ISSN:0975-9646

Performance Investigation and Analysis of Secured MANET Routing Protocols

A.Jayanand [#] , Prof.Dr.T.Jebarajan [*]

[#] *Principal, Maria Polytechnic College,Attoor, India (Research scholar, MSU)*

[*] *Principal, Kings Engineering College, Chennai, India*

Abstract— **In this research proposal, we present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. We then develop Rushing Attack Prevention (RAP), a generic defence against the rushing attack for on-demand protocols. RAP incurs no cost unless the underlying protocol fails to find a working route, and it provides provable security properties even against the strongest rushing attackers.**

Keywords— **Ariadne, Ad hoc network, MANET, Rushing attack.**

I. Introduction

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. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. They can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost. Applications such as military exercises, disaster relief, and mine site operation, for example, may benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications.

In a mobile wireless ad hoc network, computers (nodes) in the network cooperate to forward packets for each other, due to the limited wireless transmission range of each individual node. The network route from some sender node to a destination node may require a number of intermediate nodes to forward packets to create a ‘‘multi-hop’’ path from this sender to this destination. The role of the routing protocol in an ad hoc network is to allow nodes to learn such multi-hop paths. Since the nodes in the network may move at any time, or may even move continuously, and since sources of wireless interference and wireless transmission propagation conditions may change frequently, the routing protocol must also be able to react to these changes and to learn new routes to maintain connectivity.

Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network.

Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g., wired and stationary) network.

In this paper, we present a new attack, the rushing attack, which results in denial-of-service when used against all previously published on-demand ad hoc network routing protocols. Specifically, the rushing attack prevents previously published secure on demand routing protocols to find routes longer than two-hops (one intermediate node between the initiator and target). To defend this important class of protocols against the rushing attack, we develop a generic secure Route Discovery component, called Rushing Attack Prevention (RAP), that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

We also present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

II. Overview of Routing Security Protocols

A. Overview of ARIADNE

In this paper, we describe Ariadne primarily using the TESLA[3] broadcast authentication protocol for authenticating routing messages, since TESLA is efficient and adds only a single message authentication code (MAC) to a message for broadcast authentication. Adding a MAC (computed with a shared key) to a message can provide secure authentication in point-to-point communication; for broadcast communication, however, multiple receivers need to know the MAC key for verification, which would also allow any receiver to forge packets and impersonate the sender.

To use TESLA for authentication, each sender chooses a random initial key KN and generates a one-way key chain by repeatedly computing a one-way hash function H on this starting value: KN−1 = H[KN], KN−2 = H[KN−1], ...

In general, Ki = H[Ki+1] = HN−i [KN]. To compute any previous key Kj from a key Ki , j < i, a node uses the equation Kj = Hi−j [Ki]. To authenticate any received value on the one-way chain, a node applies this equation to the received value to determine if the computed value matches a previous known authentic key on the chain. Coppersmith and Jakobsson present efficient mechanisms for storing and generating values of hash chains [4].

B.Overview of SEAD

We present the design and evaluation of a new secure ad hoc network routing protocol using distance vector routing. Our protocol, which we call the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. We base the design of SEAD in part on the Destination-Sequenced Distance-Vector Ad Hoc network routing protocol (DSDV) [5], which was designed for trusted environments. In order to support use of SEAD with nodes of limited CPU processing capability, and to guard against Denial-of-Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one way hash functions and do not use asymmetric cryptographic operations in the protocol.

C. Overview of RAP

We introduce here a new attack, which we call the rushing attack that acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols including protocols that were designed to be secure. In an on-demand protocol, a node needing a route to a destination floods the network with ROUTE REQUEST packets in an attempt to find a route to the destination. To limit the overhead of this flood, each node typically forwards only one ROUTE REQUEST originating from any Route Discovery. In particular, existing on-demand routing protocols, such as DSR [6], LAR [7], Ariadne [8], SAODV [9], ARAN [10], AODV secured with SUCV [11] and SRP [12] only forward the REQUEST that arrives first from each Route Discovery.

