International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 4: Issue 2 *[ISSN: 2250-3757]*
Publication Date : 25 June 2014

DIFFERENT ROUTING PROTOCOLS AND THEIR VULNERABILITIES AND THEIR MEASURES

Himadri Nath Saha[1], Dr. Debika Bhattacharyya[2] Bipasha Banerjee[3] Sulagna Mukherjee[4] Rohit Singh[5] and Debopam Ghosh[6]

ABSTRACT: Mobile Ad-hoc Network (MANET) is a wireless network model which is infrastructure-less and consists of mobile nodes. Since MANET does not have any centralized base station and is robust in nature, it is a major center of attraction. Due to the open nature, access to trusted authorities, the security in MANET poses a huge threat. Also energy constraint is another factor to be considered and thus, routing in MANET is a big challenge .In this paper we have discussed in depth about the various routing protocols in MANET and classify them. We have also discussed and compared their vulnerabilities in form of attacks, and classify these attacks. Brief descriptions of these attacks are given, mainly emphasizing on the network level attacks. Further we briefly review the existing secured MANET routing protocols to tackle these attacks and discuss their efficiency and shortcomings.

Keywords: reactive, proactive, hybrid, MANET, position based routing, attacks in MANET, Secured Routing Protocol.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. MANETs differ from conventional wireless networks, such as cellular networks and IEEE 802.11 (infrastructure mode) networks; in that they are self-containing the network nodes can communicate directly with each other without reliance on centralized infrastructures such as base stations. Additionally, MANETs are self organizing and adaptive; they can therefore form and de-form on-the-way without the need for any system administration. These unique features make MANETs very attractive for scenarios requiring rapid network deployment, such as search and rescue operations. MANET (mobile ad-hoc network) is a collection of mobile nodes which are dynamically connected to transfer information without the presence of any centralized infrastructure. It is a fully self organized network as it does not rely on any established infrastructure for the network initialization and operation. Initially it was conceptualized mainly for crisis situations like battle-fields and so on. Nodes can be any wireless device like personal computers (laptops), mobile phones etc.

Figure 1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the nodes wirelessly communication among them.

There are some challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment.

One of the core security issues is trust management. Trust is generally established and managed in wired and other wireless networks via centralized entities, such as certificate authorities (CAs) or key distribution centers. The absence of centralized entities in MANETs makes trust management a rather challenging problem, primarily due to the unavailability of trusted authorities to perform necessary functions such as the revocation of digital certificates.

Figure 1 MANET Overview

Another intriguing MANET security problem is the issue of secure routing in the presence of selfish or malicious nodes, which selectively drop packets they are required to forward; and in so doing, these selfish or malicious entities can cause various communication problems.Also since the network is self-organizing, the topology changes randomly. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.

Due to presence of a fixed supporting structure, limits the adaptability wireless system is required easy and quick deployment of wireless network. Recent advancements of wireless technologies like Bluetooth[1],IEEE 802.11[2] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs)[3][4][5][6], which operate in the absence of central access point. It provides high mobility and device portability that allow nodes to connect to network and communicate to each other. It allows the devices to maintain connections to the network as well as add and remove devices to and from the network. User can design such networks at cheapest costs and minimum time. MANET has the following characteristics, such as:

- Weaker in security
- Device size Limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

II. ROUTING PROTOCOLS

Before proceeding to describe each of the routing protocols of MANET, it is fitting to list some desirable qualitative properties of these protocols. This list is adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo [7].

Loop-free: It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.

Demand-based operation: In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.

Proactive operation: This is the flip-side of demand-based operation. In cases where the additional latency—which demand-

Himadri Nath Saha[1]
[1]Institute of Engg & Management
Kolkata, India

based operations incur—may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.

"Sleep" period operation: It may be necessary—for reasons such as the need for energy conservation—for nodes to stop transmitting or receiving signals for arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.

Security: It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

There are two general categories of MANET routing protocols: Topology-based and Position-based . Firstly we start by classifying MANET routing protocols as given in Figure 2 followed by a brief overview of each of the protocols in the upcoming sections.

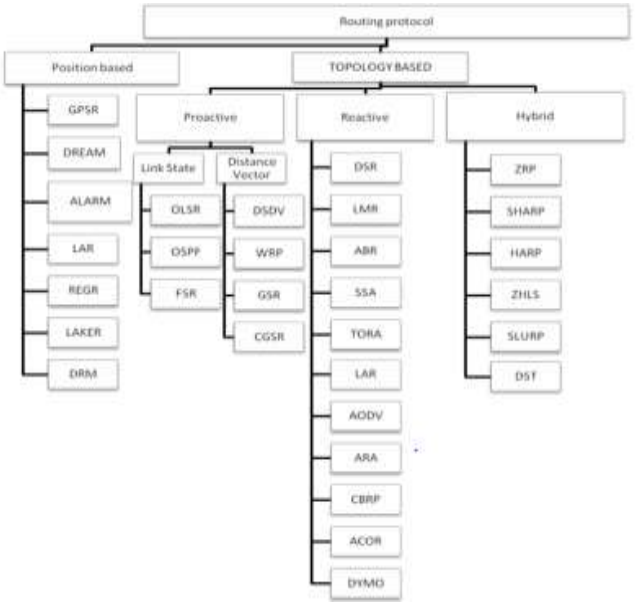

Figure 2 General Categories of Routing Protocols

A. *Position-based routing protocols*

Position-based routing protocols employ nodes' geographical position to make routing decisions. In order to utilize a position-based routing protocol, a node must be able to ascertain the geographical position of it and that of all the nodes it wishes to communicate with. This information is typically obtained via Global Positioning System (GPS) and location services.

Position-based routing protocols are completely dependent on GPS (Global Position System) for routing. GPS demands external battery power and hence results in a low battery life. These systems are also not well run in real time for all models, because if there is any malfunction with the GPS system, then the Position Based Routing fails. Hence this is the main cause of using Topological based Routing Protocols.

