IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 52-60
www.iosrjournals.org

Survey on Security Issues and Secure Protocols for Manet

Indu Singh

***Abstract*:** *A **mobile ad-hoc network** (**MANET**) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. Besides the general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion. In MANET , any node may compromise the routing protocol functionality by disrupting the route discovery process .We present a route discovery protocol that mitigates the detrimental effects of such malicious behavior as to provide correct connectivity information . Here scheme guarantees that node initiating a route discovery will be able to identify and discard replies providing false topological information, or, avoid receiving them. For this basic route query broadcast that provides. Secure Routing we propose the Secure Routing Protocol (SRP) that is to be applied on extension of ZRP, DSR and IERP.*

Index Terms: *Ad hoc networks, security attacks, secure routing.*

I. INTRODUCTION

Ad-hoc networks are a new standard 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 other nodes 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. The following flowchart depicts the working of any general ad-hoc network.

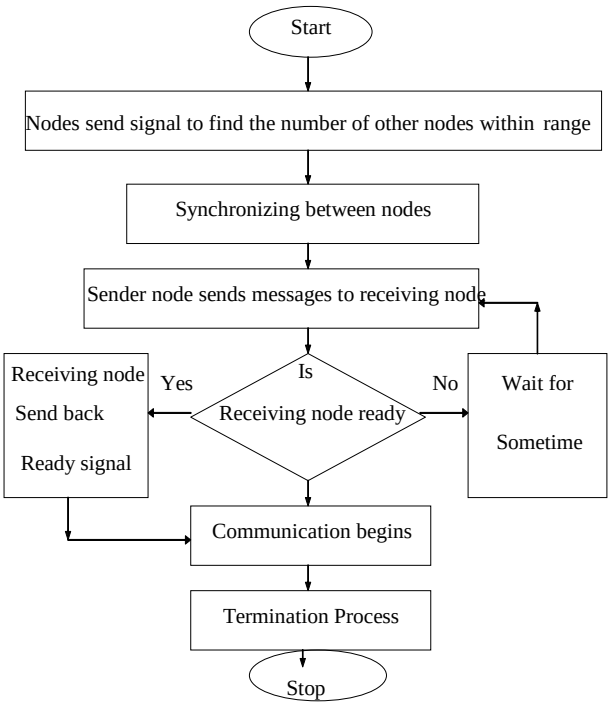


Figure 1: Working of a general Ad-Hoc Network

There are two different types of wireless networks:

- The 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.

This being said, we can now concentrate on the security aspect of the ad-hoc network. 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 described above.

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. 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 above security mechanisms must be implemented in any ad-hoc networks so as to ensure the security of the transmissions along that network. Thus whenever considering any security issues with respect to a network, we always need to ensure that the above mentioned 5 security goals have been put into effect and none (most) of them are flawed.

Contemporary Routing Protocols for ad-hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocol captures the common security threats and provides the guidelines to a secure routing scheme. Routers exchange network topology, informally, in order to establish routes between nodes and other networks which act as another potential target for malicious attackers. Broadly there are two major categories of attacks when considering any network *Attacks from external sources* and a*ttacks from within the network.* The second attack is more severe and detection and correction is difficult. Routing protocol should be able to secure themselves against both of these attacks.

Malicious vs. selfish behavior: As there is no infrastructure in mobile ad-hoc networks, the nodes have to cooperate in order to communicate. Intentional non-cooperation is mainly caused by two types of nodes: selfish ones that, e.g., want to save power, and malicious nodes that are not primarily concerned with power saving but that are interested in attacking the network.

II. TYPES OF AD-HOC ROUTING PROTOCOLS

Basically there are two types of routing protocols:

1. *Proactive Routing Protocols:* Herein the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and the Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF).
2. *Reactive or On Demand Routing Protocols:* Here the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV).

In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology. This is because in the AODV and DSR protocols, the route discovery packets are carried in clear text. Thus a malicious node can discover the network structure just by analyzing this kind of packets and may be able to determine the role of each node in the network. With all this information more serious attacks can be launched in order to disrupt network operations.

Types of Attacks Faced by Routing Protocols

Due to their underlined architecture, ad-hoc networks are more easily attacked than a wired network. The attacks prevalent on ad-hoc routing protocols can be broadly classified into passive and active attacks.

