ISSN:0975-9646

Survey on Ad Hoc Wireless Networks And Routing Security issues

Prasuna V G1, Dr. S. Madhusudhana Verma2

1.MCA Department, Assistant Prof., Basaveswara Institute Of Information Technology, Hyderabad,AndhraPradesh,INDIA500027
2.HOD,Department of OR & SQC , Rayalaseema University, Kurnool, Andhra Pradesh, India. 518002

Abstract:

The outgrowth of the Ad Hoc networking technology urge self-organized wireless interconnection of devices that would either extend or operate in contrive by mutual agreement with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the a rapid increase in number of Ad Hoc based applications depends on a large number of factors, with the trait of deserving trust and confidence being one of the primary challenges to be met. Contempt the existence of well-known security mechanisms, additional vulnerabilities and features to the point to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the demand of cooperative network operation, since any node may limit the routing protocol functionality by interrupting or breakup the route discovery process. This survey paper discusses the past and most resent research carried out in "Ad hoc network's routing security"

.

Keywords : Ad hoc networks, Attcks, Routing , Security**.**

I. INTRODUCTION

Ad Hoc Wireless Networks

A wireless ad hoc network is a decentralized wireless network that gives a speedy, unhitched route to information and computing, removing the impediments of factors such as distance, time and location for a number of applications stretching from collaborative, distributed mobile computing to disaster recovery (such as earthquake, fire, flood etc), law enforcement (such as crowd control, search and rescue) and military communications (command, surveillance, control, and reconnaissance) [8]. Ad hoc networks consist of a set of wireless mobile hosts that collectively form a transitory network without the help of any organized infrastructure or integrated administration.

An ad hoc network lets every wireless device within the range of each other to ascertain and commune in peer-to-peer fashion without involving central access points (including those built in to broadband wireless routers) and to actively take part in data forwarding.

There are two ways in which communication can be transmitted – if communication is between two nodes, then, it can be performed directly if the end-point is in the sender's transmission range otherwise it can be performed by an intermediate node that acts as a router (multi-hop transmission) if the destination is outside the sender's transmission range. Some of the distinguishing features that set apart ad hoc wireless networks from other networks are:

1. Dynamic Network Topology: This is prompted by node mobility, nodes departing or unifying with the network, node disabled due to the lack of energy supply, etc. Nevertheless, network coupling should be maintained by employing particular network protocol functions so as to permit applications and services to function uninterruptedly.
2. Fluctuating Link Capacity: The effects of increased probability of bit and frame errors are more severe in wireless communication. The effects of these error rates are aggregated along the multihop paths. More than one back-to-back path can employ a given link in ad hoc wireless networks, and if this were to break, it could interrupt multiple sessions through the stage of high bit transmission rate.
3. Distributed Operations: This aspect is embedded in ad hoc networks. The protocols and algorithms planned for an ad hoc wireless network should be dispersed to facilitate the accommodation of a dynamic topology and an infrastructure-less architecture.
4. Restricted Energy Resources: Wireless devices are powered by batteries. Thus, there is a constraint of time when ad hoc network participants operate due to the changing or replenishing nature of their energy resources. Designing power optimization mechanisms are hence a vital element in all layers when designing algorithms and protocols. Ways to diminish energy consumption consist of (a) letting nodes enter a sleep state when data is not sent or received , (b) opting for routing paths that reduce energy consumption, (c) carefully selecting nodes as per their energy status, (d) create communication and data delivery arrangements

that curtail energy consumption, and (e) trim down networking overheads. Designing communication protocols in the ad hoc wireless networks is not easy because of the limited wireless transmission range, broadcast nature of the wireless medium (hidden terminal and exposed terminal problems), node mobility, inadequate power resources, and restricted physical security. The rewards of using an ad hoc wireless network comprise uncomplicated and swift deployment, robustness (no infrastructure required), adjustable and self-organizing network.

Security of routing protocols in ad hoc wireless network is an important concern for us because routing is a key operation that offers the communication protocol for data delivery involving wireless devices. Because the uniquely characterized ad hoc wireless networks, are greatly susceptible due to security threats, assuring a secure protocol is a challenging task indeed. Traditional routing protocol design does not concentrate on this specific issue and are based on reciprocated trust relationships between nodes

II. OVERVIEW OF ROUTING PROTOCOLS IN AD HOC WIRELESS NETWORKS

Routing is a significant operation in ad hoc wireless networks because they are the basis of data exchange between wireless devices [1]. Every individual wireless node acts as a router and contributes in the routing protocol. Implicit trust relationship among participating devices is the foundation on which routing depends. The central duty of routing is to exchange routing data, locate a viable path between source and destination based on several metrics, and path-maintenance. The primary requirements [17] of a routing protocol are:

(a) Minimum route acquisition delay.
(b) Quick route reconfiguration in the case of path breaks.
(c) loop-free routing.
(d) Distributed routing protocol.
(e) low control overhead.
(f) Scalability with network size.
(h) QoS support as demanded by the application.
(i) Support of time-sensitive traffic.
(j) security and privacy.

The unique characteristics of ad hoc wireless networks pose [17] a number of challenges. Node mobility influences network topology and could invite packet loss, path disconnection, network partition and hindrances in resource distribution. The three main factors that wireless nodes are constrained in general resource are battery power, memory and computing power. Wireless channel has a high bit error rate (10−5 to 10−3) vis-à-vis wired counterparts (10−12 to 10−9). Because wireless channel is shared by the nodes in the same broadcast area, the link bandwidth available per node is limited, and fluctuates with the number of nodes present in that area. The design of routing protocols must take these issues into concern. Routing protocols in ad hoc wireless networks can be classified as proactive (or table-driven) protocols, reactive (or on-demand) protocols, and hybrid routing protocols based on the routing information update mechanism. In the next three subsections we present essential attributes of each group with brief descriptions of a number of representative routing protocols.

1. Proactive Routing Protocols

In proactive routing protocols [1], information is periodically exchanged by nodes to manage the routing of consistent and accurate information. This updated information available in the routing table helps to compute the path rapidly, whenever a node has to transmit data to a destination. The drawback of utilizing a proactive protocol is high overhead required to sustain the latest routing information. In ad hoc wireless networks, node mobility triggers a dynamic topology that could require a great number of routing updates. This has an unconstructive influence on resource allotted to wireless devices, bandwidth usage, and throughput. The protocols in this category are extensions of the wired network routing protocols such as Destination Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP) , Optimized Links State Routing (OLSR) [3], etc.

The other distance vector protocols, DSDV protocol also finds shortest paths between nodes using a distributed Bellman-Ford algorithm. Each node maintains a routing table, with an entry for all possible destination in the network. For every entry, the following fields are maintained: the destination address, next hop on the shortest path to that destination, shortest known distance to this destination, and a destination sequence number that is produced by the destination itself. Each node periodically sends its routing table information to each of its neighbors in order to maintain an updated view of the network topology. Based on the routing information received from its neighbors, each node updates its routing table to reflect current status of the network.

Sequence numbers play an essential role in DSDV and are employed for checking loop formation. Every entry in the routing table has a sequence number. This is the most recent sequence number known for that destination, and is incorporated in the periodic routing updates. If an update with a lesser sequence number is received by a node, then that update is overlooked. A newly advertised path is adopted if it has a bigger sequence number, or if it has identical sequence number but a lower metric. In addition to the periodic updates, there are triggered updates, issued when important routing updates should be transmitted.