In the rushing attack, the attacker exploits this property of the operation of Route Discovery. We now describe the rushing attack in terms of its effect on the operation of DSR Route Discovery; other protocols such as AODV [11], Ariadne [8], SAODV [9], and ARAN [10] are vulnerable in the same way. In the network shown in Figure 1, the initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbour of the target (shown in grey in the figure), then any route discovered by this Route Discovery will include a hop through the attacker. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

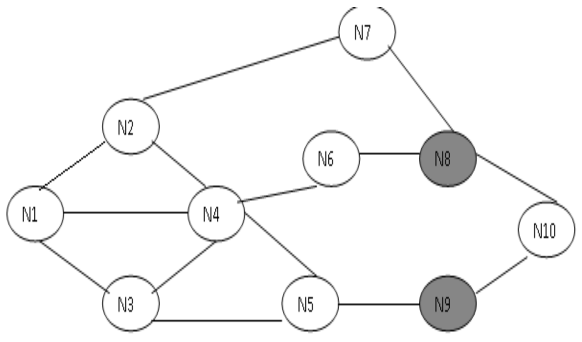


Figure1. Network illustrating Rushing Attack
N1 – Initiator, N10 – Target

● **Rushed Node**

III. Assumption

A. *Basic Ariadne Route Discovery*

Ariadne Route Discovery using MACs is the most efficient of the three alternative authentication mechanisms, but it requires pair wise shared keys between all nodes. When Ariadne is used in this way, the MAC list in the ROUTE REQUEST is computed using a key shared between the target and the current node, rather than using the TESLA key of the current node. The MACs are verified at the target and are not returned in the ROUTE REPLY. As a result, the target MAC is not computed over the MAC list in the REQUEST. In addition, no key list is required in the REPLY.

Route Discovery has two stages:

The initiator floods the network with a ROUTE REQUEST,

The target returns a ROUTE REPLY.

To secure the ROUTE REQUEST packet, Ariadne provides the following properties:

The target node can authenticate the initiator (using a MAC with a key shared between the initiator and the target).

The initiator can authenticate each entry of the path in the ROUTE REPLY (each intermediate node appends a MAC with its TESLA key)

No intermediate node can remove a previous node in the node list in the REQUEST or REPLY (a one-way function prevents a compromised node from removing a node from the node list).

A ROUTE REQUEST packet in Ariadne contains eight fields namely Route Request, Initiator, target, Id, time interval, hash chain, node list, MAC list.

TABLE I
Scenario parameters – ARIADNE

Number of nodes	50
Maximum velocity	20 m/s
Dimensions of space	1500 · 300 m2
Nominal radio range	250 m
Source–destination pairs	20
Application data payload size	512 bytes/packet
Total application data load	327 kilobytes/s
Raw physical link bandwidth	2 Megabytes/s

B. SEAD Route Discovery

The following six metrics to be computed for each simulation run:

- Packet Delivery Ratio (PDR).

The fraction of application level data packets sent that are actually received at the respective destination node.

- Packet Overhead.

The number of transmissions of routing packets; for example, a ROUTE REPLY sent over three hops would count as three overhead packets in this metric.

- Byte Overhead.

The number of transmissions of overhead (non-data) bytes, counting each hops as above.

- Mean Latency.

The average time elapsed from when a data packet is first sent to when it is first received at its destination.

- 99.99th Percentile Latency.

Computed as the 99.99th percentile of the packet delivery latency.

- Path Optimality.

Compares the length of routes used to the optimal (minimum possible) hop length as determined by an off-line omniscient algorithm, based on the nominal wireless transmission range of 250 m per hop.

TABLE 2
SEAD Parameters

Periodic route update interval	15s
Periodic updates missed before link is declared broken	3
Maximum packets buffered per node per destination	5
Hash length (q)	80 bits

C. RAP – Secure Route Discovery

In this section, we describe our secure route discovery protocol. We use three techniques in concert to prevent the rushing attack: our secure Neighbour Discovery protocol, our secure Route Delegation and delegation acceptance protocol, and randomized selection of which ROUTE REQUEST will be forwarded. The intuition behind Secure Route Discovery is to make the forwarding of REQUEST packets less predictable by buffering the first n REQUESTs received, then randomly choosing one of those REQUESTs.

However, we need to prevent an attacker from filling too many of these n REQUESTs, since otherwise the attacker could simply rush n copies of a REQUEST, rather than a single REQUEST, and We implement two additional security optimizations to this basic scheme. In general, these optimizations are based on using the property of no repudiation to spread information about malicious nodes. First, we require that each REQUEST be signed by the forwarding node.

A node detecting an attacker forwarding more than one REQUEST can expose the attacker by flooding the two REQUESTs. Second, if location information is available, and used for example to implement geographic packet leashes, an attacker claiming to be in two places at the same time can be blacklisted in the same way. For example, if each REQUEST includes in the node list location information and time information for each forwarding node, a node can keep a database of previous location information, and find two location claims that significantly exceed the maximum speed achievable by legitimate nodes.