B. *Topology based routing protocol*

Topology based routing mechanism utilizes topology information to make routing decisions at each node. Topology information means separate route management process, like Route Request, Route Reply, etc. There are three major categories of Topology-based routing protocols: On-demand (Reactive), Proactive & Hybrid protocols.

1) Proactive protocols:

Proactive protocols are also referred to as periodic protocols. It maintains one or more tables representing the entire topology of the network, which are updated from time to time.

There are many proactive protocols, as shown in Figure 3., out of which some of them are described as follows, Destination-Sequenced Distance-Vector (DSDV) [8] utilizes the classical Distributed Bellman-Ford Distance-Vector algorithm [9][10][11]. DSDV (Perkins & Bhagwat, 1994) is a distance vector routing protocol that ensures loop-free routing by tagging each route table entry with a sequence number.

Fisheye State Routing (FSR) :
This protocol reduces the amount of traffic for transmitting the update messages. The basic idea is that each update message does not contain information about all nodes. Instead, it contains update information about the nearer nodes more frequently than that of the farther nodes. Hence, each node can have accurate and exact information about its own neighboring nodes. The novelty of FSR is that it uses a special structure of the network called the ''fisheye.''

Source Tree Adaptive Routing (STAR) :
The Source Tree Adaptive Routing (STAR) protocol [12] has significantly decreased the routing overhead disseminated in the network by employing a least overhead routing approach (LORA) to exchange routing information. It also employees optimum routing approaches (ORA) if required. This protocol scales very well for large networks since it has significantly reduced the bandwidth consumption for routing updates.

Optimised Link-State Routing (OLSR):
(Jacquet, Muhlethaler, Clausen, Laouiti, Qayyum, & Viennot, 2001)[13] optimises the linkstate algorithm by compacting the size of the control packets that contain link-state information and reducing the number of transmissions needed to flood these control packets to the whole network.

Clusterhead gateway switch routing (CGSR): [14]
The CGSR protocol, by Chiang et al., uses a distributed algorithm called the Least Cluster Change (LCC). By aggregating nodes into clusters controlled by the cluster heads, a framework is created for developing additional features for channel access, bandwidth allocation and routing. Nodes communicate with the cluster head which in turn communicates with other cluster heads within the network.

Wireless routing protocol (WRP):[15]
Murthy and Garcia–Luna–Aceves propose WRP which builds upon the distributed Bellman-Ford algorithm. The routing table contains an entry for each destination with the next hop and a cost metric. The route is chosen by selecting a neighbor node that would minimize the path cost. Link costs are also defined and maintained in a separate table.

Global state routing (GSR) :[16]
Chen and Gerla propose the GSR protocol, where the control packet size is adjusted to optimize the MAC throughput. Each node maintains the neighbor list and three routing tables containing the topology, the next hop, and the distance respectively. The neighbor list contains all neighbors of the current node. The topology table contains the link state information and a timestamp indicating the

time in which the link state information is generated. The next hop table contains a list of next hop neighbors to forward the packets while the distance table maintains the shortest distance to and from the node to various destinations. A weight function computes the distance of a link which may be replaced by other QoS routing parameter.

Table 1: Comparison of Proactive Routing Protocol[36]

Protocols	No of required tables	Freq of updated transmission	Advantages	Disadvantages
DSDV	Two	Periodically & as Needed	Loop free	High overhead
WRP	Four	Periodical ly & as Needed	Loop free	High MO
CGSR	Two	Periodically	Loop free	High overhead
GSR	Three and a list	Periodic , local	Localize d updates	High MO
FSR	Three and a list	Periodic, local	Reduce CO	High MO,Reduced Accuracy
STAR	One and Five Lists	Conditional	Employs LORA and ORA	High MO, processing overhead
OLSR	Three	Periodic	Reduced CO and connecti on	2-hop neighbo r knowledge required
DREAM	One	Mobility Based	Low CO and MO	Requires GPS

In general, every node maintains a list of destinations and their routes by processing periodic topology broadcasts originated by each node in the network, which increases the routing table space and requires periodic routing [17]. When a packet arrives, the node checks its routing table and forwards the packet accordingly. Each node monitors its neighboring links and every change in connectivity with any neighbor results in a topology broadcast packet that is flooded over the entire network, hence causing excessive traffic in the network. The delivery of packet data is much more inefficient in Proactive Protocols and they are not adaptive with respect to topology changes.

Proactive routing protocols provide fast responses to topology changes by maintaining routing information for all network destinations and react to changes in the network. However, the price to pay is the signaling overhead incurred in maintaining routing information for those destinations in which large numbers of nodes have no interest. On the other hand, reactive routing protocols provide routing information on a need-to-have basis and, at least in theory, can reduce the signaling overhead incurred in maintaining routing tables compared to proactive approaches[17].

2) On-demand protocols:

On-demand protocols are also referred to as reactive protocols. Unlike proactive protocols which seek to maintain routes to all destinations ,and maintaining an up-to-date routing table for the entire network calls for excessive communication between the nodes, as periodic and triggered updates are flooded throughout the network. On-demand protocols establish routes on a per need basis. We present brief description of some of the more widely known on-demand protocols below.

Dynamic Source Routing (DSR):
Dynamic Source Routing (DSR) was developed by Johnson and Maltz [18][19].The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead(proportional to the path length) is involved due to the source-routing mechanism employed in DSR.

SSA (Signal Stability-Based Adaptive Routing):
SSA routing protocol as proposed by DUBE[20] provides an on-demand route discovery by selecting longer-lived routes based on signal strength and location stability. The rational being that links which exhibit the strongest signal for the maximum amount of time leads to longer-lived routes and less route maintenance. SSA tries to find a completely stable paths form the beginning, a process that if succeeded to find a path, it will be a very positive side of SSA. On the other hand if this process fails to find a path it may start the procedure from the beginning allowing paths with unstable link, which means additional effort to find a path.

