Security in Routing Protocol for Ad Hoc Networks

Abu Taha Zamani[1], Syed Zubair[2]

[1]Lecturer,Deanship of Information Technology,Northern Border University, Kingdom of Saudi Arabia

[2]Lecturer,Deanship of Information Technology,Northern Border University, Kingdom of Saudi Arabia

Abstract: ***In this paper, we discuss security issues and their current solutions in the ad hoc Networks. Ad hoc networks are a key factor in the evolution of wireless communications. An ad hoc wireless network is a collection of wireless nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Security in ad hoc network is a grand challenge problem now a day. To enhance the security levels in the routing protocol to prevent the network against active and passive attacks without the presence of central authority. A peer review process has been introduced to check the integrity and non-repudiation of the routing packets and key exchange packets. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and nonrepudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. Various approaches and protocols have been proposed to address ad hoc networking problems, and multiple standardization efforts are under way within the Internet Engineering Task Force, as well as academic and industrial research projects. In this paper we attempt to analyze threats faced by the ad hoc network environment and provide a classification of the various security mechanisms.***

Keywords: wireless networks; routing; routing protocol, ad hoc network, security

1. Introduction

An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required.Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile ad-hoc network. Nodes rely on each other to established communication, thus each node acts as a router. Therefore, in a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes.

In a wireless world, dominated by Wi-Fi, architectures which mix mesh networking and ad-hoc connections are the beginning of a technology revolution based on their simplicity. On wireless computer networks, ad hoc mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage. Ad-hoc networks cannot bridge to wire Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links while those which are far apart rely on othernodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems [1] [2]. Figure 1 shows the working of ad hoc network. There are two different types of wireless networks. The first and easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes "can see" the others. The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

In this paper our main focus is regarding the security of the currently implemented routing algorithms. The focus is mainly on the security of the routing protocols used in the second kind of ad-hoc network. Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

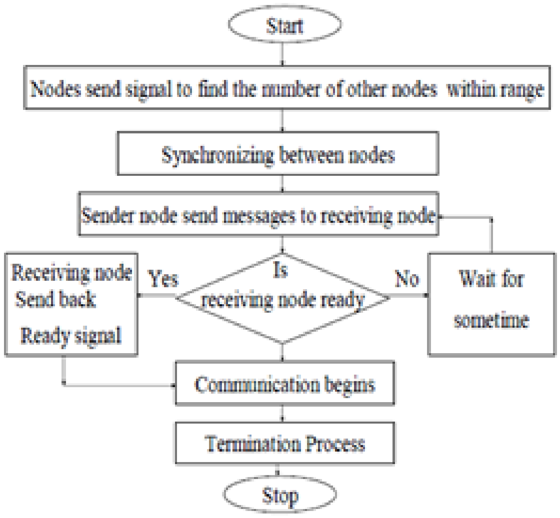

Figure 1: Working of a general Ad Hoc Network

They are mainly; *Confidentiality*: Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed; *Availability:* Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g. key management service.

- Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
- Integrity: Message being transmitted is never altered.
- Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

All the security mechanisms must be implemented in anyad-hoc networks so as to ensure the security of thetransmissions along that network. Whenever considering anysecurity issues with respect to a network, there is a need toensure that the above mentioned security goals have been putinto effect and none (most) of them are flawed. ContemporaryRouting Protocols for ad-hoc networks cope well withdynamically changing topology but are not designed toaccommodate defense against malicious attackers. No singlestandard protocol captures the common security threats andprovides the guidelines to a secure routing scheme. Routersexchange network topology, informally, in order to establishroutes between nodes and other networks which act as anotherpotential target for malicious attackers. Broadly there are twomajor categories of attacks when considering any networkAttacks from external sources and attacks from within thenetwork. The second attack is more severe and detection andcorrection is difficult. Routing protocol should be able tosecure themselves against both of these attacks.

2. Security Issues in Routing Protocols

The contemporary routing protocols for ad-hoc networkscope well with dynamically changing topology but are notdesigned to accommodate defense against malicious attackers.Today's routing algorithms are not able to thwart commonsecurity threats. Most of the existing ad hoc routing protocolsdo not accommodate any security and are highly vulnerable toattacks. Threats and attacks against ad hoc routing underseveral areas of application and suggested [13] solutions thatcould be used when secure protocols are designed. Routers exchange network topology informally in order to establishroutes between nodes - another potential target for maliciousattackers who intend to bring down the network. Externalattackers inject erroneous routing information, replaying oldrouting information or distort routing information in order topartition a network or overload a network with retransmissions,thereby causing congestion, and hence a denial of service. Internally compromised nodes are harder to detect and correct.Routing information signed by each node will not work sincecompromised nodes can generate valid signatures using theirprivate keys. Detection of compromised nodes through routinginformation is also difficult due to the dynamic topology of adhocnetworks.

