International Journal of Innovative Research and Review ISSN: 2347 – 4424 (Online)
An Online International Journal Available at http://www.cibtech.org/jirr.htm
2013 Vol. 1 (2) October-December, pp.12-36 /Himadri et al.
Review Article

A REVIEW ON ATTACKS AND SECURE ROUTING PROTOCOLS IN MANET

Himadri Nath Saha, Debika Bhattacharyya, *Bipasha Banerjee, Sulagna Mukherjee, Rohit Singh and Debopam Ghosh
Department of Computer Science, Institute of Engg & Management, Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex, Kolkata - 700 091, West Bengal, India
**Author for Correspondence*

ABSTRACT
MANET (mobile ad-hoc network) is a network model which is infrastructure- less. It consists of mobile networks which are free to move and the communication between them are wireless. Due to lack of any centralized infrastructure and access to trusted authorities, the security in MANET poses a huge threat. The conventional method of certificate revocation is not applicable in such mobile communication. The prominent routing protocols we know are generally designed for non-adversarial environments, where the nodes within a network are non-malicious, unselfish and well-behaving. The reality however is that in any network, there are likely to be malicious, selfish or miss-behaving nodes which have intentions of disrupting the routing protocol. Owing to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. In this paper we make a review of all the threats faced by the commonly known routing protocols, 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.

Key Words: *MANET, Routing Protocols, Attacks in MANET, Secured Routing Protocol*

INTRODUCTION
Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms, wireless links and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

Attacks and Exploits on Existing Routing Protocols
There are a wide variety of attacks that target the weakness of MANET (Milanovic, 2004). 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) (Milanovic, 2004; Ullah, 2010; Al-Shurman, 2004; Byzantine and Lamport, 1982; Alam, 2011; Grayhole and Shanmuganathan, 2012) and Wormhole attacks (Thalor, 2013; Maulik, 2011). Currently routing security is one of the hottest research areas in MANET.

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 (Rai, 2010; Razak), according to the attack means, as shown in Table 1. 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: 1 Active and Passive Attacks

Active attacks	1.Repudiation 2.SYN flooding 3.Gray hole attacks 4.Blackhole attacks 5.Jellyfish attack 6.Jamming (Muraleedharan, 2006)
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 (Rai, 2010; Razak), the domain of the attacks, as shown in Table 2.
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 (Gagandeep, 2012).

Table 2: External and Internal Attacks

Internal attacks	1.SYN flooding 2.Jamming 3.Blackhole attack 4.Byzantine attack 5.Internal eavesdropping
External attacks	1.DOS attacks(Yang (2004)) 2.Packet dropping

Attacks can also be classified according to network protocol stacks (Xiao, 2006; Wu, 2006).
Table 3 shows an example of classification of security attacks based on protocol stacks (Makkar, 2011) some attacks can be launched at multiple layers (Mamatha, 2010).

Table 3: Attacks on different attscks

Layers	Attacks	Purpose
Application Layer	Mobile virus, worm attack	Infect operating system or application softwares
	Repudiation	Deny participation in all or part of communication
Transport Layer	SYN flooding	Deny legitimate service access
	Session Hijacking	Malicious nodes behave as a legitimate system
Network Layer	Gray hole attack	Forwards all packets to certain nodes but may drop packets coming from or destined to specific nodes
	Black hole attack	Drop intercepted messages
	Co operative black hole attack	Drop intercepted messages
	Worm hole attack	Disrupt network routing
	IP spoofing attack	Hides the address of the packet
	Byzantine attack	Disruption or degradation of the routing services
	SYBIL attack	Tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve.
	Information disclosure	Leak confidential or important information to unauthorized nodes present in the network
	Resource consumption attack	Tries to waste away resources of other nodes present in the network
	Jelly fish attack	Delays data packets unnecessarily for some amount of time before forwarding them
	Routing attacks:	
	Route overflow	The attacker creates routes to nonexistent nodes
	Route table poisoning	congestion in portions of the network
	Rushing attack	Unable to find secure routes
	Packet replication	Replicates stale packets
	Sleep deprivation attack	The resources of the specific

		node/nodes of the network are consumed by constantly keeping them engaged in routing decisions
MAC Layer	Jamming	To hinder error-free reception at the receiver side
Multi-layer attacks	DoS attack	Deny legitimate service access
	SYN flooding	Congestion in network
	Impersonation	Change the configuration of the system as a super-user who has special privileges.
Other attacks	Location disclosure	With the help of traffic analysis techniques an attacker is able to discover the location of a node, and the structure of the network.
	Blackmail attack	Isolates legitimate nodes from the network
	Node isolation attack	Isolates a given node from communicating with other nodes in the network
	Invisible node attack	Participates in a protocol without revealing its identity

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) (Smaha, 1988; Mukherjee, 1994). But other attacks such as DoS(Denko) cannot be made stealth. Some attacks are non-cryptography related, and others are cryptography primitive attacks (Boora, 2013; Wu, 2006). Table 4 shows cryptography primitive attacks and some examples.