ABR(Associativity-Based Routing):
C-H Toh developed the Associativity-Based Routing (ABR) [21]. ABR utilizes the observation that a mobile node's association with its neighbor changes as it migrates and its transiting period can be identified by the associativity "ticks". Associativity ticks are updated by the mobile node's data-link protocol which periodically transmits beacons identifying itself and updates its associativity ticks in accordance with the mobile nodes in its neighborhood. A mobile node exhibits high associativity ticks (high association stability) with its neighbors when it is in a state of low mobility. Conversely, a state of high mobility is associated with low associativity ticks. The main drawback of this approach is short beaconing interval to reflect association degree precisely

AODV(Ad-hoc On-demand Distance Vector)
Ad-hoc On-demand Distance Vector Routing was designed by Perkins and Royer [22]. The key feature of this protocol is that applying a distributed routing scheme. In contrast to the source routing applied by DSR, AODV depends on storing the next hops of a path as entries in the intermediate nodes, which is considered as an advantage. However this may require additional resources form the intermediate nodes, which is the negative side of AODV[23].

DYMO (Dynamic Manet Ondemand):
DYMO was proposed by Perkins and Chakeres [24][25] is a successor to AODV reactive protocol. It is, however, slightly easier to implement and accumulates the routing information of all nodes in the path and does not support unnecessary HELLO messages and operation is purely based on sequence numbers assigned to all the packets. It is a reactive routing protocol that computes unicast routes on demand or when required. It employs sequence numbers to ensure loop freedom. One of the special features of DYMO is that it is energy efficient. If a node is low on energy, it has the option to not participate in the route discovery process. In such a case, the node will not forward any of the incoming RREQ messages. It however

will analyze the incoming RREP messages and update its routing tables for future use.

The DYMO protocol [26], however, does not perform well with low mobility. The control message overhead for such scenarios is rather high and unnecessary. Another limitation lies in the applicability of the protocol as stated in the DYMO Draft which states that DYMO performs well when traffic is directed from one part of the network to another. It shows a degraded performance when there is very low traffic random and routing overhead outruns the actual traffic.

TORA(Temporally-Ordered Routing Algorithm):
Temporally-Ordered Routing Algorithm (TORA) was developed by Park and Corson [27]. It is a highly adaptive multipath, loop-free, distributed routing algorithm which was designed for highly dynamic MANET environments. A key design concept of TORA is the localization of routing control messages to a small set of nodes near the topological change. TORA builds and maintains a directed acyclic graph (DAG) rooted at the destination. The DAG, by design, ensures that all directed paths are loop-free and lead to the destination. Links between routers are directed (to form the DAG) based on a metric, maintained by the routers, that can conceptually be viewed as a "height"[28].

This protocol can often falsely detect partitions. It even requires reliable and in-order delivery of route control packets. The main disadvantage of TORA is that the algorithm may also produce temporary invalid routes. TORA is not much used since DSR and AODV outperforms it.

Table 2 Comparison of Reactive Protocols

	Advantages	Disadvantages
DSR	Intermediate nodes do not store route information; Can provide multiple paths	Stale caches and relay storm problems may arise in large and highly mobile MANETs. Communication overhead due to source routing.
ABR	Stable routes; Localised route repair mechanism	Suitable for small MANETs. Frequent beacons may result in extra bandwidth and power consumptions.
SSA	Stable routes	Introduces more delays than DSR to find routes. Does not have any localised route repair mechanism
AODV	Adaptable to highly dynamic topologies; Multicast routing capability	Requires HELLO messages. Does not support multiple routes. Intermediate nodes need to store routing information. May not scale well with network size.
DYMO	It has a high throughput and packet delivery, low average end to end delay but incurs a low routing overhead.	Does not perform well with low mobility. It shows a degraded performance when there is very low traffic.
RDMAR	Limits the propagation of routing control packets	Flooding is used if nodes do not have any prior communication. Suited for MANETs having low to moderate topological changes.
TORA	Localised route maintenance	Can falsely detect partitions.Requires reliable and in-order delivery of route control packets. Temporary routing loops
CBRP	Reduces communication; Localised route maintenance	Introduces additional overhead for forming and maintaining clusters. Temporary routing loops.
MSR	Multi-path routing and load balancing	Requires periodic probe packets to gather information.
LMR	Multiple routes	Requires reliable delivery of routing control packets; Can suffer from temporary routing loops.
ARA	Multiple routes; Localised route maintenance	Route discovery is based on Flooding.

The other On-demand routing protocols as mentioned in Figure 2.2 (for example ARA[29], CBRP[30], RDMAR[31], LMR[32]) are not so relevant to our work. So they have not been described in this section. In Table 2 we try to present a comparative study between all the reactive protocols which we have described above.

3) Hybrid protocols:

These types of protocols combine proactive and reactive protocols to try and exploit their strengths. One approach is to divide the network into zones, and use one protocol within the zone, and another between them. It initially establishes some proactively prospected routes and then serves the demand from additional active nodes through reactive flooding. The main disadvantages are that the advantages depend on the no of nodes activated. Also the reaction to traffic demand depends on gradient of traffic volume.

Zone Routing Protocol (ZRP):
Zone routing protocol is a hybrid routing protocol which effectively combines the best features of proactive and reactive routing protocol [33][34]. The key concept is to use a proactive routing scheme within a limited zone in the r-hop neighborhood of every node, and use reactive routing scheme for nodes beyond this zone. An Intra-zone routing protocol (IARP) is used in the zone where particular node employs proactive routing whereas inter-zone routing protocol (IERP) is used outside the zone. The routing zone of a given nodes is a subset of the network, within which all nodes are reachable within less than or equal to the zone radius hops. The IERP is responsible for finding paths to the nodes which are not within the routing zone.

Zone-Based Hierarchical Link State Routing Protocol(ZHLS):
In ZHLS protocol [35], the network is divided into non overlapping zones as in cellular networks. Each node knows the node connectivity within its own zone and the zone connectivity information of the entire network. The link state routing is performed by employing two levels: node level and global zone level. The zone level topological

information is distributed to all nodes. Since only zone ID and node ID of a destination are needed for routing, the route from a source to a destination is adaptable to changing topology. The zone ID of the destination is found by sending one location request to every zone.

