IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

Security Issues Pertaining to Ad-Hoc Networks - A Survey

Rishu Bhatia [1], Deepak Gupta [2], Shankar Kumar Vijay [3]

[1]Assistant Professor, GITAM, Kablana, Haryana
rishubhatia8725@gmail.com

[2]M.Tech. Scholar,S.B.M.N. , Rohtak , Haryana [2]
er_dgupta@yahoo.co.in

[3]M.Tech. Scholar, ITM , Bhilwara, Rajasthan [3]
shivankvijay07@gmail.com

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. MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load). 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 this paper we attempt to analyze threats faced by the ad hoc network environment and provide a classification of the various security mechanisms. We analyzed the respective strengths and vulnerabilities of the existing routing protocols and suggest a broad and comprehensive framework that can provide a tangible solution.

Keywords: *MANET, Security issues, Routing Protocols.*

I. INTRODUCTION

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 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.

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.

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

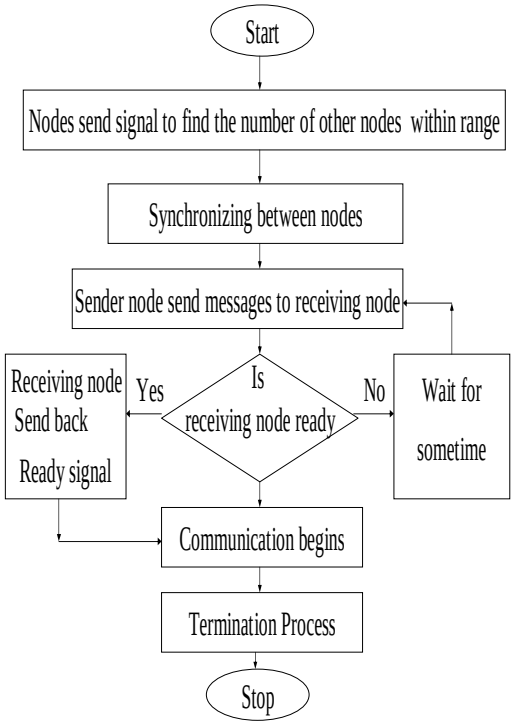

Figure 1: Working of a general Ad-Hoc Network

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. 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. SECURITY ISSUES CONCERNING ROUTING PROTOCOLS

The contemporary routing protocols for ad-hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. Today's routing algorithms are not able to thwart common security threats. Most of the existing ad hoc routing protocols

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

do not accommodate any security and are highly vulnerable to attacks.

Routers exchange network topology informally in order to establish routes between nodes - another potential target for malicious attackers who intend to bring down the network. External attackers inject erroneous routing information, replaying old routing information or distort routing information in order to partition 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 since compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is also difficult due to the dynamic topology of ad-hoc networks.

In mobile ad-hoc networks, nodes do not rely on any routing infrastructure but relay packets for each other. Thus communication in mobile ad-hoc networks functions properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate, for example to save power or to launch security attacks such as denial-of-service. In this paper, we give an overview of potential vulnerabilities and security requirements of mobile ad-hoc networks, and proposed prevention, detection and reaction mechanisms to thwart attacks.

A. Types of Ad-Hoc Routing Protocols

Basically there are two types of routing protocols:

- *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).
- *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.

B. 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

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

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

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

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 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:

IT is 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 SAODV, 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. 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. CLASSIFICATION OF TECHNIQUES USED TO SECURE AD-HOC NETWORKS

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

- Prevention
- Detection and Reaction

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals.

Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network. Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. A node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish or malicious. An overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets. A selfish node is unwilling to spend battery life, CPU cycles or available network bandwidth to forward packets not of direct interest to it, even though it expects others to forward packets on its behalf. A malicious node launches a denial of service attack by dropping packets. All protocols defined in this category detect and react to such misbehavior.

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

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

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

A.(a) Prevention using asymmetric cryptography

Asymmetric cryptographic techniques specify the underlined basic methodology of operation for protocols under this category. A secure wired networks or a similar network is required to distribute public keys or digital certificates in the ad-hoc network. Mathematically speaking a network with n nodes would require n public keys stored in the network. SAODV (an extension to AODV routing protocol) and ARAN are two of the protocols defined in this category.