A *Passive Attack* does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Passive attacks basically involve obtaining vital routing information by sniffing about the network. Such attacks are usually difficult to detect and hence, defending against such attacks is complicated. Even if it is not possible to identify the exact location of a node, one may be able to discover information about the network topology, using these attacks.

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

We will now present a brief overview of 3 of the more prominent attacks prevalent against ad-hoc networks, most of which are active attacks.

1. Attacks based on modification

This is the simplest way for a malicious node to disturb the operations of an ad-hoc network. The only task the malicious node needs to perform, is to announce better routes (to reach other nodes or just a specific one) than the ones presently existing. This kind of attack is based on the modification of the metric value for a route or by altering control message fields. There are 3 ways in which this can be achieved:

- *Redirection by Changing the Route Sequence Number*: When deciding upon the best / optimum path to take through a network, the node always relies on a metric of values, such as hop count delays etc. The smaller that value, the more optimum the path. Hence, a simple way to attack a network is to change this value with a smaller number than the last "better" value.
- *Redirection by Altering the Hop Count:* This attack is more specific to the AODV protocol wherein the optimum path is chosen by the hop count metric. A malicious node can disturb the network by announcing the smallest hop count value to reach the compromised node. In general, an attacker would use a value zero to ensure to the smallest hop count.
  Taking for example the 'wormhole' attack, an attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the network. This could potentially lead to a situation where, it would not be possible to find routes longer than one or two hops, probably disrupting communication.
- *Denial of Service by Altering Routing Information:* Consider, in a bus topology, a scenario wherein a node A wants to communicate with node E. At node A the routing path in the header would be A-B-C-D-E. If B is a compromised 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 drop the packet. Thus, A will never be able to access any service / information from E.

Another instance can be seen when considering a category of attacks called 'The Black Hole Attacks'. Here, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Once the malicious node has been able to insert itself between the communicating nodes, it can do anything with the packets passing between them. It can then choose to drop the packets thereby creating a DoS.

2. Impersonation Attacks

More generally known as '*spoofing*', since the malicious node hides its' IP and or MAC address and uses that of another node. Since current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. Take for example a situation where in an attacker creates loops in the network to isolate a node from the remainder of the network. To do this, the attacker

needs to spoof the IP address of the node he wants to isolate from the network and then announce new route to the others nodes. By doing this, he can easily modify the network topology as he wants.

3. Attack 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 AODV and DSR, because these two protocols use path maintenance to recover the optimum path when nodes move. The weakness of this architecture is that whenever a node moves, the closest node sends an "error" message to the other nodes so as to inform them that a route is no longer accessible. If an attacker can cause a DoS attack by spoofing any node and sending error messages to the all other nodes. Thus, the malicious node can isolate any node quite easily.
- *Corrupting Routing State - Route Cache Poisoning:* A passive attack that can occur especially in DSR due to the promiscuous mode of updating routing tables which is employed. This occurs when information stored in routing tables is deleted, altered or injected with false information. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination. The vulnerability of this system is that an attacker could easily exploit this method of learning routes and poison route caches by broadcast a message with a spoofed IP address to other nodes. When they receive this message, the nodes would add this new route to their cache and would now communicate using the route to reach the malicious node.

Routing table overflow attack: Consider ad-hoc network is using a "proactive" protocol i.e. an algorithm which tries to find routing information even before it is needed. This creates vulnerabilities since the attacker can attempt to create routes to non-existent nodes. If enough routes are created, new routes can no longer be added due to an overwhelming pressure on the protocol.

After considering all the above plausible attacks we can draw a conclusion that we need to have a routing protocol that establishes routes without being susceptible to false information from any malicious node. A good routing protocol should also be able to detect the malicious nodes and to react in consequence, by changing routes, etc. A malicious node can however, be either a potential attacker or a regular node which encountered problems (low battery, etc.).

Insider Attacks:

Dr. Peng Ning and Kun Sun provide a comprehensive analysis of the insider attacks against MANET routing protocols . They identified the misuse goals an inside attacker may desire to achieve and further classify the misuses of the AODV protocol into two categories namely atomic misuses and compound misuses.

Misuse goals:

- Route Disruption (RD): Breaking down an existing route or preventing a new route from being established.
- Route Invasion (RI): Inside attacker adds itself between two endpoints of a communication channel.
- Node Isolation (NI): Preventing a node from communicating with any other node.
- Resource Consumption (RC): Consuming network bandwidth or storage space.