Table 3: Comparision Of Proactive And Reactive And Hybrid Routing Protocols In Manet[48]

Routing class	PROACTIVE	REACTIVE	HYBRID
Routing structure	Both Flat and hierarchical structures	Mostly Flat, Except CBRP	Flat
Periodic updates	Yes, some may use conditional.	Not required. Some nodes may require periodic beacons.	Yes(Locally)
Control Overhead	High	Low	Medium
Route acquisition delay	Low	High	Lower for Intra-zone; Higher for Inter-zone
Bandwidth requirement	High	Low	Medium
Power requirement	High	Low	Medium

We have classified, described and compared various existing MANET routing protocols. Having reviewed these routing protocols we conclude that there exists definite advantages and disadvantages for each routing protocol and each of them is well suited for only certain situations and vulnerable for others. The common drawback in the above mentioned protocols is concerning their security. Hence, the requirement for secure routing protocols is inevitable.

III. ATTACKS AND EXPLOITS ON EXISTING ROUTING PROTOCOLS

There are a wide variety of attacks that target the weakness of MANET[37]. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Mobile nodes present within the range of wireless link can overhear and even participate in the network. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV. More sophisticated and subtle routing attacks have been identified in recent published papers, such as the Blackhole (or sinkhole) [37] [38] ,Byzantine[39], and Wormhole attacks[40]. Currently routing security is one of the hottest research areas in MANET.

A. GENERAL CLASSIFICATION OF ATTACKS:

There are various kinds of attacks in MANETs and they have been classified on the basis of layers or protocol stack, behavior, type of packets and source of the attacks in this paper.

The attacks in MANET can roughly be classified into two major categories, namely Passive Attacks and Active Attacks, according to the attack means, as shown in Table 4. Passive Attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET.

Table: 4 Active and Passive Attacks

Active attacks	1.Repudiation
	2.SYN flooding
	3.Gray hole attacks
	4.Blackhole attacks
	5.Jellyfish attack
	6.Jamming
Passive attacks	1.Snooping- Unauthorized access to another person's data
	2.Eavesdropping attacks- Captures packets from the network transmitted by others' computers

The attacks can also be classified into two categories, namely External Attacks and Internal Attacks, the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Some security attacks use stealth, whereby the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealth. Some attacks are non-cryptography related, and others are cryptography primitive attacks,as mentioned in Table 5.[42]

Table: 5 Primitive Attacks

Cryptography Primitive Attacks	Examples
Pseudorandom Number Attack	Nonce,timestamp,intialization vector(IV)
Digital Signature Attack [43].	RSA signature, ElGamal signature, Digital Signature Standard(DSS)
Hash Collision Attack	SHA-0,MD4,MD5,HAVAL-128,RIPEMD
Security Handshake Attacks	Diffie-Hellman key exchange protocol, Needham-Schroeder protocol

Attacks can also be classified according to network protocol stacks. Table 6 shows an example of classification of security attacks based on protocol stacks ;some attacks can be launched at multiple layers[41].

Table 6 Attacks on different attscks.

Layers	Attacks
Application Layer	Mobile virus, worm attack
	Repudiation

Transport Layer	SYN flooding
	Session Hijacking
Network Layer	Gray hole attack
	Black hole attack
	Co operative black hole attack
	Worm hole attack
	IP spoofing attack
	Byzantine attack
	SYBIL attack
	Information disclosure
	Resource consumption attack
	Jelly fish attack
	Routing attacks: Route overflow; Route table poisoning; Rushing attack
	Packet replication
	Sleep deprivation attack
MAC Layer	Jamming
Multi-layer attacks	DoS attack
	SYN flooding
	Impersonation
Other attacks	Location disclosure
	Blackmail attack
	Node isolation attack

B. *NETWORK LAYER ATTACKS*

Now we are briefly discussing about the different attacks and their solutions, and we mostly emphasize on the Network Level.

Black Hole Attacks:
Most frequent attack happened here is stop forwarding the data packets. If we consider a malicious node which keeps waiting for its neighbor node to initiate RREQ packet [37,38]. As a node receives the RREQ packet, it will send a false RREP packet instantly with a modified high sequence number. So that the source node will assume that there is a new route is available towards the destination. The source node ignores the RREP packet from the other nodes including the correct nodes where it automatically denies the other nodes and it will start sending the packets towards the malicious nodes [44]. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets anywhere. This type of attack will happen frequently which is severe to find out and we use a detection techniques to solve these attacks. This attack is called a black hole where it swallows all the data.

Gray Hole Attacks:
A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are
• Dropping all UDP packets while forwarding TCP packets.
• Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node .If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbor, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source . A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

Co-operative blackhole attack:
A cooperative black hole attack is when several malicious nodes work together as a group.

Wormhole attack:
In this, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. The wormhole attack involves the cooperation between two attacking nodes. One attacker captures routing traffic at one point of the network and tunnels it to another point in the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link[40].

IP spoofing attack:
It is most frequently used in denial-of-service attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose—they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. Denial of service attacks that use spoofing typically randomly choose addresses from the entire IP address space, though more sophisticated spoofing mechanisms might avoid unroutable addresses or unused portions of the IP address space. The proliferation of large botnets makes spoofing less important in denial of service attacks, but

attackers typically have spoofing available as a tool, if they want to use it, so defenses against denial-of-service attacks that rely on the validity of the source IP address in attack packets might have trouble with spoofed packets. Backscatter, a technique used to observe denial-of-service attack activity in the Internet, relies on attackers' use of IP spoofing for its effectiveness.

Byzantine Attack:
In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior[39].