In mobile ad-hoc networks, nodes do not rely on anyrouting infrastructure but relay packets for each other. Thuscommunication in mobile ad-hoc networks functions properlyonly if the participating nodes cooperate in routing andforwarding [19]. However, it may be advantageous forindividual nodes not to cooperate, for example to save power orto launch security attacks such as denial-of-service. In thispaper, we give an overview of potential vulnerabilities andsecurity requirements of mobile ad-hoc networks, and proposedprevention, detection and reaction mechanisms to thwartattacks.

2.1 Types of ad hoc Routing Protocols

In general there are two types of routing protocols:

- Proactive Routing Protocols
- Reactive Routing Protocols

In Proactive Routing Protocols, the nodes keep updating their routing table's byperiodical messages. This can be seen in Optimized Link StateRouting Protocol (OLSR) and the Topology Broadcast basedon Reverse Path Forwarding Protocol (TBRPF). In Reactive orOn Demand Routing Protocols the routes are created onlywhen they are needed. The application of this protocol can beseen in the Dynamic Source Routing Protocol (DSR) and theAd-hoc On-demand Distance Vector Routing Protocol (AODV).In today's world the most common ad-hoc protocols are theAd-hoc On-demand Distance Vector routing protocol and theDestination-Sequenced Distance-Vector routing protocol andthe Dynamic Source Routing. All these protocols are quiteinsecure because attackers can easily obtain information aboutthe network topology. This is because in the AODV and DSRprotocols, the route discovery packets are carried in clear text.Thus a malicious node can discover the network structure justby analyzing this kind of packets and may be able to determinethe role of each node in the network. With all these informationmore serious attacks can be launched in order to disruptnetwork operations.First, confirm that you have the correct template for yourpaper size. This template has been tailored for output on theUS-letter paper size. If you are using A4-sized paper, pleaseclose this file and download the file for "MSW A4 format".

2.2 Types of Attacks Faced by RoutingProtocols

Due to their underlined architecture, ad-hoc networks aremore easily attacked than a wired network. The attacksprevalent on ad-hoc routing protocols can be broadly classifiedinto passive and active attacks.

A *Passive Attack* does not disrupt the operation of theprotocol, but tries to discover valuable information by listeningto traffic. Passive attacks basically involve obtaining vitalrouting information by sniffing about the network. Such attacksare usually difficult to detect and hence, defending against suchattacks is complicated. Even if it is not possible to identify theexact location of a node, one may be able to discoverinformation about the network topology, using these attacks.

An *Active Attack*, however, injects arbitrary packets andtries to disrupt the operation of the protocol in order to limitavailability, gain authentication, or attract packets destined toother nodes. The goal is basically to attract all packets to theattacker for analysis or to disable the network. Such attacks canbe detected and the nodes can be identified.

2.3 Attacks against Ad Hoc Networks

The most prominent attacks prevalent against ad hocnetworks, most of which are active attack [5]. We addressthese attacks are

1) Attacks based on modification

This is the simplest way for a malicious node to disturb theoperations of an ad-hoc network. The only task the maliciousnode needs to perform is to announce better routes (to reachother nodes or just a specific one) than the ones presentlyexisting. This kind of attack is based on the modification of themetric value for a route or by altering control message fields.There are 3 ways in which this can be achieved: *Redirection byChanging the Route Sequence Number*: When deciding uponthe best / optimum path to take through a network, the nodealways relies on a metric of values, such as hop count delaysetc. The smaller the value, the more optimum the path. Hence,a simple way to attack a network is to change this value with asmaller number than the last "better" value. *Redirection byAltering the Hop Count:* This attack is more specific to theAODV protocol wherein the optimum path is chosen by thehop count metric. A malicious node can disturb the network byannouncing the smallest hop count value to reach thecompromised node. In general, an attacker would use a valuezero to ensure to the smallest hop count. Taking for examplethe 'wormhole' attack,[14] an attacker records packets at onelocation in the network, tunnels them to another location, andretransmits them there into the network. This could potentiallylead to a situation where, it would not be possible to find routeslonger than one or two hops, probably disruptingcommunication. *Denial of Service by Altering RoutingInformation:* Consider, in a bus topology, a scenario wherein anode A wants to communicate with node E. At node A therouting path in the header would be A-B-C-D-E. If B is acompromised node, it can alter this routing detail to A-B-C-E.But since there exists no direct route from C to E, C will dropthe packet. Thus, A will never be able to access any service /information from E. Another instance can be seen whenconsidering a category of attacks called 'The Black HoleAttacks'. Here, a malicious node uses the routing protocol toadvertise itself as having the shortest path to the node whosepackets it wants to intercept. Once the malicious node has beenable to insert itself between the communicating nodes, it can doanything with the packets passing between them. It can thenchoose to drop the packets thereby creating a DoS.