In particular, if location information is accurate to δ, and time information is consistent to Δ, and maximum speed is ν, then two locations claimed t time apart is maliciously claimed if the distance between the two locations is greater than $2\delta+\nu(t+2\Delta)$. Our blacklist mechanisms do not need authentication, since the no repudiation of contradicting information can be verified by any nodes. We route blacklist information by flooding: contradictory information is rebroadcast by any node that verifies the no repudiation and did not have this malicious node on its blacklist. This approach is similar to the blacklist mechanism used by Ariadne.

A : |A←R {0,1}>

M1a = <ROUTE REQUEST, id . . .>

M1b = <NEIGHBOR SOLICITATION,A,|A>

∑M1 = Sign(H(M1a || M1b))

A→ : <M1a,M1b, ∑M1>

B : |B←R {0,1}>

M2a = <NEIGHBOR REPLY, A,B,|A,|B>

∑M2 = Sign(H(M2a))

B→A : <M2a,M2b, ∑M2>

A : M3a = <NEIGHBOR VERIFICATION,A,B,|A,|B>

∑M3a = Sign(H(M3a))

M3b = <ROUTE DELEGATION,A,B,S,R, id>

∑M3b = Sign(H(M3b))

A→B : <M3a, ∑M3a ,M3b, ∑M3b>

B : |B←R {0,1}>

M4a = <ROUTE REQUEST, id. . . ∑M3b, ∑M4a . . .>

M4b = <NEIGHBOR SOLICITATION, B,|>

∑M4 = Sign (H (M4a) || H (M4b))

B→ : <M4a, M4b, ∑M4>

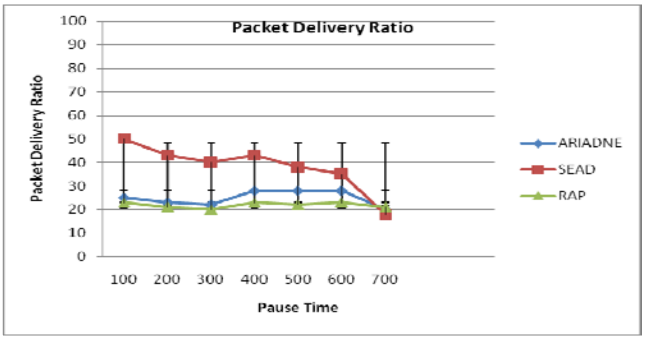
Explanation

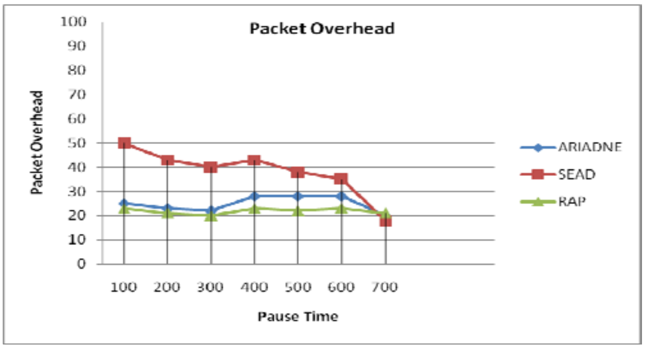
B forwarding the REQUEST from A. ΣM2 can be generated using a shared key, if available. The ROUTE REQUEST in M4a includes the bidirectional Neighbour Verification messages M3a and M4c, together with the necessary authenticators (H (M3b) and ΣM3). The use of H (M3b) in ΣM3 allows the verification of M3a without needing M3b, which decreases the overhead caused by the REQUEST packet. The same technique is used in creating ΣM4.