Sybil Attack :
SYBIL attack manifests itself by allowing malicious users obtaining multiple fake identities by pretending to be multiple , distinct nodes in the system. This way the malicious nodes can control the decisions of the system, especially if the decision process involves voting or any type of collaboration. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

Routing Attacks :
Route overflow- In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. In the case of proactive routing algorithms we need to discover routing information even before it is needed, while in the case of reactive algorithms we need to find a route only when it is needed. Thus main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.

Route table poisoning:
In routing table poisoning, the compromised nodes present in the networks send fictitious routing updates or modify genuine route update packets sent to other authorized nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

Rushing attack:
A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group/ to increase the probability of being included in a route/ to invade into routing paths. Its target is to multicast routing protocols that use a duplicate suppression mechanism in order to reduce routing overheads. It quickly forwards route discovery (control) packets by skipping processing or routing steps. Rushing attack otherwise, falsely sending malicious control messages and then forwards the packet firstly than clear node reachable.

Blackmail attack:
In a blackmail attack, or more effectively a cooperative blackmail attack, malicious nodes complain against an honest node to make other nodes that need to send data to believe that routing through the victim is harmful. Such attacks can prevent senders from choosing the best route to the destination thereby hampering efficiency and throughput in the network. In a blackmail attack, malicious nodes libel legitimate nodes and make them unreachable. Moreover, a blackmail attack is not effective because a node cannot cause a route or link to be blacklisted if it is not part of that route or link.

In the above section we have briefly described the different network layer attacks and other attacks faced by MANET protocols followed by a comparative study of various routing schemes against the most widely known attacks in MANET.

IV. SECURE MANET ROUTING PROTOCOLS

The types of attacks that we reviewed in the previous Section cannot be ignored and calls for security measures, since it will give rise to the vulnerability in the network and might highly affect the efficiency of the system. This section reviews some of the routing security schemes which have been proposed to address the security shortcomings of these protocols.

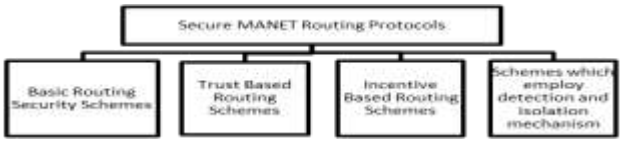

Figure 3. Classification of Secure MANET Routing Protocols

A. *Basic routing security schemes:*

The routing schemes which fall in this category provide authentication services which guard against modification and refplaying of routing control messages, but they do not attempt to provide solutions for issues such as the dropping of packets by selfish or malicious nodes.

We commence the review with one of the earlier proposals. Binkley and Trost [49] presented an authenticated link-level ad hoc routing protocol which uses ICMP router discovery message to discover mobile-IP nodes. It extended the ICMP router discovery packet format to include the MAC (Media Access Control) and IP address of the sender, and authentication info that can be used to verify the broadcast beacon. The protocol requires nodes to have shared secret keys for generating message authentication codes which are used to authenticate the routing control messages.

Venkatraman and Agrawal introduced an inter-router authentication scheme [50] for securing AODV routing protocol against external attacks (such as impersonation attacks, replaying of routing control messages and certain denial of service attacks). The scheme is based on the assumption that the nodes in the network mutually trust each other and it employs public key cryptography for providing the security services. The integrity of routing requests are ensured by the originating node hashing the messages and signing the resulted message digest. Recipients of a route request can check its authenticity and integrity by computing the hash of a the message using the agreed upon hash function, compare the computed hash with that attached to the message and verifying the signature. “Strong authentication” is provided for adjacent pair of nodes which transmit route replies to detect nodes which impersonate other nodes.

SRP:
Papadimitratos and Haas presented secure routing protocol (SRP) . SRP assumes the existence of a security associate on between a node initiating a route request query and the sought destination. The basic operation is as follows: A source node S initiates a route discovery by constructing and broadcasting a route request packet containing a source and destination address, a query sequence number, a random query identifier, a route record field (for accumulating the traversed intermediate nodes) and the message integrity codes (MIC) of the random query identifier, computed using HMAC and the secret key shared between the S and the destination. Intermediate nodes relay the route request packet so that one or more query packet(s) arrive(s) at the destination. When the route requests reach the destination D, D verifies that (a) the MIC is indeed that of the random query identifier, and (b) the sequence number is equal to or greater than the last known sequence number from S. If both (a) and (b) hold, D constructs a corresponding route reply packet containing the source, destination, the accumulated route in the route record field of the request query, the sequence number, the random query identifier and the computed MIC of the above. D then sends the route reply to S using the reverse path in the route record field. When S receives a route reply packet it validates the info it contains and verifies the computed MIC. If all is well, it uses the ascertained route to communicate with D.

SEAD:
Hu, Johnson and Perrig proposed the Secure Efficient Ad hoc Distance vector routing protocol (SEAD) . SEAD is a secure proactive protocol which is based on the design of DSDV . SEAD uses one-way hash chains for authenticating the hop count values in advertised routes and routing updates. For the authentication of the sender of routing update messages, SEAD allows authentication to be done using broadcast authentication mechanisms such as TESLA, HORS or TIK which require the network nodes to have time synchronized clocks. Alternatively, SEAD allows message authentication codes to be used to authenticate the sender of routing update messages; however, this is based on the assumption that shared secret keys are established among each pair of nodes.

SAODV:
Zapata presented Secure AODV (SAODV) . SAODV uses two mechanisms to secure AODV: digital signatures to authenticate non-mutable fields of the routing control messages and one-way hash chains (as is the case for SEAD) to secure hop count information.

TIARA:
Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) mechanisms protect ad-hoc networks against denial-of-service (DoS) attacks launched by malicious intruders. TIARA addresses two types of attacks on data traffic which are flow disruption and resource depletion.
The innovation is following:
• Routing algorithm independent approach for dealing with flow disruption and resource depletion attacks
• Fully distributed, self configuring firewall confines impact of DoS attack to immediate neighborhood of offending node
• Intrusion-resistant overlay routing reconfigures routes to circumvent malicious nodes Wireless Router Extension implementation architecture enables TIARA survivability mechanisms to be easily incorporated within existing wireless IP routers.