The node creates a routing update with the next odd sequence number and metric value of infinity when a broken link is

detected. Routing update messages can be incremental, when only information changed from the last full dump, is sent or full dump, when information for all destinations is sent.
The main benefit of using DSDV is that routes to each and every one of the destinations are available at all times without involving a route discovery process. The main drawback of DSDV is the high overhead as a result of the periodic routing updates.

2. Reactive Routing Protocols

In the reactive routing protocols, a route discovery mechanism is set off only when a node does not discern a path to a destination it wants to communicate with. In the case of mobile ad hoc network, reactive routing protocols have been shown to enhanced performance with considerably lower overheads than proactive routing protocols as they are able to respond promptly to the countless changes that may arise in node connectivity, and hitherto, are able to decrease (or eliminate) routing overhead in periods or areas of the network in which changes are less frequent.
A reactive routing protocol has two main operations, route discovery (broadcasting using a form of controlled flooding) and route maintenance. A range of reactive protocols have been proposed in literature such as Ad Hoc On-demand Distance Vector (AODV) [15] , Dynamic Source Routing (DSR) [8], Temporally Ordered Routing Algorithm (TORA) [18], etc.
Next, we present the main features of DSR [8] and AODV. DSR is a source routing protocol, and hence has the property that each data packet carries the source-destination path in its header. By making use of this information, intermediate nodes can establish which would be the next hop this packet should be forwarded to. Each node maintains a routing cache that consists of the routing information that the node learned from routing information forwarded or overheard. Every entry has a termination time following which the access is deleted with the intention of circumventing outdated information.
DSR executes route discovery by making the sender broadcast by flooding a Route Request packet. Each Route Request has a sequence number produced by the source node, in order to prevent loop formation and to evade multiple retransmissions by a node of the same Route Request packet. An intermediate node checks the sequence number, and appends its own identifier and forwards the Route Request only if this message is not duplicate.
On receiver side, upon receiving the Route Request, sends back a Route Reply packet along the reverse route recorded in Route Request. When the sender receives the Route Reply, it starts sending data to the receiver.
If a node detects a failure (e.g. broken link), it sends a Route Error message to the source as part of the route maintenance. Upon hearing the Route Error, all intermediate nodes update their routing cache and all routes that consist of this hop are truncated. The source has to re-initiate the path discovery mechanism if it does not have an alternative path to the destination.
There are several optimization techniques of DSR. To begin with, it permits intermediate nodes that know a path to the destination to reply to the Route Request message in place of forwarding the request. This accelerates the route discovery. Secondly, path discovery can apply an expanding ring search mechanism while sending the Route Request messages. This is particularly helpful for close destinations which prevent broadcasting in the entire network.

The advantages of DSR include:
(1) route maintenance applies just to active routes.
(2) route caching can speed up and reduce overhead of route discovery.
(3) a single route discovery might yield more routes to the destination when intermediate nodes reply from local caches.

The disadvantages of DSR are:
(1) Adding the source-destination path in each packet will create overhead, for long paths and small data.
(2) The flooding process used in route discovery is unpredictable, may initiate collisions, and contentions.
(3) Intermediate nodes may send Route Reply from stale routing caches, thus polluting other caches as well.

AODV [15] puts into operation similar main operations as the DSR. It discovers a path to a destination using a Route Request (RREQ) and Route Reply (RREP) sequence, and performs route maintenance for link failures by propagating a Route Error message to the source. AODV tries to develop on the DSR by maintaining routing tables at nodes, such that data packets do not have the source destination path. Each node maintains a routing table for each destination of interest, including the following fields: destination, next hop, number of hops, destination sequence number, and expiration time.
When a source node broadcasts a Route Request (RREQ) to discover a path to a destination, intermediate nodes that forward the message set up a reverse path, pointing toward the node from which the request was received. In this way, Route Reply (RREP) travels along the reverse paths set-up when Route Request was forwarded, without carrying the full path in the header. As a result of this, each node sets up forward links that are later used to forward data packets between the source and destination.
Whenever a source node sends a Route Request, it allocates a higher sequence number for that destination. Intermediate nodes are permitted to respond with Route Reply provided they identify a recent path to the destination (with the same

or higher sequence number). The reverse and forward paths are purged from the routing tables if they are not used within a specific time interval. The key advantages of AODV are: (1) paths are excluded and carried in the packet headers, (2) nodes keep routing tables with entries just for the active routes (if not used for specific time interval they are purged), and (3) AODV uses a destination sequence number mechanism to limit the chances of an intermediate node replying with stale information to a Route Request packet.

3. Hybrid Routing Protocols

A few ad hoc network routing protocols are hybrids of proactive and reactive mechanisms. Examples of hybrid routing protocols are Zone Routing Protocol (ZRP) [2], Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) [19], etc. ZRP [2] is a hybrid of proactive and reactive routing protocols. The network is partitioned into zones, where each zone is a r-hop neighborhood of a node. The intra-zone routing protocol is a proactive routing protocol, whereas the inter-zone routing protocol is a reactive routing protocol. By varying r, we can run the routing update control traffic. The node directly uses the proactive routing protocol and the information already available in routing tables when it wants to transmit data to a destination within the same zone. However, the source node border casts the RouteRequest (e.g. this message is forwarded by the border routers) until it reaches the destination zone if it wants to transmit the data to another zone. The border node of the destination zone then sends back a RouteReply message. Any node forwarding the RouteRequest appends its address to it. This information is used when sending RouteReply back to the source. In case a broken link is spotted, the path reconstruction can be performed locally, and then a path update be sent to the source. Alternatively, by getting the source to re-initiate the path discovery, the path reconstruction can be also done globally.

ZRP resourcefully investigate the characteristics of proactive and reactive proto- cols. It cuts down the control overhead by maintaining the proactive protocols limits within zones, and decreases the flooding drawbacks by positioning the reactive protocol and bordercast mechanism only between the zones. The zone radius r should be specifically given particular attention as it can drastically affect the routing performance.

4. Broadcasting in Ad Hoc Wireless Networks

Broadcasting refers to the operation of sending a message to all other hosts in the network. Network wide broadcasting in ad-hoc wireless networks provides important control and route establishment functionality for a number of unicast and multicast protocols. Broadcasting is used for the route discovery in reactive routing protocols. In broadcasting, a source node sends the same message to all the nodes in the network. Broadcasting, in a mobile environment is a frequently used approach as nodes mobility could trigger path disconnection and therefore, discovery is summoned as part of the path maintenance procedure. Broadcasting operation exhibit the following features [20]: (1) the broadcast is unprompted, which implies that each node can commence broadcasting at anytime, and (2) broadcasting is undependable. No response packet is sent, for example, in IEEE 802.11 by a node after receiving a broadcast message.

One clear-cut process that is used to implement broadcasting is via a form of controlled flooding. In this technique, each node retransmits a broadcast message when it receives it for the first time. Transmitting a broadcast through flooding in a CSMA/CA network triggers several issues, generally referred to, as the broadcast storm problem [20]:

1. Redundant Rebroadcast. This occurs when a node sends a broadcast message that has previously been sent and all its neighbors have already received the message from some other neighbors.
2. Contention. This happens when neighboring transmission nodes get the message at nearly the same time, and when they re-send the message, they compete for the wireless communication.
3. Collision. They are expected to occur because of back-off mechanism deficiency and the lack of RTS/CTS dialogue. For example, when more neighbors simultaneously retransmit a freshly received message.

Several propositions [20] have been put forth to assuage the broadcast storm problem, by limiting the cases when a node rebroadcasts a message:

(1) probabilistic scheme, when each node rebroadcasts a message with a specific probability.
(2) counter-based scheme, when a node retransmits a message if it was received less than a threshold number of times over a fixed interval.
(3) distance-based scheme, when a message is resent only if it is received from neighbors farther away than a specific threshold distance.
(4) location- based scheme, when a node retransmits a message only if the additional area covered is larger than a specific threshold area.