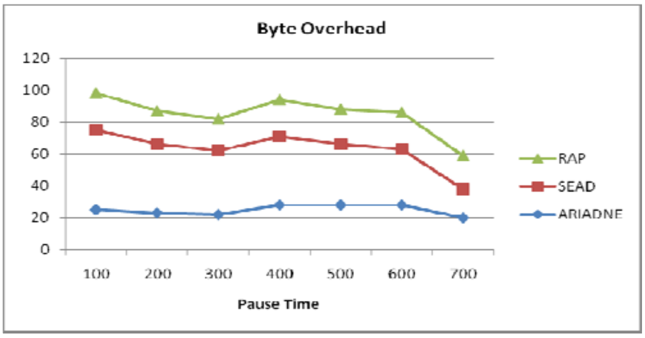
IV. SIMULATION

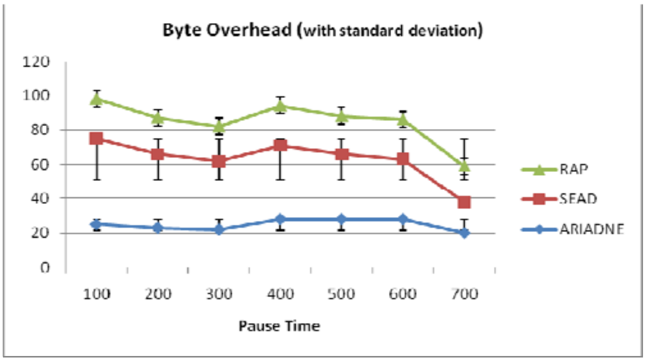
To evaluate the overhead of using our secure neighbour discovery mechanism in a non-adversarial environment, we simulated our scheme using the ns-2 simulator, using Ariadne as our underlying routing protocol. We call this modified protocol RAP (Rushing Attack Prevention). We did not implement the optimizations because our simulations did not include an attacker, so our results would be equivalent to just using Ariadne. We used the original Ariadne source code [21], and modified it to use digital signatures based on HORS and geographical leashes for wormhole protection.

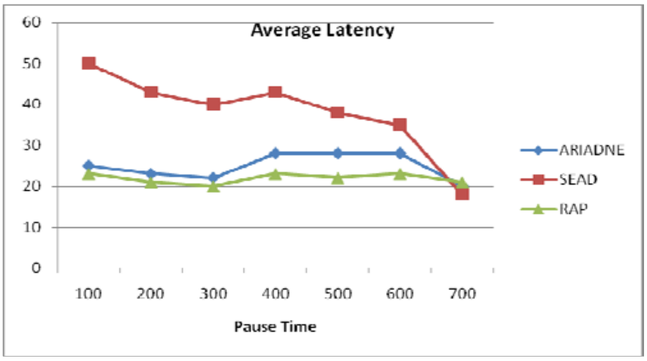
We compared our results with Ariadne and SEAD in order to determine the added costs of RAP when there are no attackers. However, when a rushing attacker is present, existing on-demand ad hoc network routing protocol would in general be unable to deliver packets over paths longer than two hops. RAP, on the other hand, would be able to discover working paths much of the time, and as a result, would generally outperform existing on-demand routing protocols. In this model, each node is randomly placed; at the beginning of the simulation, it waits for a pause time, and then chooses a velocity uniformly between 0 and 20 meters per second. It then proceeds to a random location at that velocity, and upon arriving waits for the pause time and repeats. We simulated pause times of 0, 30, 60, 120, 300, 600, and 900 seconds.

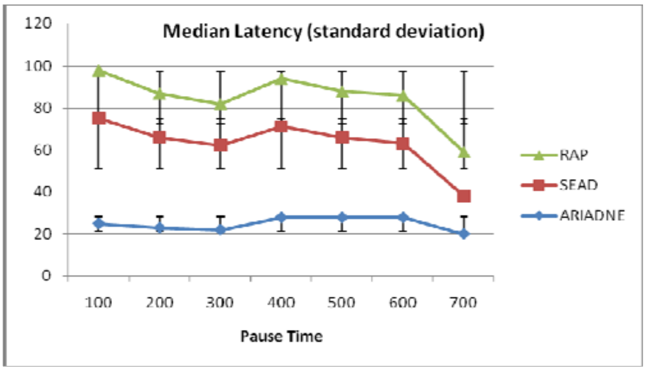


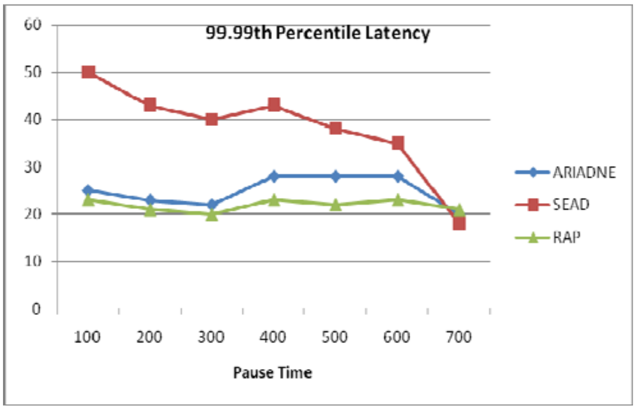












V. RELATED WORK

Dr.B.Anandampillai [1][2], proposes a novel method to assess different models of the usage of static and JADE Mobile Agents to determine the best route through Ad-Hoc networks. These are appraised in the terms of performance, re-configurability and ease of installation.

Lundberg [13], presents several potential problems including node compromise, computational overload attacks, energy consumption attacks, and black hole attacks.