A.(b) Prevention using symmetric cryptography

Symmetric cryptographic techniques are used to avoid attacks on routing protocols in this section. We assume that symmetric keys are pre-negotiated via a secured wired connection. Taking a mathematical approach we see that a network with 'n' nodes would require n * (n + 1) / 2 pair wise keys stored in the network. SAR and SRP are the two protocols that belong to this category.

A.(c) Prevention using one-way hash chains

This category defines a one-way hash chain to prevent attacks on routing protocols. They protect modification of routing information such as metric, sequence number and source route. SEAD and Ariadne fall into this category.

B. Detection and Reaction

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. All protocols in this category are designed such that they are able to detect malicious activates and react to the threat as needed. Byzantine , CONFIDANT , DSR, CORE and a protocol that uses Watchdog and Pathrater are the few protocols specified in this section.

IV. DESCRIPTION OF THE CLASSIFICATION

A.(a) Prevention using Asymmetric Cryptography:

Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV) adds security to the famous AODV protocol. Its basic functionality lies in securing the ADOV protocol by authenticating the non-mutable fields of the routing message using digital signatures.
It also provides an end-to-end authentication and node-to-node verification of these messages. The underlined process is relatively simple. The source node digitally signs the route request packet (RREQ) and broadcasts it to its neighbors. When an intermediate node receives a RREQ message, it first verifies the signature before creating or updating a reverse route to its predecessor. It then stores or updates the route only if the signature is verified. A similar procedure is followed for the route reply packet (RREP). As an optimization, intermediate nodes can reply with RREP messages, if they have a "fresh enough" route to the destination. Since the intermediate node will have to digitally sign the RREP message as if it came from the destination, it uses the double signature extension described in this protocol.

The only mutable field in SAODV messages is the hop-count value. In order to prevent wormhole attacks this protocol computes a hash of the hop count field.

Authenticated Routing for Ad-hoc Networks (ARAN) is an on-demand routing protocol that makes use of cryptographic certificates to offer routing security. Its main usage is seen in managed-open environments. It consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication.

This protocol requires the use of a trusted certificate server T, whose public key is known to all the nodes in the network. End-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet. The RDP packet contains a nonce and timestamp to prevent replay attacks and to detect looping. Similarly, each node along the reverse path (destination to source) signs the REP and appends its own certificate before forwarding the REP to the next hop.

Although hashing the hop-count value prevents malicious nodes in advertising shorter routes in SAODV, it does not prevent nodes from advertising longer routes. Nodes can forward routing messages by applying the hash function multiple times making the route appear longer than it is.

One of the main issues with the ARAN protocol is the requirement of a certificate server, which means that the integrity of that server is vital. This is by however, only a design issue and as it is intended for securing communication over a managed-open environment it shouldn't be considered a big issue.

Both the protocols in this category do not address wormhole attacks. While ARAN provides both node-to-node and end-to-end authentication, it does not have any significant gain over SAODV (that uses only end-to-end authentication) in terms of security.

A.(b) Prevention using Symmetric Cryptography:

Security-Aware ad hoc Routing (SAR) an attempt to use traditional shared symmetric key encryption in order to provide a higher level of security in ad-hoc networks. SAR can basically extend any of the current ad-hoc routing protocols without any major issues.
The SAR protocol makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Although current routing protocols discover the shortest path between two nodes, SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key). The different trust levels are implemented using shared symmetric keys. In order for a node to forward or receive a packet it first has to decrypt it and therefore it needs the required key. Any nodes not on the requested trust level will not have the key and cannot forward or read the packets Every node sending a packet decides what trust level to use for the transfer and thereby decides the trust level required by every node that will forward the packet to its final destination.