An added suggestion expounds numerous local and deterministic schemes, where a subset of nodes, called forward nodes, are chosen locally while ensuring broadcast coverage. One such scheme, suggest that each node decides its own forwarding status, while another scheme suggests that the status of each node is to be determined by neighbors mutually.

III. SECURITY SERVICES AND CHALLENGES IN AD HOC WIRELESS NETWORKS

Many security services are needed so as to guarantee a consistent data transfer over the communication networks,

and to guard the system resources. Security services have been categorized into five divisions based on their objectives: availability, confidentiality, authentication, integrity and non-repudiation.

• Availability: Availability indicates that the services demanded, like the bandwidth and connectivity are available in a timely manner despite the fact that there is the likelihood of a problem in the system. By dropping off packets and through resource depletion attacks, the availability of network can be tempered.

• Confidentiality: Confidentiality guarantees that the classified information in the network is in no way divulged to unauthorized entities. Confidentiality can be accomplished by making use of several encryption techniques so that analysis and understanding of the transmission can only be done by legitimate communicating nodes. The content disclosure attack and location disclosure attack discloses the contents of the transmitted message as well as the physical information about a particular node.

• Authenticity: Authenticity is a network service to establish a user's identity. Devoid of authentication, an attacker can pretend to be any node, and thus, gain control over the entire network.

• Integrity: Integrity ensures that information transmitted between the nodes has not been tempered in the process. Data can be tainted either purposely or inadvertently (e.g., through hardware glitches, or in case of ad hoc wireless connections, through interference).

• Non-Repudiation: Non-repudiation guarantees that the information originator cannot refute the information it has sent. This service is valuable for finding and separating compromised nodes in the network. Countless authentication and secure routing algorithms implemented in ad hoc networks depend on trust-based concepts. The fact that a message can be attributed to a particular node assists in making these algorithms highly protected.

Designing a secure ad hoc wireless networks communication is a difficult assignment as a result of :

(1) Insecure wireless communication links.

(2) Absence of a fixed infrastructure.

(3) Resource constraints (e.g. battery power, bandwidth, memory, CPU processing capacity).

(4) Node mobility that triggers a dynamic network topology.

A huge number of conventional routing protocols designs are [17] unsuccessful in providing security. The most important requirements of a secure routing protocol are: (1) discovery of malicious nodes that are to be circumvented in the routing process, (2) guarantee of correct route discovery, (3) confidentiality of network topology; if an attacker learns the network topology, he can attack the bottleneck nodes, detected by studying the traffic patterns. This will give rise to disturbance in the routing process and DoS, and (4) strength against attacks; the routing protocol must be capable of resuming standard operations in a finite amount of time following an attack.

IV .VULNARABILITIES AND SECURITY ATTACKS ON ROUTING PROTOCOLS IN AD HOC WIRELESS NETWORKS

1. Vulnerabilities

Operation in an ad hoc network introduces some new security problems in addition to the ones already present in fixed networks. Some new vulnerabilities include the following.

Easy theft of nodes. Many nodes are expected to be small in size and thus vulnerable to theft. From a routing perspective this means that a node may easily become compromised. Thus, a previously well-behaving node can unexpectedly become hostile.

Vulnerability to tampering. This difficulty is related to the problem of easy theft. It must not be trivial for example to recover private keys from the device. A less stringent version of tamper proofness is tamper evidence where it is only required that a tampered node can be distinguished from the rest.

Limited computational abilities. Nodes can be devices with limited computing power. This may exclude techniques such as frequent public key cryptography during normal operation. However, symmetric cryptography is likely to be feasible in authenticating or encrypting routing message exchanges.

Battery powered operation. Many devices in an ad hoc network are assumed to be battery powered. An attacker may attempt a denial-of-service attack by creating additional transmissions or expensive computations to be carried out by a node in an attempt to exhaust its batteries.

Transient nature of services and devices. Because an ad hoc network consists of nodes that may frequently move, the set of nodes that are connected to some particular ad hoc network frequently changes. This can create problems for example with key management if cryptography is used in the routing protocol.

2. Attacks:

A secure system can be established by evading attacks or by detecting them in a timely manner and by providing a mechanism to quickly recover from such attacks. Depending on whether the normal operation of the network is disrupted or not, attacks on ad hoc wireless networks can be classified as active and passive attacks.

1) Passive Attack: In passive attacks, an intruder spies on the data exchanged without changing it. The attacker does not instigate malicious actions keenly to deceive other hosts. The main purpose of the attacker is to get hold of information that is being transmitted, thus infringing on the message confidentiality. Because the activity of the network is undisrupted, these attackers are hard to identify. Powerful

encryption mechanism can ease the effect of these passive attackers by making difficult-to-read overheard packets.
2):Active Attack: In active attacks, an attacker actively participates in disturbing the standard operation of the network services. A malicious host can generate an active attack by altering packets or by setting up bogus information in the ad hoc network. It puzzles routing procedures
and corrupts network performance. Active attacks can be further categorized into internal and external attacks:
External Attacks are carried by nodes that are not a legitimate part of the network. Such attacks can be shielded from by using encryption, firewalls and source authentication. In external attacks, it is feasible to disrupt the communication of an organization from the parking lot in front of the company office.
Internal Attacks occur from compromised nodes that were earlier a legitimate part of the network. Since these challengers were previously a component of the ad hoc wireless network as authorized nodes, they are extremely persistent and complicated to identify when weighed against external attacks. A huge number of attacks have been detected in literature that affects the routing in ad hoc wireless networks.

2.1. Attacks using Impersonation

In impersonation attacks, as the name implies, an intruder presumes the characteristics and privileges of another node so as to use its resources or to agitate the normal network operation. An attacker node is able to achieve impersonation by feigning its identity. This can be achieved by changing its own IP or MAC address to that of some other legitimate node. Several resilient authentication methods can be adopted to impede attacks by impersonation.

- **Man-in-the-Middle Attack**

In this type of attack, a malicious node reads and probably alters the message that is communicated between two parties. The attacker can impersonate the receiver with regard to the sender, and the sender as regards the receiver, with none of them been aware that they have been attacked.

- **Sybil Attack**

In the Sybil attack, an attacker feigns multiple identities. A malicious node can act as if it were a larger number of nodes either by simply claiming false identities or by impersonating other nodes. There are three categories of Sybil attacks: direct/indirect communication, fabricated/stolen identity, and simultaneity. In direct communication, Sybil nodes directly communicate with legitimate nodes, while in indirect communication messages sent to Sybil nodes are routed all the way through malicious nodes. An attacker can built-up a new identity or it can just steal it after obliterating or briefly disabling the impersonated node. All Sybil identities can get simultaneously involved in the network or maybe cycled through.

2.2. Attacks using Modification

This attack disrupts normal routing function by having the attacker illegally modifying the content of the messages. Redirection by altering the route sequence number and redirection with modified hop count that can prompt the black hole attack are a few examples of such attacks.

Some other modification-based attacks are as follows:

- **Misrouting Attack**

In the misrouting attack, a non-legitimate node transmits data packet to an incorrect destination. This sort of attack is instigated by forwarding a data packet to the wrong next hop in the route to the destination or by modifying the final destination address of the data packet.