2) Impersonation Attacks

More generally known as '*spoofing*', since the maliciousnode hides its' IP and or MAC address and uses that of anothernode. Since current ad-hoc routing protocols like AODV andDSR do not authenticate source IP address, a malicious nodecan launch many attacks by using spoofing. Take for example asituation wherein an attacker creates loops in the network toisolate a node from the remainder of the network. To do this, the attacker needs to spoof the IP address of the node he wantsto isolate from the network and then announce new route to theothers nodes. By doing this, he can easily modify the networktopology as he wants.

3) Attacks by Fabrication of Information

There are basically 3 sub categories for fabrication attacks.In any of the 3 cases, detection is very difficult. *Falsification of Rote Error Messages:* This attack is very prominent in AODVand DSR, because these two protocols use path maintenance torecover the optimum path when nodes move. The weakness ofthis architecture is that whenever a node moves, the closestnode sends an "error" message to the other nodes so as toinform them that a route is no longer accessible. If an attacker can cause a DoS attack by spoofing any node and sending errormessages to the all other nodes. Thus, the malicious node canisolate any node quite easily. *Corrupting Routing State – RouteCache Poisoning:* A passive attack that can occur especially inDSR due to the promiscuous mode of updating routing tableswhich is employed. This occurs when information stored inrouting tables is deleted, altered or injected with falseinformation. A node overhearing any packet may add therouting information contained in that packet's header to its ownroute cache, even if that node is not on the path from source todestination. The vulnerability of this system is that an attackercould easily exploit this method of learning routes and poisonroute caches by broadcast a message with a spoofed IP addressto other nodes. When they receive this message, the nodeswould add this new route to their cache and would nowcommunicate using the route to reach the malicious node.

Routing table overflow attack: Consider ad-hoc network isusing a "proactive" protocol i.e. an algorithm which tries tofind routing information even before it is needed. This createsvulnerabilities since the attacker can attempt to create routes tonon-existent nodes. If enough routes are created, new routescan no longer be added due to an overwhelming pressure on theprotocol. After considering all the above plausible attacks wecan draw a conclusion that we need to have a routing protocolthat establishes routes without being susceptible to falseinformation from any malicious node. A good routing protocolshould also be able to detect the malicious nodes and to react inconsequence, by changing routes, etc. A malicious node canhowever, be either a potential attacker or a regular node whichencountered problems (low battery, etc.).

3. Classification of Techniques Used to Secured Hoc Networks

In order to provide solutions to the security issues involvedin ad-hoc networks, we must elaborate on the two of the mostcommonly used approaches in use today:

- Prevention
- Detection and Reaction

Prevention dictates solutions that are designed such thatmalicious nodes are thwarted from actively initiating attacks.Prevention mechanisms require encryption techniques toprovide authentication, confidentiality, integrity and nonrepudiationof routing information. Among the existingpreventive approaches, some proposals use symmetricalgorithms, some use asymmetric algorithms, while the othersuse one-way hashing, each having different trade-offs andgoals.Prevention mechanisms, by themselves cannot ensurecomplete cooperation among nodes in the network. Detectionon the other hand specifics solutions that attempt to identifyclues of any malicious activity in the network and take punitiveactions against such nodes. A node may misbehave by agreeingto forward packets and then failing to do so, because it isoverloaded, selfish or malicious. An overloaded node lacks theCPU cycles, buffer space or available network bandwidth toforward packets. A selfish node [18] is unwilling to spendbattery life, CPU cycles or available network bandwidth toforward packets not of direct interest to it, even though itexpects others to forward packets on its behalf. A maliciousnode [14] launches a denial of service attack by droppingpackets. All protocols defined in this category detect and reactto such misbehavior.