Table 4: Primitive Attacks

Cryptography Primitive Attacks	**Examples**
Pseudorandom Number Attack (Kaufman, 2002)	Nonce,timestamp,intialization vector(IV)
Digital Signature Attack (Mehuron, 1994).	RSA signature, ElGamal signature, Digital Signature Standard(DSS)
Hash Collision Attack (Wang, 2004)	SHA-0,MD4,MD5,HAVAL-128,RIPEMD
Security Handshake Attacks	Diffie-Hellman key exchange protocol, Needham-Schroeder protocol

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 (Al-Shurman, 2004; Chandure, 2011). 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 (Guan, 2012). 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. In the paper (Bala, 2009) it has been simulated that the Blackhole attack which is one of the possible attacks on AODV routing protocol in mobile ad hoc networks by the help of network simulator (NS-2). The simulation results show the packet loss, throughput, and end-to-end delay with Blackhole and without Blackhole on AODV in MANET. It analyzed that the packet loss increases in the network with a Blackhole node.

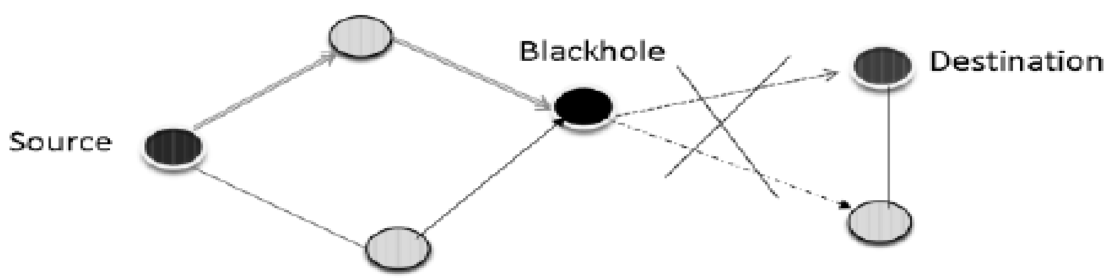

Figure 1: Black Hole

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 (Shanmuganathan, 2012) 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 (Vishnu, 2010). 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 (Arya, 2011). 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.

Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behavior:

(i) Node dependent attack – drops DATA packets destined towards a certain victim node or coming from certain node (figure 2), while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.

(ii) Time dependent attack – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances (figure 3).

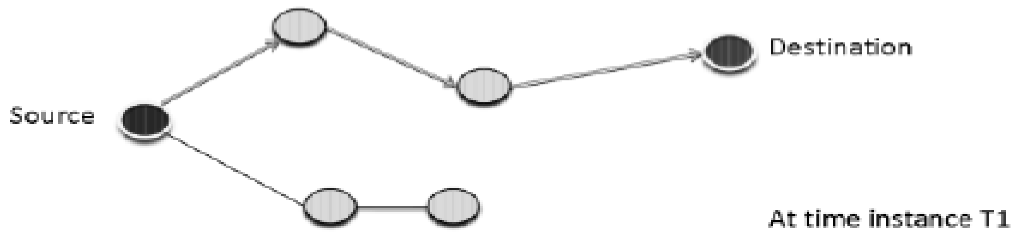

Figure 2: Gray Hole - Node Dependent Attack

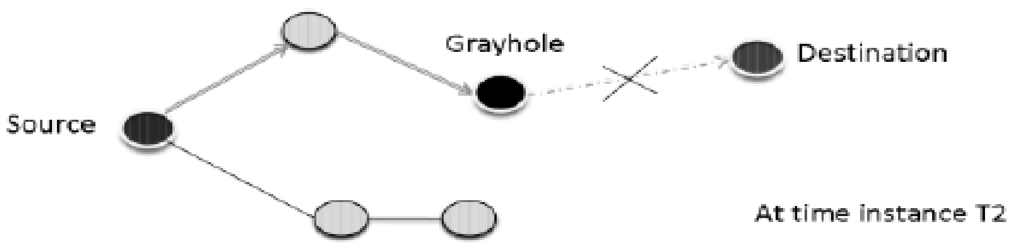

Figure 3: Gray Hole - Time Dependent Attack

Co-operative Blackhole Attack
A cooperative black hole attack is when several malicious nodes work together as a group (Ramaswamy, 2008). The black hole attack is one of the security attacks that occur in mobile ad hoc networks (MANETs). In this article (Min, 2009), the routing security issues and the problem of coordinated attack by multiple black holes acting in group in MANET are addressed in detail. Two authentication mechanisms, based on the hash function, the message authentication code (MAC) and the pseudo random function (PRF), are proposed to provide fast message verification and group identification, identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack.