- **Detour Attack**

In this form of attack, the attacker appends many virtual nodes into a route at some point in the route discovery phase. Consequently, the traffic is redirected to other routes that seem to be smaller and could contain malicious nodes which might generate additional attacks. The attacking node can conserve energy in a detour attack since it need not forward packets to that destination on its own. This attack is particular to source routing protocols

- **Blackmail Attack**

Blackmail attack triggers misleading identification of a good node as a malicious node. In ad hoc wireless networks, nodes typically maintain information of perceived malicious nodes in a blacklist. An attacker can blackmail a good node and inform other nodes in the network to put in that node to their blacklists also, so as to avoid the victim node in future routes.

2.3. Attacks using Fabrication

In fabrication attacks, an intruder produces fallacious routing messages, such as routing updates and route error messages, with the purpose of disturbing network operations or to devour other node resources.
A number of fabrication messages are presented next:

- **Resource Consumption Attack**

In this attack, a malicious node intentionally attempts to expend the resources (e.g. battery power, bandwidth, etc.) of other nodes in the network. The attack can be exhibit itself in the form of superfluous route requests, route discovery, control messages, or by sending stale information. For example, in routing table overflow attack, a malicious node advertises routes to non-existent nodes, thus causing routing table overflow. By utilizing packet replication attack, an adversary uses up bandwidth and battery power of other nodes.

- **Routing Table Poisoning**

In this sort of attack, a malicious node transmits fake routing updates which ensues sub-optimal routing, network clogging, or network division.

- **Rushing Attack**

A malicious node in this attack tries to interfere with Route Request packets, modifying the node list, and speeding up its packet to the next node. In view of the fact that in on-demand routing protocol just one RouteRequest packet is forwarded, if the route requests forwarded by the attacker are the earliest to arrive at the target (destination), subsequently any route discovered by the route discovery mechanism will take in a path through the attacker.

- **Black Hole**

In this mode of attack, a malicious node promotes itself as having the shortest path to all nodes in the network. The attacker can cause DoS by dropping all the received packets.
The attacker can also keep a check and scrutinize the traffic to get the activity patterns of each node. The black hole often becomes the gateway of a man-in-the-middle attack.

- **Gray Hole**

Under this style of attack, an attacker drops all data packets but it allows the controlling of messages to route through it. Gray hole attacks are therefore, much more difficult to detect then blackhole attack due to this selective dropping.

2.4. Replay Attacks

In the replay attack method, an attacker retransmits data to produce an unauthorized effect. Examples of replay attacks are wormhole attack and tunneling attack.

- **Wormhole Attack**

In wormhole attacks, two compromised nodes are capable of communicating with one another through a private network connection. The attacker can execute a vertex cut of nodes in the network by recording a packet at one location in network, tunneling the packet to another location, and replaying it there.
The attacker has no need of key material as it only requires two transceivers and one high quality out-of-band channel. The wormhole can drop packets or it can selectively forward packets to avoid detection. It is chiefly hazardous against different network routing protocols wherein the nodes regard themselves as neighbor after hearing a packet transmission directly from some node.

- **Tunneling Attack**

In a tunneling attack [16], two or more nodes team up to swap encapsulated messages along existing data routes. For example, if a RouteRequest packet is encapsulated and sent between two attackers, the packet will not contain the path traveled between the two attackers. This would wrongly make the receiver construe that the path comprising the attackers is the shortest available path.

2.5. Denial of Service (DoS)

In the DoS attack [17], an attacker openly makes an effort to avert legitimate users from using system services. This mode of attack greatly effects system availability. An ad hoc wireless network is at a risk to DoS attacks considering its dynamic changing topology and distributed protocols.
Examples of DoS attacks include:

- **Consumption of Scarce Resources**

The attacker is in a position to use up important network resources such as bandwidth, memory and access points. Thus, the whole network is unavailable to users.

- **Destruction or Alteration of Configuration Information**

Here, the attacker tries to change or wreck the configuration data so that legitimate users are prevented from accessing the network. A network that is improperly configured will not have effective performance levels or may be inoperable as well.

V . SECURITY MECHANISMS AND SOLUTIONS FOR ROUTING PROTOCOLS IN AD HOC WIRELESS NETWORKS

Two of the most important factors for data integrity and user authentication is message encryption and digital signatures. Further, data encryption mechanism are of two types – symmetric and asymmetric (the public key) mechanisms. While the symmetric cryptosystems utilize the same key (secret key) for encryption and decryption of messages, an asymmetric cryptosystem makes use of one key (the public key) to encrypt messages and another key (the private key) to decrypt it.
These two keys are interrelated in such a manner that only the public key can be used to encrypt a message and only the corresponding private key can be used to decrypt the message. It is nearly impossible to figure out the private key even if the attacker comprises a public key.
Any code attached to an electronically transmitted message that uniquely identifies the sender is known as digital code. Digital signatures are key component of most authentication schemes. Digital signatures have to be completely non-forgeable in order to be highly effective. The process of creation and verification of a digital signature makes use of the hash functions.
An algorithm of a hash value (or hash result) of a standard length usually smaller than the message and unique to it is creates a digital representation or fingerprint. Any change to the message will generate a different hash result even when the same hash function is used. In the case of a secure hash function, also known as a one-way hash function, it is computationally infeasible to derive the original message from knowledge of its hash value.
The secrecy of a key in an ad hoc network is not an assurance of the integrity of the message. A

Message Authentication Code (MAC), which is a hashed representation of a message, is used for this purpose. It is impossible to compute the message that generated it even if MAC is known.
A MAC, which is a cryptographic checksum, is computed by the message initiator as a function of the secret key and the message being transmitted and it is appended to the message. Similarly, upon getting the message, the recipient re-computes the MAC. In case the MAC that was computed by the receiver matches the MAC received with the message, then the recipient is guaranteed of the fact that the message was not modified. Next, we present security mechanisms specifically tailored for specific routing mechanisms.

1. Secure Efficient Ad hoc Distance Vector (SEAD)

Secure Efficient Ad hoc Distance Vector (SEAD) [1] is a proactive routing protocol, based on the design of DSDV [15]. Besides the fields common with DSDV, such as destination, metric, next hop and sequence number, SEAD routing tables maintain a hash value for each entry, as described below.
This paper deals with routing updates protection - both periodic and triggered - by preventing an attacker to forge better metrics or sequence numbers in such update packets.
The key feature of the proposed security protocol is the use one-way hash chains, using an one way hash function H. Each node computes a list of hash values h0, h1, ・ ・ ・ , hn, where hi = H(hi−1) and $0 < i \leq n$, based on an initial random value h0.
The paper assumes the existence of a mechanism for distributing hn to all intended receivers. If a node knows H and a trusted value hn, then it can authenticate any other value hi, $0 < i \leq n$ by successively applying the hash function H and then comparing the result with hn.
To authenticate a route update, a node adds a hash value to each routing table entry. For a metric j and a sequence number i, the hash value hn−mi+j is used to authenticate the routing update entry for that sequence number, where m − 1 is the maximum network diameter.
An attacker is unable to advertise a route to the same destination with a greater sequence number, or with a better metric because he is not in a position to compute a hash value with a smaller index than the advertised value.
The prime advantage of SEAD is that it supplies a robust protocol against attackers who try to produce wrong or misleading routing state in other node by changing the sequence number or the routing metric. The main disadvantage of SEAD is that it cannot prevent an attacker from tampering next hop or destination field in a routing update and it cannot stop an attacker to utilize the same metric and sequence number which it has learnt from some recent update [1] message for transmitting a new routing update to a different destination.