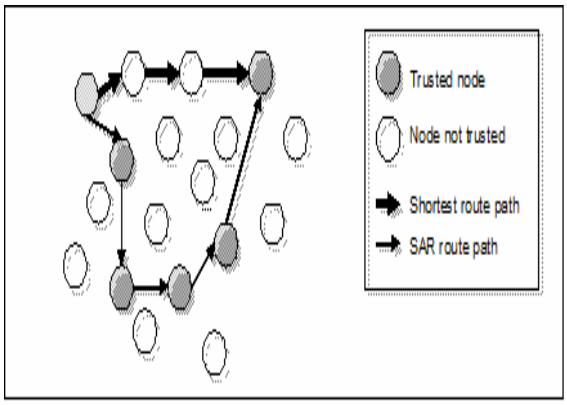

Figure 2: Variation of shortest path route selection between SAR and other routing algorithms

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

- Nothing is done to prevent intervention of a possibly malicious node from being used for routing, as long as they have the required key
- If a malicious node somehow retrieves the required key the protocol has no further security measure to prevent against the attacker from bringing the entire network to a standstill.
- There is excessive encryption and decryption required at each hop. Since we are dealing with mobile environments the extra processing leading to increased power consumption can be a problem.

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

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

Secure Routing Protocol (SRP) is another protocol extension that can be applied to any of the most commonly used protocols today. The basic idea of SRP is to set up a security association (SA) between the source and the destination node. An SA is a secret-key scheme used to preserve integrity in the routing information. The SA is usually set up by negotiating a shared key based on the other party's public key, and after that the key can be used to encrypt and decrypt the messages. The routing path is always sent along with the packets, unencrypted though (since none of the intermediate nodes have knowledge of the shared key).

The above features are achieved with low computational cost and bit overhead. In addition, the protocol is practically immune to IP spoofing and implements partial caching without compromising security in the network. More than one RREQ packet reaches the destination through different routes. The destination calculates a MAC covering the RREP contents and then returns the packet to the source over the reverse route accumulated in the respective RREQ packet. The destination responds to one or more route request packets to provide the source with an as diverse topology picture as possible.

A sample working of the protocol follows:

The source node (S) initiates the route discovery by constructing a route request packet. The route request packet is identified by a random query identifier (rnd#) and a sequence number (sq#). We assume that a security association (a shared key K_{ST}) is established between source (S) and destination (T).

S constructs a MAC such that, MAC = h(S, T, rnd#, sq#, K_{ST}). In addition the IP addresses of the traversed intermediate nodes are accumulated in the route request packet.

Intermediate nodes relay route requests. The intermediate nodes also maintain a limited amount of state information regarding relayed queries (by storing their random sequence number), so that previously seen route requests are discarded.

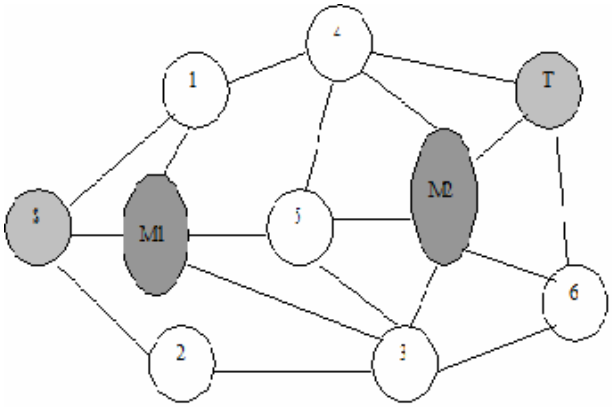

Figure 3: Sample working of SRP

More than one route request packet reaches the destination through different routes. The destination T calculates a MAC covering the route reply contents and then returns the packet to S over the reverse route accumulated in the respective request packet. The destination responds to one or more route request packets to provide the source with an as diverse topology picture as possible.

The evident failing, however, is that it exposes network infrastructure information to potential attackers. In fact one of the main security issues in SRP is that it has no defense against the "invisible node" attack that simply puts itself (and possibly a large number of other invisible nodes) somewhere along the message path without adding itself to the path, thereby causing potentially big problems as far as routing goes.

A.(c) Prevention using One-Way Hash Chains:

SEAD

The main objective of the protocol is to avoid any malicious node from falsely advertising a better route or tamper the sequence number in the packet that it received from the source. They basically implement features to protect modification of routing information such as metric, sequence number and source route.

SEAD uses a one-way hash chains for authenticating the metric and the sequence number. Each node creates a one-way hash chain and uses the elements in groups of 'm' (given m as the diameter of the network) for each sequence number. Each node uses a specific single next element from its hash chain in

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

each routing update that it sends about itself (metric 0). The upper bound of the network is denoted by (m-1).