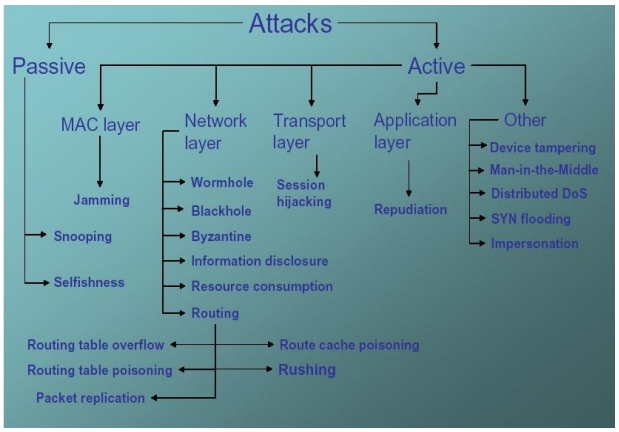
Rushing Attacks:

The rushing attack, a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Ariadne , ARAN, and SAOD], are unable to discover routes longer than two hops when subject to this attack.

In general terms, an attacker that can forward ROUTE REQUESTs more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes. This attack is also particularly damaging because it can be performed by a relatively weak attacker.

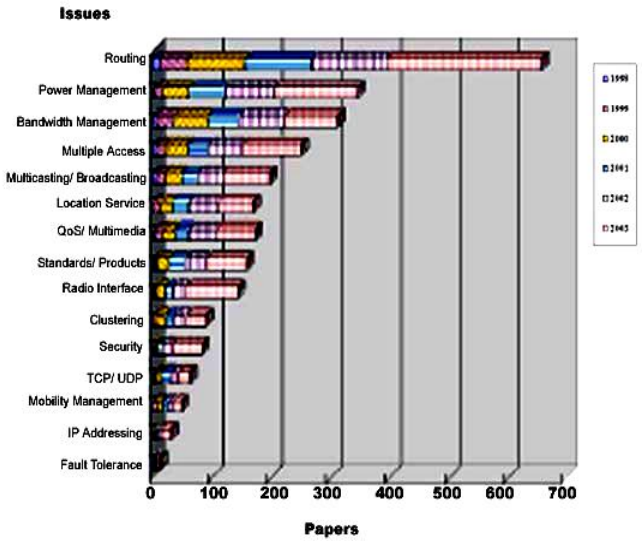
A Rushing Attack Prevention (RAP) is a generic defense against the rushing attack for on-demand protocols.[23] also identifies the threats to routing protocols of wired networks and wireless Ad Hoc networks and discusses the existing secure routing protocols, and point out their drawbacks and vulnerabilities.

III. ATTACKS ON MANET AND SURVEYS



Survey – 1

According to a survey* of more than 1300 MANET related papers in IEEE/ IEE Electronic Library (IEL online) from 1998 to 2003, some of the issues like routing and power management attracted much attention of the researchers. Figure showing the trends for various issues (grouped in 15 categories) over the six year (1998 to 2003).

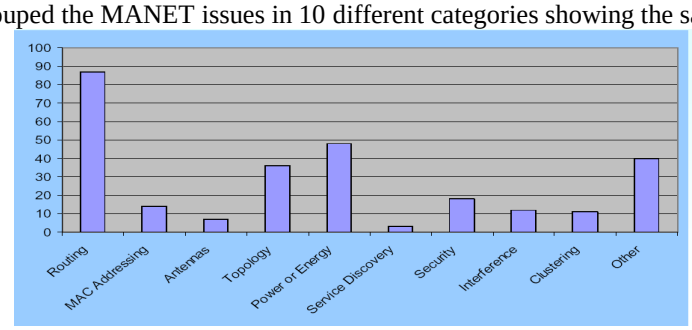


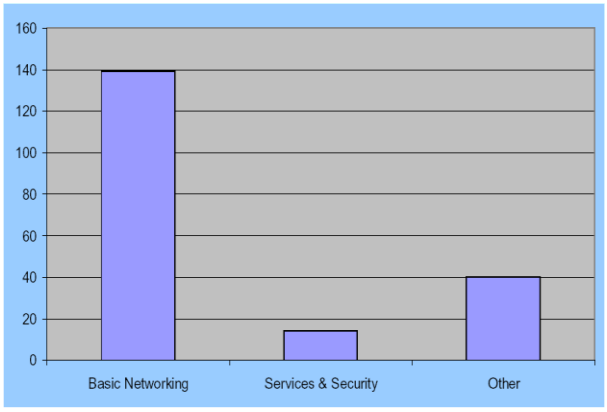
Conclusion – Survey 1

The Quantity of papers shows that the Routing, Power management and Bandwidth management are larger than the other issues While the IP addressing and fault tolerance issues are very few in quantity. These trends shows the maturity of some issues like routing and power management and the potential study value for IP addressing and fault tolerance. The growth rate for radio interface and the security are greater than the other issues. Similarly the issues of mobility management and fault tolerance are also positive. It shows that these issues have more potential study values in the near future.