2. ARIADNE

ARIADNE [4] is an effective on-demand secure routing protocol that provides security against arbitrary active attackers and depends only on safe symmetric cryptography. It stops attackers from tampering uncompromised routes that consist of uncompromised nodes. ARIADNE guarantees point-to-point authentication of a routing message by uniting a shared key involving the two parties and MAC. But it relies on the TESLA broadcast authentication protocol for secure authentication of a routing message.
The design of ARIADNE is based on DSR. Like DSR, it too comprises of two basic operations - route discovery and route maintenance. However, ARIADNE takes advantage of a resourceful combination of one way hash function and shared keys. It works on the assumption that the sender and receiver share secret (non-TESLA) keys for message authentication. The initiator (or sender) includes a MAC computed with an end-to-end key and the target (or destination) verifies the authenticity and freshness of the request using the shared key.
ARIADNE also utilizes pre-hop hashing mechanism, a one-way hash function that verifies that no hop is omitted. If there is any dead link, the intiator is sent back a Route Error message. Errors are generated just as regular data packets and intermediate nodes remove routes that use dead links in the selected path.
This routing protocol also acts as a resilient guard against attacks which modify and fabricate routing information. When used in conjunction with an advanced version of TESLA called TIK, it becomes immune to wormhole attacks. Conversely, it is still exposed to inconsiderate node attacks. ARIADNE is unfeasible in the present as hoc environments because general security mechanisms though very reliable have complicated key exchanges.

3. Security Aware Routing (SAR)

Security Aware Routing (SAR) [9] is an on-demand routing protocol based on AODV (ref section 2.2). It integrates the trust level of a node and the security attributes of a route to provide an integrated security metric for the requested route. By incorporating a Quality of Protection (QoP) as a routing metric, the route discovery can return quantifiable secure routes.
The QoP vector that is used here is a grouping of security level and available cryptographic techniques. SAR establishes the concept of a trust hierarchy in which nodes of the ad hoc wireless network are segregated into dissimilar trust levels so that an initiator can compel a base trust level for all the nodes that take part in the source-destination communication. Notice that a path with the necessary trust level may not be present even if there is network connectivity.

Even if SAR discovers fewer routes than AODV, they are always secured. The initiator of the route in SAR includes a security metric in the route request. This security metric is the minimum trust level of the nodes that can participate in the route discovery. Consequently, only those nodes that have this minimum security level can participate in the route discovery. All other nodes that are below that trust level will drop the request packets. If an back-to-back path with the required security is found, the intermediate node or destination sends a suitably modified RouteReply. SAR selects the shortest such route in case of multiple paths satisfying the required security features. In case of failure of route discovery, a message can be sent to the initiator so that it reduces the trust level. Whenever there is a successful path search, SAR always locates a route with quantifiable guarantee of security. This is done by having the nodes of a trust level share a key. Accordingly, a node that does not have a particular trust level will not have the key for that specific level, and so it will be unable to decrypt the packets using the key of that level. Consequently, it will not have any other option except to drop the packet. SAR uses sequence numbers and timestamps to end replay attacks.

Threats such as interception and subversion can be halted by trust level key authentication. Modification and fabrication attacks can be prevented by validating the digital signatures of the transmitted packets. One of the major problems of using SAR is the extreme encrypting and decrypting needed at each hop during the path discovery. In a mobile environment, the extra processing leads to an escalated consumption of power. A route discovered by SAR is secure although it may not be the shortest route in terms of hop-count. Such a path helps to read only the nodes that have the required trust level and thereby re-route the packets. malicious node can however, simultaneously steal the required key - a situation in which the protocol is still vulnerable to all kinds of attacks.

4. Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP), is another protocol extension that can be used for many of the on demand routing protocols applied nowadays. SRP shields against attacks that interrupt the route discovery process and ensures the identification of accurate topological information. The fundamental design of SRP is to create a security association (SA) with a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes. SRP assumes that this SA can be achieved through a shared key KST between the source S and target T. This sort of a security association must be present prior to the route initiation phase. The source S initiates the route discovery by sending a route request packet to the destination T. The SRP uses an additional header called SRP header to the underlying routing protocol (e.g. AODV) packet. SRP header contains the following fields: the query sequence number QSEC, query identifier number QID, and a 96 bit MAC field.

If the SRP header is absent, the intermediate notes will reject a route request message. Or else, they will pass on the route request message towards destination after extracting QID, source, and destination address. Maximum priority is given to nodes that create requests at the lowest rates and vice versa.

When the target T receives this request packet, it verifies if the packet has originated from the node with which it has SA. The request is dropped if QSEC is greater or equal to QMAX, as it is considered to be replayed. Otherwise it calculates the keyed hash of the request fields and if the output matches SRP MAC then authenticity of the sender and integrity of the request are verified.

S checks the source address, destination addresses, QID, and QSEC on receipt of a route reply. It however, rejects the route reply if it does not go with the currently pending query. In case of a match, it evaluates the reply IP source route with the precise reverse of the route carried in reply packet. If the two routes match then S calculates the MAC by using the replied route, the SRP header fields, and the secure key between source and destination. If the two MAC match then the validation is successful and it confirms that the reply did came from the destination T.

SRP drawback is that it suffers from the lack of validation mechanism for route maintenance messages as it does not stop a malicious node from harming routes to which that node already belongs to. SRP is immune to IP spoofing because it secures the binding of the MAC and IP address of the nodes but it is prone to wormhole attacks and invisible node attacks.

5. Secure Routing Protocol for Ad Hoc Networks (ARAN)

A Secure Routing Protocol for Ad Hoc Networks (ARAN) is an on-demand protocol designed to provide secure communications in managed open environments. Nodes in a managed-open environment exchange initialization parameters before the start of communication. Session keys are exchanged or distributed through a trusted third party like a certifica

Each node in ARAN receives a certificate once a secure identity authentication to a trusted certificate server T is done. Nodes utilize these certificates to authenticate themselves to other nodes during the exchange of routing messages. The certificate contains the node's IP address, its public key, as well as the time of issuing and expiration. These fields are concatenated and signed by the server T. A node A receives a certificate as: $T \rightarrow A$: certA =[IPA, KA+, t, e] KT−. In the authentication phase, ARAN ensures the existence of a secure path to the destination. Each intermediate node in the network stores the route pair (previous node, the destination node). All the fields are

concatenated and signed with source node I's private key. A combination of the nonce number (NI) and timestamp (t) is used to get data freshness and timeliness property. Each time I performs a route discovery, it monotonically increases the nonce. The signature prevents spoofing attacks that may alter the route or form loops. Source node I broadcasts a Route Discovery Packet (RDP) for a destination D as I → brdcst :[RDP, IPD, certI , NI , t]KI−.

Each node that receives the RDP for the first time removes any other intermediate node's signature, signs the RDP using its own key, and broadcasts it to all its neighboring nodes. This continues until destination node D eventually receives the packet.

Upon receiving the RDP, the destination node D sends a Reply (REP) packet back along the reverse path to the source node I. If J is the first node on the reverse path, REP packet is sent as D → J :[REP, IPI , certD, NI , t] KD−. When the source node I receives the REP packet, it verifies the destination's signature KD− and nonce NI. In case there is no traffic on an existing route during some specific time, then that route is deactivated in the routing table. Nodes use an ERR message to report links in active routes broken due to node movement.

ARAN provides network services like authentication and non-repudiation using pre-determined cryptographic certificates. Simulations demonstrate that ARAN is very resourceful in discovering and maintaining routes but routing packets are larger in size and overall routing load is high. Due to heavy asymmetric cryptographic computation, ARAN is highly expensive for route discovery. It is susceptible to wormhole attack and if nodes do not have time synchronization, then it is vulnerable to replay attacks as well.