Wormhole Attack
In this (Maulik, 2011; Hu, 2006), 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 (Baras, 2007; Mahajan, 2008; Chiu, 2006).

Review Article

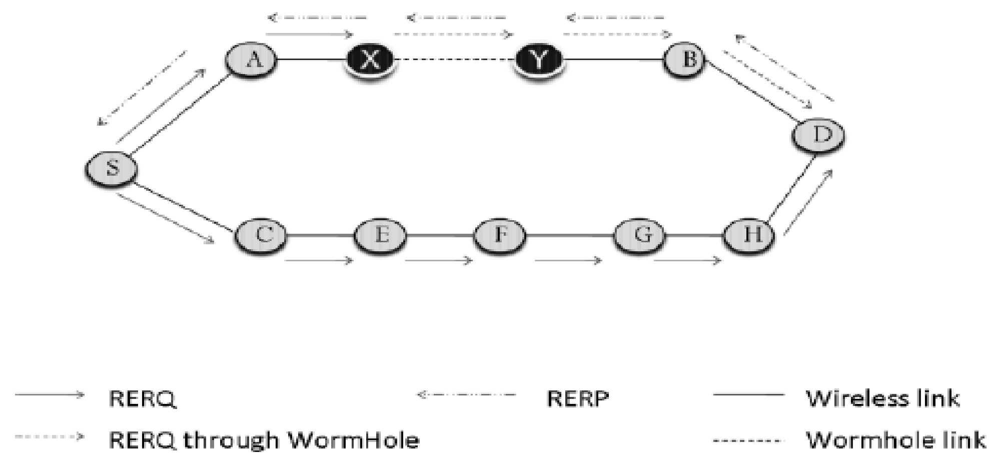

Figure 4: Worm Hole Attack

Wormhole attack can be done with single node also but generally two or more malicious node connects via a *wormhole-link*. In figure 4, Node X and Y performing wormhole attack.

IP Spoofing Attack

IP address spoofing (Saha, 2010) refers to the creation of Internet Protocol packets with a forged source IP address, called spoofing, it is a method of attacking a network in order to gain unauthorized access. The distributed denial-of-service (DDoS) attack is a serious threat to the legitimate use of the Internet. The attack is based on the fact that Internet communication between distant computers is routinely handled by routers which find the best route by examining the destination address. 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 (Templeton, 2003). 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 (Alam, 2011; Sofi, 2012), 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 (Lamport, 1982).

Sybil Attack

SYBIL (Llewellyn-Jones, 2009; Brooke, 2010; Guette, 2007) 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 (Piro, 2006; Saha, 2010).

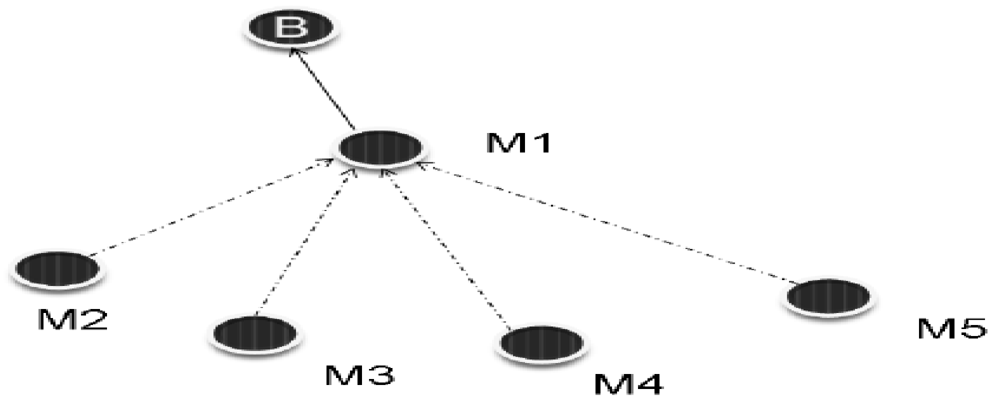

Figure 5: Sybil Attack

In figure 5, node M1 assumes identities of M2, M3, M4, and M5. So, to node B, M1 is equivalent to those nodes

Information Disclosure

Any confidential information exchange must be protected during the communication process. Also, the critical data stored on nodes must be protected from unauthorized access. In ad- hoc networks, such information may contain anything, e.g., the specific status details of a node, the location of nodes, private keys or secret keys, passwords, and so on. Sometimes the control data are more critical for security than the traffic data. For instance, the routing directives in packet headers such as the identity or location of the nodes can be more valuable than the application-level messages. A compromised node may leak confidential or important information to unauthorized nodes present in the network. Such information may contain information regarding the network topology, geographic location of nodes or optimal routes to authorized nodes in the network (Basagni, 2004).