ARIADNE:
Hu, Perrig and Johnson proposed a routing security scheme called Ariadne which is based on the design of DSR. Ariadne uses message authentication code for authenticating routing control messages, and it requires time synchronization hardware for synchronizing the release of the secret keys used for generating the message authentication codes.

B. *Trust-based routing schemes*

The routing security schemes which fall in this category assign quantitative or qualitative trust values to the nodes in the network, based on observed behavior of the nodes in question. The trust values are then used as additional metrics for the routing protocols. We commence the review with one of the earlier protocols.

TRUST BASED DSR:
Pirzada and McDonald presented a model for trust-based communication in ad hoc networks . In this model, each node passively observes other nodes and assigns quantitative values (which range from 0 to +1) to nodes based on observed behavior. The authors proposed an extension of DSR which incorporates the trust model and utilizes trust as an additional routing metric.

TAODV:
Nekkanti and Lee presented a trust based adaptive on demand routing proto- col. The authors articulated that the most effective way of preventing certain routing attacks is to totally hide certain routing information from unauthorized nodes. In this regard, the main aim of their proposed scheme is to mask the routing path between a source and a destination from all other node. The scheme is based on AODV.

SDAR:
Boukerche [51] et al proposed secure distributed anonymous routing protocol (SDAR) . The main objective of SDAR is to allow trustworthy intermediate nodes to participate in routing without compromising their anonymity. SDAR utilizes a trust management system which assigns trust values to nodes based on observed behavior of the nodes, along with recommendation from other nodes. SDAR requires each node to construct two symmetric keys, and shares one with its neighbors which have high trust values, and the other with its neighbors which have medium trust values.

SLSP:
The Secure Link State Protocol (SLSP) [47] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops, which is termed as their zone. Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (LSU) packets from malicious alteration, as they propagate across the network. It disallows advertisements of non-existent, fabricated links, stops nodes from masquerading their peers, strengthens the robustness of neighbor discovery, and thwarts deliberate floods of control traffic that exhausts network and node resources.

C. *Incentive-base schemes*

In this section we present a brief description of proposed schemes which attempt to stimulate cooperation among selfish nodes by providing incentives to the network nodes.

Buttya´n and Hubaux[52] proposed an incentive-based system for stimulating cooperation in MANETs. The scheme requires each network node to have a tamper resistant hardware module, called security module. The security module maintains a counter, called nuglet counter, which decreases when a node sends a packet as originator, and increases when a node forwards a packet.

Zhong, Chen and Yang presented Sprite: A Simple, Cheat-Proof, Credit- Based System for MANETs. [53] Sprite provides incentive for MANET nodes to cooperate and report actions honestly. Sprite requires a centralized entity called a Credit Clearance Service (CCS) which determines the charge and credit involve in sending a message.

D. *Schemes which employ detection and isolation mechanisms*

This section contains a brief description of schemes which utilize detection and isolation techniques.

Marti[54]et al proposed a scheme for mitigating against the presence of MANETs nodes that agree to forward packet but fail to do so. The scheme utilizes a "watchdog" for identifying misbehaving nodes and a "pathrater" for avoiding those nodes. Each node has its own watchdog and pathrater modules. Watchdog operation requires the nodes within a MANET to operate in promiscuous mode: meaning that a node that is within the transmission range of a node should be able to overhear communications to and from even if those communications do not involve ni. Watchdog is based on the assumption that if a packet was transmitted to node for it to forward the packet to node , and a neighboring node to ni does not hear the transmission going from to then it is likely that ni is malicious and should therefore be assigned a lower rating. Pathrater is responsible of assigning ratings. The rating is assigned as follows: when a node become known to the pathrater, is assigned a "neutral" rating of 0.5. The ratings of nodes which are on actively used path are consequently incremented by 0.01 every 200 ms; whereas, a node's rating is decremented by 0.05 when a link to the node is surmised to be nonfunctional. "Neutral" ratings are bounded with an upper bound of 0.8 and a lower bound of 0.0; but a node always assign a rating of 1.0 to itself. Rather than selecting a path to a given destination based on the number of hops in the path, the pathrater selects the path which has the highest average rating.

Buchegger and Le Boudec [45] proposed a protocol called CONFIDANT that aims to detect and isolate misbehaving nodes in MANETs. CONFIDANT uses a form of reputation systems [Resnick(2000)] where the nodes within a MANET rate each other based on observed behaviors. Nodes that are deemed to be misbehaving are placed on black lists and are consequently isolated.

Awerbuch [46]et al presented a routing security scheme aimed at providing resilience to byzantine failure caused by individual or colluding MANET nodes. The scheme utilizes digital signature for authentication at each hop, and it requires each node to maintain a weight list consisting of the reliability metric of the nodes within the network. The weight list is used in the route discovery phase to avoid faulty paths. When faults are detected in established paths, an adaptive probing technique is launched in an attempt to detect the faulty links. Faulty links are given decreased rating and are consequently avoided.

In the above section we briefly describe the well-known basic secure routing protocols and the security modifications made on the standard routing protocols in MANET. Table 7 gives a summary of various types of secured schemes discussed above, their characteristics and examples.

Table 7 Summary of routing security analysis

Schemes	Comments
Schemes which do not address packet dropping	SRP , SEAD , SAODV, Bliss, Tiara, Ariadne , ARAN, Binkley (2001) et al and Venkatraman et al schemes do not address packet dropping.
Trust-based schemes	SAR requires shared group keys. Pirzada et al and Nekkanti et al do not provide protection against packet dropping; SDAR [51] is subjected to the short comings indicated below for Marti et al scheme; Li et al scheme can be thwarted by dropping the trust query messages. SLSP's security considerations are limited to individual Byzantine attackers. The protocol is not claimed to be secure when challenged by two or more malicious nodes that collude.
Incentive-based schemes	Buttya´n et al requires tamper resistant hardware and Zhong et al requires on-line access to a centralized entity; there-fore, these schemes are limited in their applications.
Schemes which employ detection and isolation mechanisms	Marti et al, in the author's own words, has the following weaknesses: "it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) lim-ited transmission power, 4) false misbehavior, 5)collusion, and 6) partial dropping. "Buchegger et al scheme does not provide protection against false accusations.