6. Security Protocols for Sensor Network (SPINS)

Security Protocols for Sensor Network (SPINS) is a suite of two security building blocks which are optimized for ad hoc wireless networks. It provides important network services like data confidentiality, two party data authentication, and data freshness through Secure Network Encryption Protocol (SNEP) and secure broadcast through Micro Timed Efficient Stream Lossolerant Authentication (μTESLA).

A large number of the available protocols are impractical for secure broadcast as they utilize asymmetric digital signatures which are highly costly on creation and verification. SPINS introduces μTESLA, an enhanced version of TESLA which uses symmetric cryptographic techniques for authentications and asymmetry cryptography only for the delayed disclosure of keys. Tight lower bound on the key disclosure delay and robustness against DoS attacks makes μTESLA a very efficient and secure protocol for data broadcast.

SNEP provides point-to-point communication in wireless network. It depends on a shared counter between the sender and the receiver so as to confirm semantic security. In this way, it protects message contents of encrypted messages from eavesdroppers. The counter does not need to be sent with the message since both nodes share the counter and increment it after each block. Thus, the same message is differently encrypted every time. A receiver node is assured that the message originated from the legitimate node if the MAC verifies successfully. The counter value in the MAC eliminates replaying of old messages in the network.

SPINS is the first broadcast authentication protocol which is lightweight and secure. The computation costs of symmetric cryptography are small and the communication overhead of 8 bytes per message is nearly insignificant when contrasted to message size. SNEP ensures semantic security, data authentication, replay protection, and message freshness whereas μTESLA provides authentication for secure data broadcast.

7. Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks (CONFIDANT)

Cooperation Of Nodes Fairness In Dynamic Ad-hoc Networks (CONFI DANT) protocol is designed as an extension to reactive source-routing protocol such as DSR. It is a compilation of elements that work together with each other for monitoring, reporting, and establishing routes by staying away from counteracting nodes. CONFIDANT components in each node include a network monitor, reputation system, trust manager, and a path manager. Each node in this protocol monitors their neighbors and updates the reputation accordingly. If any misbehaving or malicious node is detected, they can notify other conforming nodes by sending an ALARM message. When a node gets this kind of an ALARM either by listening to the ad hoc network or directly from another node, it determines how reliable the ALARM is on the basis of the source of the ALARM and the total number of ALARM messages about the misbehaving node.

To warn them of malicious nodes, trust manager sends alarm messages to other nodes. Incoming alarms are verified for trustworthiness. Trust manager contains an alarm table, trust level table and a friend list of all trust worthy nodes to which a node will send alarms.

Local rating lists and black lists are maintained in the reputation system. These lists are switched with friend nodes; timeouts are used to keep away from old lists. A node gives more weight to its own experience as compared to events which are observed and reported by others. Each time the threshold for the defined behavior is traversed; the path manager does the re-ranking by erasing the paths containing malicious nodes and disregarding any request from

misbehaving nodes. At the same time, it sends an alert to the source of the path so that it can discover some other route.
DSR is very scalable in terms of the total number of nodes in the network when it is fortified with the CONFIDANT protocol extensions.
It also exhibits a good performance even if more than 60% of the nodes are misbehaving. The overhead for incorporating diverse security components is controllable for ad hoc environment. However, detection based reputation system has few limitations and routes are still vulnerable to spoofing and Sybil attacks.

8. Secure Incentive Protocol (SIP)

A Secure Incentive Protocol (SIP) has been proposed [25] to motivate packet forwarding in totally self organizing MANETs without relying on any centralized infrastructure. The basic idea of SIP is simple: each node imprints a non-forged "stamp" on each packet forwarded as the proof of forwarding, based on which packet relays are remunerated, while packet sources and destinations are charged with appropriate credits. It is, however, by no means an easy task to implement SIP in a secure, efficient manner. For example, the introduction of credits may serve not only as an incentive for cooperation, but also as a stimulus for cheating. In addition, as an add-on, any incentive scheme like SIP should be efficient and lightweight enough not to disturb other normal network functions such as routing.

9. Authenticated Routing for Ad hoc Networks (ARAN)

Authenticated Routing for Ad hoc Networks (ARAN)[26], detects and protects against malicious actions by third parties and peers in one particular ad hoc environment. ARAN introduces *authentication*, *message integrity*, and *non-repudiation* to an ad hoc environment as a part of a minimal security policy. ARAN has minimal performance costs for the increased security in terms of processing and networking overhead.

10. I-SEAD

Ad hoc networks are highly dynamic routing networks cooperated by a collection of wireless mobile hosts without any assistance of centralized access point. Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV). SEAD provides a robust protocol against attackers trying to create incorrect routing state in other node. However, it does not provide a way to prevent an attacker from tampering the next hop or the destination field in route update [27]. To overcome this limit an extension to SEAD called I-SEAD[27] has been proposed.

11. Defense Mechanisms Against Rushing Attacks

Rushing attacks are by and large directed against on demand routing protocols such as DSR [9]. To counter such attacks, a generic secure route discovery component called Rushing Attack Prevention (RAP) is used. RAP combines the following mechanisms: Secure Neighbor Detection, Secure Route Delegation, and Randomized Route Request Forwarding. Any on demand routing protocol such as ARIADNE can be used as underlying protocol to RAP.
In Secure Neighbor Detection, a three round mutual authentication procedure is used between a sender and a receiver to make sure if they are within standard communication range of each other. First, a node forwards a Neighbor Solicitation packet to the neighboring node which replies with a Neighbor Reply packet and finally, the initial node sends Neighbor Verification packet to confirm that both nodes are neighbors. Secure Route Delegation checks whether all the steps in Secure Neighbor Detection phase were carried out. Prior to sending a route update to its neighbor, it signs a route attestation, entrusting the rights to the neighbor to additionally disseminate the update.
In Randomize Message Forwarding, a node buffers k route requests and then it randomly forwards only one of these k requests. By putting a cap the total number of requests sent by a node, it stops flood attacks in the network. Each request carries the list of all the nodes navigated by that request. Furthermore, bi-directional verification is also used to authenticate the neighbors.
By effectively making use of a combination of these three mechanisms, RAP can find usable routes when other protocols cannot. When it is enabled, it has higher overhead than other protocols, but presently it is the only protocol that can guard against rushing attacks. Still, the network is still prone to rushing attacks if an attacker can compromise k nodes.

12. Defense Mechanisms against Wormhole Attacks

With the aim of preventing wormhole attacks, the packet leashes mechanism [11] proposes to add supplementary information to the packets in order to limit the maximum permitted transmission distance of the packet. Geographical leash and temporal leash can be used to identify and bring wormhole attacks to a halt. Geographical leash ensures that the recipient of the packet is within a specific distance from the sender while temporal leash is used to impose an upper bound on the packet's lifetime, thus confining the packet's longest travel distance. Temporal leash make use of packet's expiration time to find a wormhole. The expiration time is computed based on the allowed maximum transmission distance and the speed of light. A node will reject packet if this expiration time has passed. TIK (TESLA with Instant Key Disclosure) protocol is an extension of TESLA and it is implemented with temporal leashes to identify wormholes. It

requires each communicating node to know one public key for each other node in the network. The TIK protocol uses an efficient mechanism Merkle Hash tree [10] for key authentication. The root value m of the resulting hash tree commits to all the keys and is used to authenticate any leaf key efficiently.