Eclipse Attack

A pattern of misbehavior called an *eclipse* attack, which consists of the gradual poisoning of good (uncompromised) nodes' routing tables with links to a conspiracy of adversarial nodes (compromised nodes) (Hu, 2004; Schütte, 2006).

Resource Consumption Attack

In this attack (Murthy, 2006), an attacker tries to consume or waste away resources of other nodes present in the network. The resources that are targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. Using up the battery power of another node by keeping that node always busy by continuously pumping packets to that node is known as a sleep deprivation attack (Pirretti, 2006).

Jellyfish Attack

JELLYFISH affects (Aad, 2004) packet end-to-end delay and the delay jitter but not packet delivery ratio or throughput. A jellyfish attacker first needs to intrude into the multicast forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real applications. Jellyfish attack is a kind of DOS (Denial of service) attack in which attackers or malicious nodes try to increase packet end-to-end delay and delay jitter. Before applying attack jellyfish attacker first gain access to the routing group in mobile ad hoc network. This can be possible by performing Rushing attack. According to change in number of senders, receivers and attack position scenarios will get change in jellyfish attack (Khirasariya, 2012).

Misrouting Attack

This attack is also known as *manipulation of network traffic attack*. This is a very simple way for a node to disturb the protocol operation by announcing that it has better route than the existing one. In the misrouting attack, a on-legitimate node redirects the routing message and transfers data packet to the wrong target (Sanzgiri, 2002).

Routing Attacks

Route Overflow

In the case of routing table overflow (Huang, 2004), 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 (Agrawal, 2011), 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.

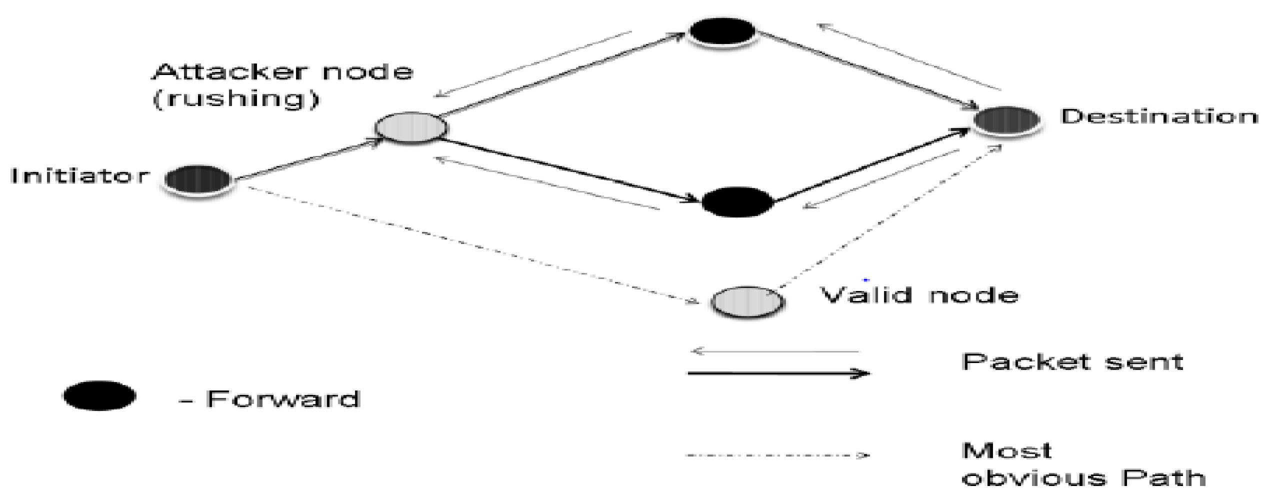

Figure 4: Rushing Attack

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.

Rushing attacks (Al-Shahrani, 2011) in mobile ad hoc networks (MANETs) cause system resources to become scarce and isolates legitimate users from the network. Therefore, this sort of attack significantly influences network connectivity and weakens networking functions and capabilities such as control and message delivery (Hu, 2003).

In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism.