Using this as the basis for our survey, we describe the following broad classifications:

- Prevention using asymmetric cryptography using symmetric cryptography using one-way hash chains
- Detection and Reaction.

3.1 Prevention using Asymmetric Cryptography

Asymmetric cryptographic techniques specify theunderlined basic methodology of operation for protocols underthis category. A secure wired networks or a similar network is required to distribute public keys or digital certificates in thead-hoc network. Mathematically speaking a network with nnodes would require n public keys stored in the network. SAODV [3] (an extension to AODV routing protocol) andARAN [4] are two of the protocols defined in this category.

3.2 Prevention using symmetric cryptography

Symmetric cryptographic techniques are used to avoidattacks on routing protocols in this section. We assume thatsymmetric keys are pre-negotiated via a secured wiredconnection. Taking a mathematical approach we see that anetwork with ‘n’ nodes would require n * (n + 1) / 2 pair wisekeys stored in the network. SAR [5] and SRP [6] [16] [15] are the two protocols that belong to this category.

1) Prevention using Asymmetric Cryptography: SecureAd-hoc On-demand Distance Vector RoutingProtocol (SAODV) [3]

SAODV adds security to the famous AODV protocol. Itsbasic functionality lies in securing the ADOV protocol byauthenticating the non-mutable fields of the routing messageusing digital signatures. It also provides an end-to-endauthentication and node-to-node verification of these messages.The underlined process is relatively simple. The source nodedigitally signs the route request packet (RREQ) and broadcastsit to its neighbors. When an intermediate node receives aRREQ message, it first verifies the signature before creating orupdating a reverse route to its predecessor. It then stores orupdates the route only if the signature is verified. A similarprocedure is followed for the route reply packet (RREP). As anoptimization, intermediate nodes can reply with RREPmessages, if they have a “fresh enough” route to thedestination. Since the intermediate node will have to digitallysign the RREP message as if it came from the destination, ituses the double signature extension described in this protocol.The only mutable field in SAODV messages is the hop-countvalue. In order to prevent wormhole attacks this protocolcomputes a hash of the hop count field.

2) Prevention using Asymmetric Cryptography: Authenticated Routing for Ad-hoc Networks (ARAN) [4]

ARAN is an on-demand routing protocol that makes use ofcryptographic certificates to offer routing security. Its mainusage is seen in managed-open environments. It consists of apreliminary certification process followed by a routeinstantiation process that guarantees end-to-end authentication.

This protocol requires the use of a trusted certificate serverT, whose public key is known to all the nodes in the network.End-to-end authentication is achieved by the source by havingit verify that the intended destination was reached. In thisprocess, the source trusts the destination to choose the returnpath. The source begins route instantiation by broadcasting aRoute Discovery Packet (RDP) that is digitally signed by thesource. Following this, every intermediate node verifies theintegrity of the packet received by verifying the signature. Thefirst intermediate node appends its own signature encapsulatedover the signed packet that it received from the source. Allsubsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to thepacket. The RDP packet contains a nonce and timestamp toprevent replay attacks and to detect looping. Similarly, eachnode along the reverse path (destination to source) signs theREP and appends its own certificate before forwarding the REPto the next hop. Although hashing the hop-count value preventsmalicious nodes in advertising shorter routes in SAODV, itdoes not prevent nodes from advertising longer routes. Nodescan forward routing messages by applying the hash functionmultiple times making the route appear longer than it is.

One of the main issues with the ARAN protocol is therequirement of a certificate server, which means that theintegrity of that server is vital. This is by however, only adesign issue and as it is intended for securing communicationover a managed-open environment it shouldn’t be considered abig issue. Both the protocols in this category do not addresswormhole attacks. While ARAN provides both node-to-nodeand end-to-end authentication, it does not have any significantgain over SAODV (that uses only end-to-end authentication) interms of security.