Survey – 2

Another survey that grouped the MANET issues in 10 different categories showing the same trends as above.





Conclusion – Survey 2

In above Figure, it is very much clear that quantity of papers in the basic networking issue is very high that shows the maturity and the research undergoing on that issue. Analysis also showing that the service and security issue require more attention of the researchers i.e. this issue has more study potential in the future.

Major Issues

Routing	Fault Tolerance
IP and MAC Addressing	QoS and Reliability
Multicasting/ Broadcasting	Mobility Management
Clustering	Multiple Access
Topology	Location Services
Bandwidth Management	TCP/ UDP
Power Management	Radio Interface
Security	Standards/ Products

Table 1. Operational requirements of the surveyed secure ad hoc routing solutions.

Proposed Solution	**Requirements**
ARAN	Online trusted certification authority. Each node knows *a priori* the public key of the CA.
SAR	Key distribution or secret sharing mechanism.
SRP	Existence of a security association between each source and destination node. Malicious nodes do not collude within one step of the protocol process.
SEAD	Clock synchronization, or a shared secret between each pair of nodes.
Ariadne	Clock synchronization and the existence of a shared secret between each pair of nodes. Also, an authentic TESLA key for each node in the network and an authentic route discovery chain element for each node for which this node will forward route requests. TESLA keys are distributed to the participating nodes via an online key distribution center.
SAODV	Online key management scheme for the acquisition and verification of public keys.
TIARA	Online public key infrastructure.
On-demand Secure Routing Protocol Resilient to Byzantine Failures	Online public key infrastructure and shared symmetric keys between source and probe nodes.
SLSP	Nodes must have their public keys certified by a TTP. No collusion between malicious nodes.
BISS	The target node of a route discovery must share secret keys with all the intermediate nodes. An off-line trusted authority has certified the public keys of all the participating nodes.
Watchdog and Pathrater	No collusion between malicious nodes.
CONFIDANT	Nodes cannot change their identifier

Requirements and Assumptions

The surveyed protocols base their proposed solutions to the problem of secure ad hoc routing on certain assumptions and operational requirements. Table 1 summarizes the results of the comparison regarding this aspect and forms a basis for the discussion in this section.

Ad hoc Routing Parameters

This section summarizes the routing approaches utilized by the presented protocols. Most of the security solutions for ad hoc routing are based on existing ad hoc routing protocols. These underlying protocols introduce parameters that must be taken into account. The complete set of these parameters is presented in Table 2.

Table 2. Ad hoc routing parameters

. **Proposed Solution**	**Routing Approach**	**Loop Freedom**	**Shortest Path Identification**	**Intermediate Nodes Allowed to Reply to Route Requests**
ARAN	On-demand	Yes	Optional	No
SAR	On-demand	Depends on the basis protocol	No	No
SRP	On-demand	Yes	No	Optional
SEAD	Table-driven	Yes	No	No
Ariadne	On-demand	Yes	No	No
SAODV	On-demand	Yes	No	Optional
TIARA	On-demand1	Depends on the basis protocol	Depends on the basis protocol	Depends on the basis protocol
OSRP2	On-demand	Yes	No	No
SLSP	Table-driven	Yes	No	No
BISS	On-demand	Yes	No	No
Watchdog and Pathrater	On-demand	Yes	Depends4	Yes
CONFIDANT	On-demand	Yes	Depends4	Yes
Packet Leashes	NA5	NA5	NA5	NA5
IPsec	NA5	NA5	NA5	NA5

1 Can also be applied on table-driven protocols, but this requires extensive modifications.
2 On-demand Secure Routing Protocol Resilient to Byzantine Failures.
3 The routing metric is distance if no reliability information has been collected.
4 On whether reliability information has been collected for the path in question.
5 Depends on the utilized underlying ad hoc routing protocol.