6. SUMMARY

Mobile Ad hoc networks (MANETs) have several advantages compared to traditional wireless networks. These include ease of deployment, speed of deployment and decreased dependency on a fixed infrastructure. Unique characteristics of MANETs topology such as open peer-to-peer architecture, dynamic network topology, shared wireless medium and limited resource (battery, memory and computation power) pose a number of non-trivial challenges to security design. These challenges and characteristics require MANETs to provide broad protection and desirable network performance. In this paper, we examine the available secure routing protocols in MANETs such as Secure On- Demand Routing Protocol – Ariadne, SAODV, SAR, SEAD, SDSDV, SLSP, On-Demand Secure Routing Protocol Resilient to Byzantine Failures, Authenticated Routing for Ad-hoc Networks – ARAN, Secure Position Aided Ad hoc Routing – SPAAR. We identify the advantages and disadvantages of each protocol, we compare them based on some security parameters, and also we discuss some open challenges present in ad hoc secure routing.

All of the large number of on-demand routing protocols proposed have their own key features, which may add positive or negative sides to the protocols. However, they share their common ability to adopt with the dynamically changing topology of the wireless ad hoc networks, in spite of the delay required to find routes to destination nodes. Owing to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the

development of it. Security mechanisms are therefore necessary to mitigate against these eventualities.

These secure routing protocols provide many approaches to secure the MANETs, however there are still many open challenges remain unsolved. First, most of the secure routing protocols are designed with certain known attacks in mind. When an unknown attack is encountered, these protocols may collapse. Second, achieving higher security always requires more computation on each mobile node. In MANETs environment, resources are very limited, thus there will always be a trade between more security and more performance. Third, one security solution is being chosen based on which security aspects are most important in that environment. However, in many ways these security schemes are not exclusive to one another. Forth, until now, many secure routing, data packet forwarding and link layer security solutions are proposed, not all of which provide complete security for MANETs.

Acknowledgment

We would all like to take this opportunity to thank our institute (Institute of Engineering and Management), our department and all its faculties for providing us with suitable resourced which aided to the completion of this review paper.

References

REFERRENCES
[1] Janne Lundberg, Routine Security in Ad Hoc Networks. Tik-110.501 seminar on Network Security
[2] http://citeseer.nj.nec.com/400961.html.2000.H. Dang, W.Li and D.P. Agarwal, "Routing Security in wireless ad hoc networks", IEEE Communications Magazine, 0613-6804, pp. 70-75, October 2009.
[3] B.Dahill, B.N.Levine, E Royer, and C. Shields, "A secure routing protocol for ad hoc networks" in Proceedings of the International Conference on Network Protocols(ICNP), pp.78-87,2002.
[4] Y.Hu, A.Perrig and D.johnson,Ariadne: A Secure on demand routing protocol for ad hoc networks, in Proceedings of ACM MOBICON '02, 2010.
[5] Jean-Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The Quest for Securityin Mobile Ad hoc Networks. Proceedings of the 2010 ACM International Symposium on Mobile Ad hoc Networking & Computing, Long Beach, CA.2001.
[6] F.Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks", Security Protocols, 7th International Workshop,LNCS,Springer-Verlag,2009.
[7] .S. Corson and J. Macker. Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations. Internet Request for Comments (RFC 2501), January 1999
[8] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance- vector routing (dsdv) for mobile computers. In Proceedings of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, pages 234–244, October 1994.
[9] R. Bellman. On a routing problem. Quarterly of Applied Mathematics, 16(1):87–90, 1958.
[10]L. R. Ford jr. and D. R Fulkerson. Flows in networks. Princeton University Press, 1962.
[11] C. Cheng, R. Riley, S. P. R. Kumar, and J. J. Garcia-Luna-Aceves. A loop- free bellman-ford routing protocol without bouncing effect. In Proceedings of ACM SIGCOMM '89, pages 224–237, September 1989.
[12] J.J. Garcia Luna Aceves, C. Marcelo Spohn, Source tree routing in wireless networks, Proceedings of the Seventh Annual International Conference on Network Protocols Toronto, Canada, p. 273, October 1999.
[13] Optimized Link State Routing Protocol for Ad Hoc Networks P.Jacquet,P.
Mühlethaler,T.Clausen,A.Lauiti,A.Qayyum,L.Viennot. Hipercom Project,INRI Rocquencourt, BP 105, 78153 Le Chesnay Cedex,France.
[14] W.L.C. Chiang, H. Wu and M. Gerla, Routing in clustered multihop, mobile wireless networks, in: Proceedings of IEEE SICON, April 1997, pp. 197–211.
[15] S. Murthy, J.J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, MONET 1 (2) (1996) 183–197.
[16] T.-W. Chen, M. Gerla, Global state routing: a new routing scheme for ad-hoc wireless networks, in: Proceedings of IEEE ICC, vol. 1,June 1998, pp. 171–175.
[17] Proactive or Reactive Routing: A Unified Analytical Framework in MANETs
Xianren Wu, Hui Xu, Hamid R. Sadjadpour and J.J. Garcia-Luna-Aceves
[18] Johnson DB, Maltz DA, Hu Y. The dynamic source routing protocol for mobile ad hoc networks (DSR),July 2004. IETF Internet Draft.
[19] D. Johnson and D. Maltz. Dynamic source routing in ad-hoc wireless networks routing protocols. In Mobile Computing, pages 153–181. Kluwer Academic Publishers, 1996.
[20] Signal stability based adaptive routing(SSA) for ad-hoc mobile network.- Rohit Dube, Cynthia d. Rias, Kuang-Yeh wang, and Satish k. Tripathi
[21] C.-K. Toh. Associativity-based routing for ad-hoc mobile networks. Wireless Personal Communications, 4(2):103–139, 1997.
[22] C. Perkins and E. Royer. Ad hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999), pages 80–100, February 1999.
[23] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols.
[24] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing draft-ietf-manetdymo-17" Internet Engineering Task Force, Mar. 2009.
[25] IMPLEMENTATION OF DYMO ROUTING PROTOCOL Anuj K. Gupta1, Harsh Sadawarti2 and Anil K. Verma3.
[26] R. E. Thorup "Implementing and Evaluating the DYMO," February 2007
[27] V. D. Park and M.S. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of the 2nd IEEE INFOCOM, pages 1405–1413, April 1997.
[28] APPLICABILITY OF THE TEMPORALLY-ORDERED ROUTING ALGORITHM FOR USE IN MOBILE TACTICAL NETWORKS Vincent D. Park Joseph P. Macker M. Scott Corson
[29] ARA – The Ant-Colony Based Routing Algorithm for MANETs ∗Mesut G¨unes¸, Udo Sorges, Imed Bouazizi
[30] The Cluster-Based Routing Protocol:Tim Daniel Hollerung, University of Paderborn
[31] RDMAR: A bandwidth-efficient Routing Protocol for Mobile Ad hoc Networks:George Aggelou, Rahim Tafazolli
Center for Communication Systems Research (CCSR), University of Surrey
[32] Label-based Multipath Routing (LMR) inWireless Sensor Networks
Xiaobing Hou, David Tipper and Joseph Kabara ,Department of Information Science & Telecommunications University of Pittsburgh, Pittsburgh, PA 15260