3) Prevention using Symmetric Cryptography: Security-Aware ad hoc Routing (SAR) [5]

SAR is an attempt to use traditional shared symmetric keyencryption in order to provide a higher level of security in adhocnetworks. SAR can basically extend any of the current adhocrouting protocols without any major issues. The SARprotocol makes use of trust levels (security attributes assignedto nodes) to make informed, secure routing decision. Althoughcurrent routing protocols discover the shortest path betweentwo nodes, SAR can discover a path with desired securityattributes (E.g. a path through nodes with a particular sharedkey). The different trust levels are implemented using sharedsymmetric keys. In order for a node to forward or receive apacket it first has to decrypt it and therefore it needs therequired key. Any nodes not on the requested trust level willnot have the key and cannot forward or read the packets. Everynode sending a packet decides what trust level to use for thetransfer and thereby decides the trust level required by everynode that will forward the packet to its final destination.

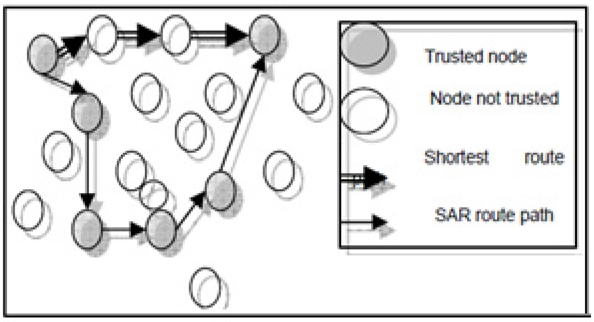

Figure 2: Variation of shortest path route selection betweenSAR and other routing algorithms

SAR is indeed secure in the way that it does ensure thatonly nodes having the required trust level will read and reroute the packets being sent. Unfortunately, SAR still leaves a lot ofsecurity issues uncovered and still open for attacks such as:

- Nothing is done to prevent intervention of a possiblymalicious node from being used for routing, as long asthey have the required key
- If a malicious node somehow retrieves the required keythe protocol has no further security measure to preventagainst the attacker from bringing the entire network toa standstill.
- There is excessive encryption and decryption required at eachhop. Since we are dealing with mobile environments the extraprocessing leading to increased power consumption can be aproblem.

SAR is intended for the managed-open environment as itrequires some sort of key distribution system in order todistribute the trust level keys to the correct devices.

4) Prevention using Symmetric Cryptography: **SecureRouting Protocol (SRP)** [6]

Secure Routing Protocol, SRP, is another protocolextension that can be applied to any of the most commonlyused protocols today. The basic idea of SRP is to set up asecurity association (SA) between the source and thedestination node.[16] An SA is a secret-key scheme used topreserve integrity in the routing information. The SA is usuallyset up by negotiating a shared key based on the other party'spublic key, and after that the key can be used to encrypt anddecrypt the messages. The routing path is always sent alongwith the packets, unencrypted though (since none of theintermediate nodes have knowledge of the shared key).

The above features are achieved with low computationalcost and bit overhead. In addition, the protocol is practicallyimmune to IP spoofing and implements partial caching withoutcompromising security in the network. More than one RREQ packet reaches the destination through different routes. Thedestination calculates a MAC covering the RREP contents andthen returns the packet to the source over the reverse routeaccumulated in the respective RREQ packet. The destinationresponds to one or more route request packets to provide thesource with an as diverse topology picture as possible.

4. Conclusion

Mobile ad-hoc networks have properties that increase theirvulnerability to attacks. Unreliable wireless links are vulnerableto jamming and by their inherent broadcast nature facilitateeavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to applicationspecifictrade-offs between security and resource consumptionof the device. Mobility/Dynamics make it hard to detectbehavior anomalies such as advertising bogus routes, becauseroutes in this environment change frequently. Self-organizationis a key property of ad-hoc networks. Besides authentication, confidentiality, integrity, availability, access control, and non-repudiation being harder to enforce because of the properties ofmobile ad-hoc networks, there are also additional requirementssuch as location confidentiality, cooperation fairness and theabsence of traffic diversion.

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers specialopportunities to attackers. Without proper security, it ispossible to gain various advantages by malicious behavior:better service than cooperating nodes, monetary benefits byexploiting incentive measures or trading confidentialinformation; saving power by selfish behavior; preventingsomeone else from getting proper service, extracting data to getconfidential information, and so on. Routes should beadvertised and set up adhering to the routing protocol chosenand should truthfully reflect the knowledge of the topology ofthe network. By diverting the traffic towards or away from anode, incorrect forwarding, no forwarding at all, or other non-cooperativebehavior, nodes can attack the network. We have discussed the various routing and forwarding attacks in thissurvey. We have also discussed prevention and detection mechanisms that were adopted to provide security in ad hocnetworks. A prevention-only strategy will only work if theprevention mechanisms are perfect; otherwise, someone willfind out how to get around them. Most of the attacks andvulnerabilities have been the result of bypassing preventionmechanisms. In view of this reality, detection and response are essential. In this paper we discussed proposals representing allof these classes.Even though prevention works as the first line of defense, itis not sufficient in addressing all the security threats. Hence we suggest an integrated layered framework which adopts theprevention techniques for the first level and detectiontechniques can be used at the second level complementing theprotection techniques.