An entry is authenticated by using the sequence number in that entry to determine a contiguous group of m elements from that destination node's hash chain, one element of which must be used to authenticate that routing update. The one-way nature of hash chains prevents any node from advertising a route with a greater sequence number than the source's sequence number.

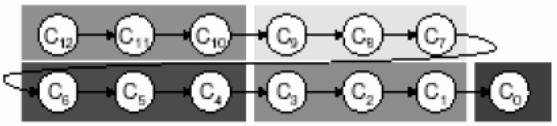

Figure 4: Hash chains in SEAD

To avoid routing loops the source of each routing update message must be authenticated. This protocol requires pair wise shared secret keys or broadcast authentication such as TESLA, HORS or TIK to authenticate neighbors.

Ariadne

The ARIADNE protocol relies only on highly efficient symmetric cryptography. The protocol primarily discusses the use of a broadcast authentication protocol namely TESLA, because of its efficiency and requires low synchronization time rather than the high key setup overhead of using pair-wise shared keys. Other authentication protocols such as BiBa are / can also be used for this purpose.

This proposal is an on-demand routing protocol. The design of Ariadne can be viewed as a 3 step process:

1. Authentication of RREQ by target: To convince the target of the legitimacy of each field in a RREQ, the initiator includes a MAC computed with a shared key over a timestamp.

2. Mechanisms for authenticating data in RREQ and RREP: The scheme allows the initiator to authenticate each individual node in the node list of the RREP. The target can authenticate each node in the node list of the RREQ, so that it will return RREP only along paths that contain legitimate nodes. 3 alternative techniques are available to achieve the node list authentication. These are the TESLA protocol, Digital Signatures and standard MAC. Out of these TESLA is the most widely used due to its inexpensive requirements.

3. Per-hop hashing technique: A one-way hash function is used to avoid a node from being removed from the node list in the RREQ message. The source initializes the hash chain to a MAC with a key shared between the source and target. When an intermediate node receives the request, it appends its identifier to the hash chain and rehashes it. The target verifies each hop of the path by comparing the received hash and the computed hash of the MAC. To change or remove a previous hop, the attacker must be able to invert the one-way hash function, which has been proved computationally infeasible

B. Detection and Reaction: For **Byzantine Failures**

It describes an on demand routing protocol that incorporates detection mechanism into its algorithm and attempts to survive under an adversarial network failures which include modification/fabrication of packets, dropping packets, among others, caused by selfish or malicious nodes, collectively known as Byzantine failures.

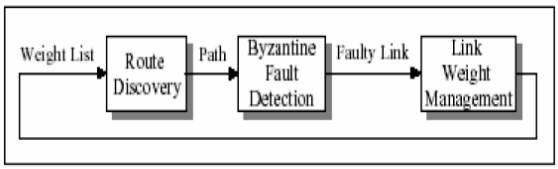

Figure 5: Hash chains in SEAD

The above figure depicts the 3 phases of the Byzantine algorithm, i.e. Link Weight Management, Route Discovery with Fault Avoidance, and Byzantine Fault Detection.

A general working schema follows:

Each node maintains reliability metrics based on the past history in the link weight management phase. During the route discovery phase, faulty paths (higher weights) are avoided by choosing alternate available paths. The Byzantine fault detection algorithm presented is an 'adaptive probing technique' that detects a malicious link after log n faults have occurred, where n is the length of the path. In the absence of malicious nodes, the algorithm has very little overheads for the

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

authentication of RREQ. However is there does exist some malicious links, they will trigger the fault detection technique, which involves overheads in terms of the encryption needed, and can detect the faulty link after log n faults.

- *Detection and Reaction:* **Core**

CORE suggests a generic mechanism to enforce node cooperation based on a collaborative monitoring technique. It can be integrated with any network and application layer function that can include packet forwarding, route discovery, network management, location management, among others. It proposes a reputation based detection framework to tackle selfish behavior of nodes. All the services available from the network, such as forwarding, are treated as functions and reputation is calculated for each such function.

CORE defines three types of reputations, subjective, indirect and functional. Each node maintains a watchdog component and a reputation table for every function with entries for other nodes in the network. Subjective reputation is based on the observed behavior of the neighboring nodes. Indirect reputation is calculated from information from other nodes. Functional reputation is a global value obtained by assigning different weights to different functions. Based on these factors, a persistent non-cooperative behavior by any node will lead to its exclusion from the network.