Deng et al. [14], further discuss energy consumption and black hole attacks along with impersonation and routing information disclosed.

Jakobsson et al. [15], categorize attacks as manipulation of routing information and exhaustive power consumption, and provide detailed treatments of many characteristic attacks.

Zhou and Haas [16], present a multi-path protocol extension that uses threshold cryptography to implement the key management system. It requires some nodes to function as servers and an authority to initialize these servers.

Zapata and Asokan propose SAODV [17], a secure version of AODV, which uses digital signatures and hash chains to secure the routing messages.

Pissinou et al. [18], propose a trust-based version of AODV using static trust levels. The same authors then extend this protocol, to thwart multiple colluding nodes. Neither of these addresses securing the trust exchanges, or the overhead involved.

Lai et al. introduce a trust-based variant of AODV in [19] that secures the trust information. However, their protocol requires an intrusion detection system in the network.

Finally, Meka et al.[20], propose a third trusted AODV with a simple method of evaluating trust even without source routing.

VI. Conclusion

Ariadne provides better average latency when compared to SEAD and RAP whereas RAP seems to be better when compared to ARIADNE and SEAD. Ariadne provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptographic operations. Ariadne operates on-demand, dynamically discovering routes between nodes only as needed; the design is based on the basic operation of the RAP and SEAD protocol. We have presented the evaluation scheme of SEAD, a new secure ad hoc network routing protocol using distance vector routing. We have also described the rushing attack, a novel and powerful attack against on-demand ad hoc network routing proto cols. This attack allows an attacker to mount a denial-of-service attack against all previously proposed secure on-demand ad hoc network routing protocols and RAP (Rushing Attack Prevention), a new protocol that thwarts the rushing attack.

References

[1] Dr.B.Anandampillai, Routing, Topology Discovery, and Automatic Network Reconfiguration in AD-Hoc Networks using JADE Mobile Agents, Asian Journal of Information Technology, Volume 6, Number 4, 2007, pp 418-423.

[2] Dr.B.Anandampillai, Content Based Multicasting Using Jade, International Journal of Soft Computing Volume 2, Number 3, 2007, PP 422-425

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J.D. Tygar, SPINS: Security Protocols for Sensor Networks, in: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom 2001) (July 2001) pp. 189–199.

[4] D. Coppersmith and M. Jakobsson, Almost optimal hash sequence traversal: Proceedings of the 4th Conference on Financial Cryptography (FC'02), Lecture Notes in Computer Science (2002) pp. 102–119.

[5] C.E. Perkins, P. Bhagwat, Highly Dynamic Destination- Sequenced Distance-Vector routing (DSDV) for mobile computers, in: Proceedings of the SIGCOMM _94 Conference on Communications Architectures, Protocols and Applications, August 1994, pp. 234–244.

[6] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). Internet-Draft, draft-ietf-manet-dsr-07.txt, February 2002.

[7] Young-Bae Ko and Nitin Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98), pages 66–75, October 1998.

[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pages 12–23, September 2002.

[9] Manel Guerrero Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), September 2002.

[10] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding Royer. A Secure Routing Protocol for Ad hoc Networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02) November 2002.

[11] Claude Castelluccia and Gabriel Montenegro. Protecting AODV against Impersonation attacks. IETF MANET Mailing List.

[12] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad Hoc Networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[13] J. Lundberg. Routing security in ad hoc networks, 2000.

[14] H. Deng. Routing security in wireless ad hoc networks, 2002.

[15] M. Jakobsson, S. Wetzel, and B. Yener. Stealth attacks on ad hoc wireless networks. In Proceedings of VTC, 2003, 2003.

[16] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network, 13(6):24–30, 1999

[17] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In WiSE '02: Proceedings of the ACM workshop on Wireless security. ACM Press, 2002.

[18] N. Pissinou, T. Ghosh, and K. Makki. Collaborative trust based secure routing in multihop ad hoc networks. In NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, 2004.

[19] T. Ghosh, N. Pissinou, and K. Makki.Collaborative trustbased secure routing against colluding malicious nodes in multi-hop ad hoc networks. In LCN '04: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04). IEEE Computer Society, 2004.

[20]. K. Meka, M. Virendra, and S. Upadhyaya. Trust basedrouting decisions in mobile ad-hoc networks. In Proceedingsof theWorkshop on Secure Knowledge Management (SKM 2006), 2006.

[21] The Monarch Project. Rice Monarch Project: Mobile Networking Architectures, project home page. Available at http://www.monarch.cs.rice.edu/