Security Analysis In this section we present a security analysis regarding the behavior of the surveyed protocols and their applicability in mobile ad hoc environments. Ideally, a secure ad hoc routing protocol should be able to provide protection against all the categories of attacks. In reality, given the highly dynamic nature of ad hoc networks and the different scenarios of their application, for example utilizing some infrastructure or being completely infrastructure less, it is difficult to design a general solution that can provide adequate protection against all kinds of attacks in all possible application scenarios, with acceptable requirements and overhead. Table 3 provides a comparison of the surveyed secure routing solutions in respect to the different attacks.

Route Discovery

The problem of securing the process of route discovery has been approached differently by the studied protocols. The basic requirement for secure route discovery in on-demand protocols is that the destination of a *route request* packet must be able to authenticate the path, or paths, included in the packet in order to utilize legitimate and not ones that are fabricated by malicious nodes for sending a *route reply*. Accordingly, the initiator must be able to authenticate all the nodes that are included in the received reply.

Ariadne uses *per-hop hashing* to verify that no node was removed from a request by using one-way hash functions. As we have seen, the authentication is performed by using the released TESLA key. ARAN, which also works in an on-demand mode, assumes that each node has a certificate issued by a universally trusted third party (TTP) that binds its IP address with its public key. Route discovery packets are broadcasted and each node

checks the signature of all previous nodes, removes the last forwarder's signature and certificate, signs it with its own private key and attaches its own certificate. The target node replies with a route reply packet that is unicasted back to the initiator using the same method. We have identified two problems with ARAN. The first concerns mobility and address reconfiguration. As the node's owner moves across different authority domains and networks the node's address changes

IV. CONCLUSION

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. Self-organization is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. Latency is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. Multiple paths are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

Besides authentication, confidentiality, integrity, availability, access control, and non repudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion.

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior; preventing someone else from getting proper service, extracting data to get confidential information, and so on. Routes should be advertised and set up adhering to the routing protocol chosen and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network. We have discussed the various routing and forwarding attacks in this survey.

We have also discussed prevention and detection mechanisms that were adopted to provide security in ad hoc networks. A prevention-only strategy will only work if the prevention mechanisms are perfect; otherwise, someone will find out how to get around them. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. In view of this reality, detection and response are essential. In this paper we discussed proposals representing all of these classes.

Even though prevention works as the first line of defense, it is not sufficient in addressing all the security threats. Hence we suggest an integrated layered framework which adopts the prevention techniques for the first level and detection techniques can be used at the second level complementing the protection techniques.

References

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

[2]. L. Zhou and Z. Haas, Securing ad hoc networks," IEEE Network Magazine, 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. A Secure Routing Protocol for Ad Hoc Networks In Proceedings of the 10 Conference on Network Protocols (ICNP), November 2002.

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

[6]. Panagiotis Papadimitratos and Zygmunt J. Haas Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

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

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

[9]. Pietro Michiardi, Refik Molva Core: A Collaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security 2002 Conference

[10]. Sergio Marti and T. J. Giuli and Kevin Lai and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking (2000):

[11]. 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

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

[13]. Levente Buttyan and Jean-Pierre Hubaux Enforcing Service Availability in Mobile Ad-Hoc WANs Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000

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

[15]. Janne Lundberg. Routing Security in Ad Hoc Networks http://citeseer.nj.nec.com/400961.html

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

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

[18]. Sonja Buchegger & Jean-Yves Le Boudec. The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks. IBM Research Report RR 3354, May 2001.

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

[20]. Stephen Carter and Alec Yasinsac, Secure Position Aided Ad hoc Routing Protocol. Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), Nov 3-4, 2002.

[21]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Efficient Security Mechanisms for Routing Protocols. Proceedings of the Tenth Annual Network and Distributed System Security Symposium (NDSS 2003), ISOC, San Diego, CA, February 2003, to appear.

[22]. Yih-Chun Hu, Adrian Perrig, and David Johnson Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols ACM Workshop on Wireless Security (WiSe 2003) September 19, 2003 Westin Horton Plaza Hotel, San Diego, California, U.S.A.

[23]. Huaizhi Li and Zhenliu Chen and Xiangyang Qin and Chengdong Li and Hui Tan Secure Routing in Wired Networks and Wireless Ad Hoc Networks

[24]. How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols Peng Ning and Kun Sun Computer Science Department, North Carolina State University

.