- *Detection and Reaction:* **Confidant**

Confidant attempts to detect and isolate misbehaving nodes(or nodes with grudges) in an ad-hoc network, thus making it unattractive to deny cooperation and participation. Trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes. The protocol has been described using Dynamic Source Routing (DSR) in the network layer.

Each node consists of 4 basic components:

1. *The Monitor:* watches its neighbors for any malicious behavior. If such behavior is detected, the reputation system is invoked.
2. *The Reputation System:* manages a table consisting of entries for each node and its ratings. Ratings are changed according to a rate function that assigns different weights to the type of behavior detected.

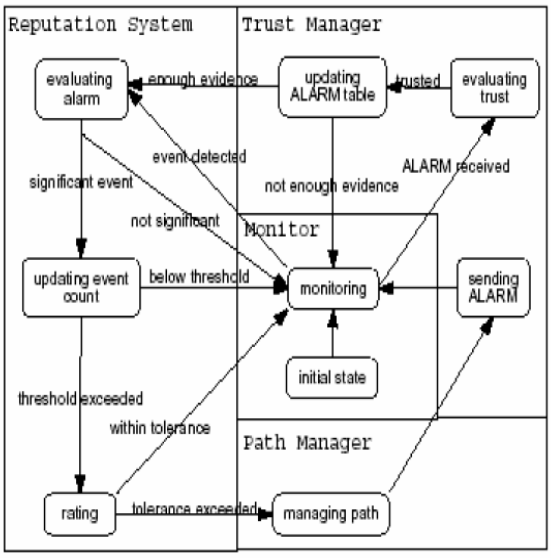

Figure 6: Trust architecture and FMS within each node of a Confidant

3. *The Trust Manager:* responsible for calculating trust levels of nodes and dealing with all incoming and outgoing alarm messages.
4. *The Path Manager:* manages all path information, i.e. adds, deletes or updates paths according to the feedback it receives from the reputation system

- *Detection and Reaction:* **Protocol Using Watchdog and Pathrater**

This proposal describes two techniques that improve throughput of an ad-hoc network in the presence of nodes that agree to forward packets but fail to do so do to some malicious activity. To mitigate this problem, the protocol proposes categorizing nodes based on their dynamically measured behavior. A watchdog is used to identify all misbehaving nodes while the parthrater avoids routing packets through these nodes. These act as upgrades / plug-ins and hence can be applied to existing protocols with minimal changes to the underlying routing algorithm.

A sample working follows:

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

When a node forwards a packet, the Watchdog verifies that the neighbor on the path also forwards the packet. This is done by listening to the transmissions of all neighbors. The watchdog then assign positive values to a node that forwards packets successfully and a negative value after a threshold level of misbehavior has been observed.

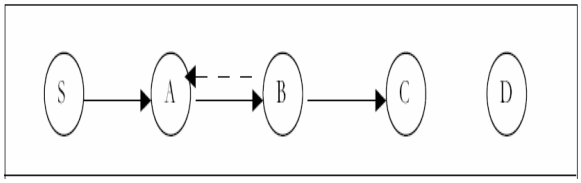

Figure 7: Operation performed by the Watchdog plug-in

The Pathrater uses this knowledge of the misbehaving nodes to choose the network path that is most likely to deliver packets. The decision is taken based on the average of the values obtained by the watchdog about each node in the path. In any reputation-based mechanism, detecting the propagation of positive ratings by colluding nodes is a challenging task. Further, if a node is unable to forward packets either due to overload or low transmission power, detection protocols assume misbehavior in such circumstances, resulting in false positives.

- *Approaches to thwart selfishness:*

addresses the problem of service availability in mobile ad-hoc WANs. A secure mechanism is studied to stimulate end users to keep their devices turned on, to refrain from overloading the network, and to thwart tampering aimed at converting the device into a ``selfish`` one. The mechanism is based on the application of a tamper resistant security module in each device and cryptographic protection of messages.

- *Position aided routing protocols:*

Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. These routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. Presents methods of protecting position information in MANET routing protocols, and ways to use the position information to enhance performance and security of MANET routing protocols. "Secure Position Aided Ad hoc Routing" (SPAAR), is a routing protocol designed to use protected position information to improve security, efficiency, and performance in MANET routing.