References

[1] J.-P. Hubaux, L. Buttyan, and S. Capkun, The quest for security inmobile ad hoc networks," in The 2nd ACM Symposium on Mobile AdHoc Networking and Computing, October 2001.

[2] L. Zhou and Z. Haas, Securing ad hoc networks," IEEE NetworkMagazine, vol. 13, November/December 1999.

[3] Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector(SAODV) Routing INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt, August 2002. First published in the IETF MANET Mailing List(October 8th 2001).

[4] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, Clay Shields. ASecure Routing Protocol for Ad Hoc Networks In Proceedings of the 10Conference on Network Protocols (ICNP), November 2002.

[5] S. Yi, P. Naldurg, and R. Kravets Security-Aware Ad hoc Routing forWireless Networks The Second ACM Symposium on Mobile Ad HocNetworking & Computing (MobiHoc'01), 2001.(another versionSecurity-Aware Ad Hoc Routing Protocol for Wireless Networks,Report, August, 2001).

[6] PanagiotisPapadimitratos and Zygmunt J. Haas Secure Routing forMobile Ad hoc Networks SCS Communication Networks and

[7] Distributed Systems Modeling and Simulation Conference (CNDS2002), San Antonio, TX, January 27-31, 2002.

[8] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: SecureEfficient Distance Vector Routing for Mobile Wireless Ad HocNetworks. Proceedings of the 4th IEEE Workshop on MobileComputing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE,Calicoon, NY, June 2002.

[9] Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru and HerbertRubens An On-Demand Secure Routing Protocol Resilent to ByzantineFailures In ACM Workshop on Wireless Security (WiSe), Atlanta,Georgia, September 28 2002.

[10] PietroMichiardi, RefikMolva Core: A Collaborative Reputationmechanism to enforrce node cooperation in Mobile Ad Hoc Networks inCommunication and Multimedia Security 2002 Conference.

[11] Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. Mitigatingrouting misbehavior in mobile ad hoc networks. Mobile Computing andNetworking (2000).

[12] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA.

[13] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis ofthe CONFIDANT Protocol: Cooperation Of Nodes - Fairness InDistributed Ad-hoc NeTworks In Proceedings of IEEE/ACM Workshopon Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne,CH, June 2002. IEEE.

[14] LeventeButtyan and Jean-Pierre Hubaux Enforcing Service Availabilityin Mobile Ad-Hoc WANs Proceedings of the IEEE/ACM Workshop onMobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA,USA, August 2000.

[15] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Packet Leashes: ADefense against Wormhole Attacks in Wireless Ad Hoc Networks.Proceedings of the Twenty-Second Annual Joint Conference of the IEEEComputer and Communications Societies.

[16] Janne Lundberg. Routing Security in Ad Hoc Networkshttp://citeseer.nj.nec.com/400961.html.

[17] P. Papadimitratos, Z.J. Haas, P. Samar The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routingprotocol-00.txt 2002-12-11.

[18] P. Papadimitratos, Z.J. Haas, P. Samar The Secure Routing Protocol (SRP) for Ad Hoc Networks. draft-papadimitratos-secure-routingprotocol-00.txt 2002-12-11.

[19] Sonja Buchegger& Jean-Yves Le Boudec. The Selfish Node: IncreasingRouting Security in Mobile Ad Hoc Networks. IBM Research ReportRR 3354 May 2001.

[20] Sonja Buchegger and Jean-Yves Le Boudec. Cooperative Routing inMobile Ad-hoc Networks: Current Efforts Against Malice andSelfishness In Lecture Notes on Informatics, Mobile Internet Workshop, Informatik 2002, Dortmund, Germany, October 2002. Springer.

[21] Stephen Carter and Alec Yasinsac, Secure Position Aided Ad hocRouting Protocol. Proceedings of the IASTED International Conferenceon Communications and Computer Networks (CCN02), Nov 3-4, 2002.