Hash trees are generally large so only the upper layers are stored while lower layers can be computed on demand. The TIK packet is transmitted by sender S as S → R : HMACKi(M), M, T, Ki, where M is the message payload, T are the tree authentication values, and Ki is the key used to generate the HMAC. After the receiver R receives the HMAC value, it uses the hash tree root m and the hash tree values T to verify that the key Ki at the end of the packet is authentic, and then uses the key Ki to verify the HMAC value in the packet. The receiver R only accepts the packet as authentic if all these verifications are successful.

A receiver can authenticate the TESLA security condition as it collects the packet, thus getting rid of the authentication delay of TESLA. Packet leashes are effectual mechanisms, but TIK is not viable in resource constraint networks owing to the expensive cryptographic mechanisms employed. The lack of precise time synchronization in today's systems prevents TIK from affording a usable wormhole detection mechanism. An additional problem that is likely to occur with leashes using a timestamp in a packet is that, that the sender may not identify the definite time at which it will send out the packet. Generating a digital signature within that specific time may be impossible.

13. Defense Mechanisms Against Sybil Attacks

In a Sybil attack [21], a malicious node acts as a representative of a larger number of nodes either by impersonating other nodes or simply by claiming false identities as discussed earlier. Most of the secure protocols are susceptible to this type of attack. However, there are a range of key distribution mechanisms which can be efficiently made use of to shield against Sybil attacks. Sybil nodes can execute a plethora of attacks. For instance, network nodes use voting for countless reasons. With adequate Sybil nodes, an attacker may be able to find out the effect of every vote. Sybil nodes are allocated more resources and they can create DoS for legitimate nodes due to their huge number. Ad hoc wireless networks can use misbehavior detection property to identify any malfunctioning node. An attacker with many Sybil nodes can extend the fault and find a way around unobserved, having only small misbehavior actions associated with each identity. There are a number of ways to detect Sybil attacks.

In radio resource testing, it is presumed that nodes have only one radio and are incapable of sending or receiving on more than one channel. If a node wants to validate whether its neighbors are Sybil nodes, then it allocates a different channel to broadcast messages to each of its neighbors. The node then, listens to one of the channels. If a message is gathered, it is an indication of a legitimate neighbor, while an idle transmission is an indication of a Sybil node.

A more bona fide method of shielding against Sybil attacks is random key pre distribution. A random set of keys are assigned to each node and then every node can compute the common keys it shares with its neighbors. If two nodes share q common keys, they can establish a secure link. An one way Pseudo Random hash Function (PRF) is used for validation. Thus, an attacker can not just gather a bunch of keys and claim an identity since PRF is an one way hash function.

There are two types of key distribution mechanisms to counter Sybil attacks [22]. In single-space pairwise key distribution, each pair of nodes is assigned a unique key. A node i stores unique public information Ui and private information Vi. The node i computes its key from f(Vi,Uj) where Uj is the public key of neighboring node j. Validation is successful if a node has the pairwise key between itself and the verifier. In multi-space pairwise key distribution, each node is assigned, by the network, k out of m random key spaces. If two neighboring nodes have at least one key space in common, then they can compute their pairwise secret key using the corresponding single space scheme.

This is the first work that suggests various defense mechanisms against the Sybil attacks, for instance radio resource testing and random key predistribution. Random key predistribution is already been used in many applications to secure radio communication. The most productive mechanism against Sybil attacks is the multi-space pairwise key distribution mechanism.

14. Security Mechanisms for Broadcast Operation

Timed Efficient Stream Loss-tolerant Authentication (TESLA) [10] is an efficacious broadcast authentication protocol with low communication and computation overhead. It can be upgraded to large numbers of receivers, can endure packet loss, and utilizes loose time synchronization between sender and receivers.

TESLA primarily uses purely symmetric cryptographic functions; nevertheless, it achieves asymmetric properties from clock synchronization and delayed key disclosure. This way, it does not involve computing expensive one-way functions. For this purpose, it needs sender and receivers to be loosely time-synchronized and for a secure authentication, either the receiver or the sender must buffer some messages.

For secure broadcasting, a sender chooses a random initial key KN and generates a one-way key chain by repeatedly computing the one-way hash function H on the starting value KN−1 = [KN] , KN−2 = H[KN−1], . . ., K0 = H[K1] . In general, Ki = H[Ki+1] = HN−i[KN] where Hi[x] is the result of applying the function H to x, for i times. The sender node predetermines a schedule at which it discloses each key

of its one-way key chain. Keys are disclosed in the reverse order from generation, i.e. K0,K1,K2, . . . ,KN then the MAC computed using the key Ki is added to the packet. When the packet reaches the receiver, it checks the security condition of the key disclosure. If the key Ki used to authenticate the packet was not disclosed, then it buffers the packet and waits for the sender to disclose Ki, while using an already disclosed key to authenticate the buffered packets. However, if the key is already disclosed, then receiver will discard the packet. Although TESLA is efficient, it still has few disadvantages. It authenticates the initial packet with a digital signature which is too costly for wireless nodes and disclosing a key in each packet requires high energy for sending and receiving. TESLA is vulnerable to DoS attacks as malicious nodes can create buffer overflow state in the receiver while it waits for the sender to disclose its keys. SPINS introduces Micro Timed Efficient Stream Loss-tolerant Authentication (μTESLA), a modified version of TESLA which only uses symmetric mechanisms for packet authentication and it discloses the key once per epoch. μTESLA is different from TESLA as it allows a receiver to authenticate the packets the moment they arrive and it substitutes receiver buffering with sender buffering. Immediate authentication with buffering only at the sender makes it a secure protocol against DoS. It has very low security overhead. The computation, memory, and communication costs are small. Since the data authentication, freshness, and confidentiality properties require transmitting only 8 bytes per message, μTESLA is considered a very robust and economical protocol for secure data broadcasting.

Another protocol is TESLA with Instant Key Disclosure (TIK). It is used for secure broadcasting implemented with temporal leashes in order to detect wormholes. TIK necessitates precise synchronization of time between all communicating parties. Its functioning is akin to the base protocol TESLA. However in TIK, the receiver can authenticate TESLA security condition while receiving the packet. By doing away with the the validation delay of TESLA, it permits the sender to unveil the key in the same packet. TIK is thus a more robust protocol than TESLA as it gets rid of the waiting time imposed by disclosing the keys only after the packet was received.

VI .CONSIDERATIONS TO FFICIENCY ASSESMENT OF SAFEGUARDING UNDER SECURITY ATTACKS

1. Observing Routing Misbehavior

Misbehavior of nodes has been used to distinguish networks that are under security attack. Previous work has pointed out two types of misbehavior: a selfish behavior and a malicious behavior [23]. Selfish nodes use the network but do not cooperate, saving battery life for their own communications: they do not intend to directly damage other nodes. Malicious nodes aim at damaging other nodes by causing network outage by partitioning while saving battery life is not a priority. This section focuses on the misbehavior model for selfish nodes and based on [23] defines two different type models for them. Node selfishness is of great interest because nodes of MANETs are often battery-powered, thus energy is a precious resource that they may not want to waste for the benefit of other nodes. All together we define three routing behaviors of nodes.

a) Type 0 well-behaved node: Nodes behave nicely according to a routing protocol including route discovery, maintenance, packet forwarding and receiving.

b)Type 1 selfish node: In this model, a selfish node does not perform packet forwarding, so every packet sent to this node is dropped by it. Thus, it disables the packet forwarding function for all packets that have a source address or a destination address different from the current selfish node address. This actually helps the selfish node in terms of consumed energy to save a significant portion of its battery life by neglecting large data packets, while still contributing to the network maintenance.

c) Type 2 selfish node: In this model, the node does nothing with the packet sent to it, thereby no execution function is performed. The selfish node can be considered as a rest node inside the network, since it stops contributing to the network maintenance, routing discovery, nor packet forwarding and receiving.