SPAAR uses position information to improve performance and security, while keeping position information protected from unauthorized nodes. For MANET routing protocols to achieve a high level of security, we allow nodes to only accept routing messages from one-hop neighbors. In SPAAR, with the aid of position information, a node may verify its one-hop neighbors before including them in the routing protocol. SPAAR requires that each device can determine its own location. GPS receivers are relatively inexpensive and lightweight, so it is reasonable to assume that all devices in our network are equipped with one.

V. EVOLVING TRENDS IN SECURE AD-HOC ROUTING

A. Routing Protocols:

Due to the resource limitations imposed in an ad hoc environment, reactive on demand routing approaches like AODV are preferred to the proactive routing protocols in order to conserve the resources of the nodes. Then security features were incorporated into those protocols (such as SAODV) which use asymmetric cryptography for authentication to address security issues. Authentication has been achieved using either node-to-node (SAODV) or end-to-end (ARIADNE) techniques. SAR provides a different direction by incorporating security itself as a metric. SEAD and its successor ARIADNE use one-way hash functions to prevent uncoordinated attackers from creating incorrect routing state in another node. ARIADNE also provides a method of broadcasting using TELSA. A new trend that has evolved makes use of a simple packet forwarding mechanism, instead of storing routing tables in devices. This mechanism uses a currency approach (nuggets), which thwarts selfish behavior in the network.

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

B. Intrusion:

(a)New architecture for Intrusion Detection Schemes (IDS):

IDS should be both distributed and cooperative to suit the needs of wireless ad-hoc networks. Every node in the wireless ad-hoc network should participate in intrusion detection. Each node is responsible for detecting intrusion locally and independently but neighboring nodes can form an association and collaboratively investigate in a broader range. Each node within the network has its own individual IDS agent and these agents run independently and monitor user and system activities as well as communication activities within the radio range. If an anomaly is detected in the local data or if the evidence is inconclusive, IDS agents on the neighboring nodes will cooperatively participate in a global intrusion detection scheme. These individual IDS agents constitute the IDS system to protect the wireless ad-hoc network

(b) Intrusion Response (IR):

The type of intrusion response depends on the type of intrusion, the type of network protocols and the confidence in the veracity of the audit trace data. The response might range from resetting the communication channels between nodes or identifying the compromised nodes and precluding them from the network. The IDS agent can notify the end user to do his/her own investigation and take the necessary action. It can also send re-authentication requests to all nodes on the network to prompt the respective end users to authenticate themselves. Only the re-authenticated nodes participate in negotiating a new communication channel and will recognize each other as legitimate nodes. Thus the malicious nodes can be precluded.

C. Anomaly detection:

(a) Detecting Abnormal Updates to Routing Tables:

A legitimate change in the routing table is caused by physical motion of the nodes or changes in the membership of the network. For a node, its physical movement from network to network and change in its own routing table are the only data entities it can trust and hence they are used as a basis for the trace. The physical movement is measured by distance, direction and velocity. The routing table change is measured by Percentage of changed routes (PCR), and the percentage change in the sum of hops of all routes (PCH). During the "training" process, a wide variety of normal situations is simulated and the corresponding trace data is gathered for each node. The audit/trace data of all the nodes in the network are then merged together to get a set of all normal changes to the routing table for all nodes. The normal profile specifies the correlation of the physical movement of the node and the changes in the routing table. The classification algorithm classifies available trace data into ranges. For a particular trace data, if the PCR value is beyond the valid range for a particular movement then it is considered to be an anomalous situation and the necessary procedures are initiated.

VI. 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.

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

IJCSMS International Journal of Computer Science and Management Studies, Vol. 12 Issue 01, January 2012
ISSN (Online): 2231-5268
www.ijcsms.com

behavior, nodes can attack the network. We have discussed the various routing and forwarding attacks in this survey.

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.

Open Problems: There are many open research challenges, because by definition mobile ad-hoc networks are self-organized and have no infrastructure and central authorities. Examples include self-organized key management, cooperation incentives, group-membership and access control, authentication and identity persistence, and trust management.

VII. 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 enforrce node cooperation in Mobile Ad Hoc Networks in Communication and Multimedia Security 2002 Conference

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