no. 9, pp. 1180-1188.

[15] Papadimitratos, P. and Haas, Z. (2002) 'Securing Mobile Ad Hoc Networks', Handbook of Adhoc Wireless Networks.

[16] Papadimitratos, P. and Haas, Z. (2002) 'Secure Routing for Mobile Ad Hoc Networks', Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS '02).

[17] Perkins C.E. and Bhagwat, P. (1994), 'Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers', Proc. ACM SIGCOMM,

[18] Perkins, C. (1997) 'Ad-Hoc On-Demand Distance Vector Routing', Proc. Military Comm. Conf. (MILCOM '97), panel on ad hoc networks.

[19] Perrig, J.T.A., Canetti, R., and Song, D. (2000) 'Efficient Authentication and Signing of Multicast Streams over Lossy Channels', Proc. IEEE Symp. Security and Privacy, pp. 56-73.

[20] Pfitzmann, B. and Waidner, M. (2000) 'Composition and Integrity Preservation of Secure Reactive Systems', Proc. ACM Conf. Computer and Comm. Security, pp. 245-254.

[21] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., and Belding-Royer.E.M. (2002) 'A Secure Routing Protocol for Ad Hoc Networks', Proc. IEEE Int'l Conf. Network Protocols (ICNP '02).