We believe that these selfishness models are simple, but realistic. Our following simulation study evaluates the performance of DSDV, DSR and AODV when a certain percentage of nodes behave following the Type 1 and Type 2 selfishness models above, while the remaining nodes are assumed to be well-behaved.

2. Performance metrics to be considered:

In comparing the protocols, network performance is evaluated according to the following metrics:

- Normalized throughput: Also called packet delivery ratio in [22] and throughput in [23], this is the ratio of the number of packets received by the CBR sink to the number of packets sent by the CBR source, both at the application layer.Packets that are sent but not received are lost in the network due to malicious drops, route failures, congestion, and wireless channel losses.

- Average delay: This is the average delay of all the packets that are correctly received. Lost packets are obviously not included in this measurement since their packet delay is infinity.

- Routing overhead: The total number of routing packets transmitted during the simulation at the network layer. Packets that are routed over multiple hops are counted multiple times – each hop is counted as one transmission.

- Normalized routing load: The ratio of the total number of routing packets transmitted or forwarded at the network layer to the total number of CBR packets received at the destination at the application layer.

These metrics together give a thorough evaluation of a routing protocol. Normalized throughput represents both the completeness and correctness of the routing protocol; average packet delay tells efficiency of the protocol to correctly deliver packets and the degree of network congestion; routing overhead measures the scalability of the routing protocol and its power consumption efficiency; and normalized routing load demonstrates to some extend the average number of hops the protocol routes a packet from sender to receiver, as well as the efficiency of the protocol.

VII CONCLUSION

The above observations may help to get a more detailed picture of the problems arising when designing 'secure' ad hoc routing protocols. Note that we did not mention well known problems in infrastructure-less environments, e.g. the absence of a trusted certification authority and possible solutions to overcome this problem, e.g. by threshold cryptography. As a first recommendation for designing new security solutions in the context of ad hoc networks we should restrict ourselves trying to reach the elementary security objectives with a reasonable message overhead and delay. We should not waste time trying to achieve unrealistic security and reliability issues that result in unacceptable signaling overhead on a meta level by only limited gain under some particular circumstances. In the Introduction the authors sketch out what routing protocols in general should routing aim at. Apparently most of the requirements seem to be fulfilled, but, according to thesis 6, we notice that injection of forged control messages is always possible. Also dropping, partial or complete, is an operation that strictly depends on the 'human' behavior of the attacker. In both cases the only countermeasure available is detection but even a detection scheme is a limitation for the system itself. In fact, detection is prerequisite for reaction. Intuitively, once misbehaving nodes have been identified, we need to propagate and share this knowledge with the other member of the ad hoc cloud. How can we reach an acceptable level of trust?

This reasoning lead us to the conclusion that when proposing a security architecture, researchers and protocol engineers have to take in account always a degree of vulnerability. The goodness of the solution will then depend on how much the system can tolerate malicious behaviors. For instance, if we consider two ad hoc clouds **a** and **b** composed by twenty nodes each, and we fix the level of tolerance $T(a) = 0.8$ and $T(b) = 0.7$ it means network **a** can tolerate not more than four misbehaving nodes and network **b** not more than six. The fine tuning of this parameter is probably the best countermeasure we can deploy against known and unknown attacks.

REFERENCES

[1] Y. -C. Hu, D. B. Johnson and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Jun. 2002.

[2] Z. J. Haas, The Routing Algorithm for the Reconfigurable Wireless Networks, Proc. of ICUPC 1997, Vol 2, Oct. 1997, pp. 562-566.

[3] T. H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation, Proc. of IEEE Symp. on Wireless Personal Mobile Communications 2001, Sep. 2001.

[4] Y. C. Hu, D. B. Johnson, and A. Perrig, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Mobicom'02, 2002.

[5] S. Buchegger and J. L. Boudec, Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks, In Proc. of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Jun. 2002.

[6] Mohammad O. Pervaiz, Mihaela Cardei, Jie Wu, Routing Security in Ad Hoc Wireless Networks. Network Security Scott Huang, David MacCallum, and Ding Zhu Du(Eds.) c 2005 Springer.

[7] D. Coppersmith and M. Jakobsson, Almost Optimal Hash Sequence Traversal, In Proc. of The Sixth Intl. Conf. on Financial Cryptography (FC 2002), Lecture Notes in Computer Science, Springer 2002. [5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks, ACM CCS 2003, Oct. 2003, pp. 42-51.

[8] D. B. Johnson and D. A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Kluwer Academic Publishers, Vol 353, pp. 153-181.

[9] R. Kravets, S. Yi, and P. Naldurg, A Security-Aware Routing Proto col for Wireless Ad Hoc Networks,

[10] A. Perrig, R. Canetti, D. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories), Vol 5, No 2, Summer/Fall 2002,

[11] Y. -C. Hu, D. B. Johnson, and A. Perrig, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, 2003.

[12] Y. -C. Hu, D. B. Johnson, and A. Perrig, Efficient Security Mechanisms for Routing Protocols, The 10th Annual Network and Distributed System Security Symp. (NDSS), Feb. 2003.

[13] Y. -C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Infocom 2003.

[15] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM'94 Conf. on Communications architectures, Protocols and Applications,

[16] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad hoc Networks, The 10th IEEE Intl. Conf. on Network Protocol (ICNP), Nov. 2002.

[17] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.
[18] V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for MobileWireless Networks, IEEE Infocom 1997, Apr. 1997, pp. 1405-1413
[19] P. Sinha, R. Sivakumar, and V. Bharghavan, CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm, IEEE Journal On Selected Areas in Communications, Vol 17,
[20] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, The Broadcast Storm Problem in a Mobile Ad Hoc Network, ACM Wireless Networks, Vol 8, No 2, Mar. 2002,
[21] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.
[22] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Predistribution Scheme for Wireless Sensor Networks, ACM CCS 2003, Oct. 2003, pp. 42-51.
[23] J. Broch, D. A.Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pages 85–97, New York, NY, USA, 1998. ACM Press.
[24] P. Michiardi and R. Molva. Simulation-based analysis of security exposures in mobile ad hoc networks. In Proceedings of European Wireless Conference, 2002.
[25] Yanchao Zhang, Wenjing Louy, Wei Liu and Yuguang Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks", in proc. of Journal on Wireless Networks, vol. 13, no. 5, pp: 569- 582, October 2007.
[26] A Secure Routing Protocol for Ad Hoc Networks, Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02)
[27] I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks, 2008 International Conference on Multimedia and Ubiquitous Engineering

AUTHORS PROFILE

PRASUNA .V. G. has received PGDCA in 1990 from JNTU,Hyderabad , MCA in 2005 from IGNOU, New Delhi and Presently pursuing Doctrate Degree (Ph. D) in Computer Science from
Sri Krishnadevaraya University, Ananthapur and working as Assistant Professor in the Department of MCA ,Basaveswara Institute Of Information Technology,Hyderabad. Her research interest includes Wireless networks, Security, Routing Protocols.

Dr. S. Madusudhana verma has received M.Sc in 1986, M.Phil in 1988 and Ph.D in 1994 from Sri Venkateswara University, Tirupathi. He is working as Associate Professor and Head Of OR&SQC at Rayalaseema University, Kurnool. His research interests are Reliability Engineering, Statistical modeling and Computer Science. He has attended 12National and International Conferences and published 20 research articles in National/International Journals and guided for Doctoral and M.Phil degrees.