[33] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc WirelessNetworks Architectures and Protocol, volume ISBN:81-297-0945-7. Pearson Education, first indian reprint,2005 edition,2005.
[34] E. Topalis S. Giannoulis, C. Antonopoulos and S. Koubias. Zrp Versus DSR and TORA: A Compressive Survey on ZRP Performance. 10th IEEE Conference ,ETFA 2005, 1(ISBN:0-7803-9401-1), Sept 2005.
[35] Arpit Bansal, Navjot Kaur, Sunil Khullar, Dr.R.P.S. Bedi. Performance Analysis of ZHLS-GF Routing Protocol for MANETs through simulations. In Research Cell: An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Dec. 2011, Vol. 5
[36] Hrituparna Paul, Dr.Prodipto Das,"Performance Evaluation of MANET Routing Protocols", IJCSI,Vol-9 Issue-2, July 2012.
[37] Milanovic N, Malek M ,Davidson A and Milutinovic V(2004). Routing and security in mobile ad hoc networks. In IEEE Computer Society journals0018-9162/0461-65.
[38] Ullah I and Rahaman S U (2010). Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols. In Master Thesis Electrical Engineering Thesis no: MEE 10:62 .
[39]Lamport L, Shostak R.E, and Pease M (1982). The Byzantine Generals Problem.ACM Trans. Programming Languages and Systems, vol. 4, no. 3382-401.
[40]Thalor J and Ms Monica (2013). Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review. In International Journal of Advanced Research in Computer Science and Software Engineering,Vol 3 ISSN: 2277 128X Issue 2 137-142
[41]Mamatha G S and Dr Sharma S C (2010). Network layer Attacks and Defense Mechanisms in MANETs- A Survey. Intrenation Journal of Computer Applications Vol.9 No 9 12-17.
[42]Wu B, Chen J, Wu Jand Cardei M (2006).A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Springer.
[43] Mehuron W(1994). Digital Signature Standard (DSS). U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL). FIPS PEB 186.
[44] Vishnu K and Paul A J (2010).Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks. IJCA Vol.1, No.22
[45] Buchegger S and Le Boudec J(2002). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'02) 226–236, June 2002.
[46]Awerbuch B, Holmer D, Nita-Rotaru C, and Rubens H(2002). An on-demand secure routing protocol resilient to byzantine failures. In Proceedings of the ACM workshop on Wireless security (WiSE '02) 21–30, September 2002.
[47] Papadimitratos P and Haas ZJ(2003). Secure Link State Routing for Mobile Ad Hoc Networks. Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 27–31,2003.
[48]Patwardhan A, Parker J, Joshi A, Iorga M, and Karygiannis T(2005). Secure routing and intrusion detection in ad hoc networks. In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom 2005)191–199, March 2005.
[49]Binkley J and Trost W(2001). Authenticated ad hoc routing at the link layer for mobile systems.
Wireless Networks, 7(2) 139–145, 2001.
[50]Venkatraman L and Agrawal DP(2001). An optimized inter-router authentication scheme for ad hoc networks. In Proceedings of the Wireless 2001 pages 129–146, July 2001.
[51] Boukerche A, El-Khatib K, Xu L, and Korba L(2005). An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks.Computer Communications, 28(10)1193–1203, 2005.
[52]Buttyan L and Hubaux JP(2003). Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5)579–592, 2003.
[53] ZhongS,Chen J, and Yang Y(2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In Proceedings of IEEE INFOCOM, March 2003.
[54] Marti S, Giuli TJ, Lai K, and Baker M(2000). Mitigating routing misbehavior in mobile ad hoc networks. In Mobile Computing and Networking pages 255–265, August 2000.

About Author (s):

Prof Himadri Nath Saha : Prof. Saha is graduated from Jadavpur University.He did his post graduate degree from Bengal Engineering and Science university.He is Assistant Professor of Institute of Engg and Management .His research interest issecurity in MANET

Prof.(Dr)Debika Bhattacharyya: Prof.Bhattacharyya did Phd. from Jadavpur University in the dept. of ETCE. She is HOD in the Dept of CSE.Her research Interest is security in MANET

Bipasha Banerjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research Interest is MANET

Sulagna Mukherjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research Interest is MANET

Rohit Singh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research Interest is MANET

Debopam Ghosh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research Interest is MANET