Rushing attacker quickly forwards with a malicious RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node (De, 2011).

Blackmail Attack

In a blackmail attack (Konate, 2011), 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.

Secure MANET Routing Protocols

The types of attacks that we reviewed in the previous Section cannot be ignored, since it will give rise to the vulnerability in the network and might highly affect the efficiency of the system. Security mechanisms are therefore necessary to mitigate against these eventualities. This section reviews some of the roupting security schemes which have been proposed to address the security shortcomings of these protocols.

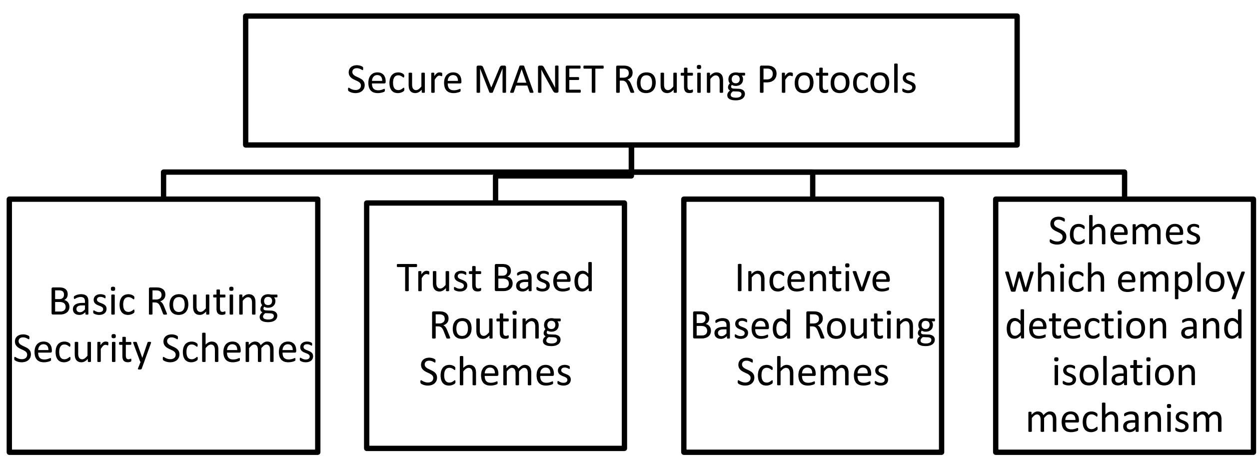

Figure 1: Classification of Secure MANET Routing Protocols

Basic Routing Security Schemes

The routing schemes which fall in this category provide authentication services which guard against modification and replaying 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 (2001) presented an authenticated link-level ad hoc routing protocol which uses ICMP router discovery message (Deering, 1991) 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 (Venkatraman, 2001) for securing AODV (Perkins, 1999) 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 is 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 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) (Papadimitratos, 2002). 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) (Huang, 2005) of the random query identifier, computed using HMAC (Krawczyk, 1997) 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 *et al.,* (2002) 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 (Perkins, 1994). SEAD uses one-way hash chains (Lamport, 1981) 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 (Perrig, 2002), HORS (Reyzin, 2002) or TIK (Hu, 2003) 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. SEAD provides a robust protocol against attackers trying to create incorrect routing state in the 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. In this paper (Lai, 2008) an I-SEAD protocol to solve the problem has been proposed.

SAODV

Zapata presented Secure AODV (SAODV) (Zapata, 2001; Zapata, 2002; Zapata *et al.*, 2002). 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) (Zhang, 2011) to secure hop count information.

TIARA

Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (TIARA) (Yan, 2003; Ramanujan, 2000) 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 *et al.*, (2002) proposed a routing security scheme called Ariadne which is based on the design of DSR (Johnson, 1996). 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. Ariadne can authenticate routing messages using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signature (Bonny, 2004).

ARAN

Sanzgiri and Dahill presented ARAN (Sanzgiri, 2002). ARAN uses digital certificates to secure the routing control messages. In ARAN route discovery phase, a source node S constructs a route discovery packet (RDP), signs it, attaches its certificate and broadcasts it to its neighbors. When a node A, which is a neighbor of S, receives the RDP message, if it has not previously seen this message, it verifies the signature using the attached certificate, signs the RDP message, attaches its certificate and broadcasts it to its neighbors.

An intermediate node B which is a neighbor of A, on receiving the RDP message, it validates the signature using the attached certificate. B then removes A’s certificate and signature, records B as its predecessor, signs the message and broadcasts it to its neighbors. The process continues in this manner until a RDP message arrives at the destination D. D selects the first RDP message it received, uses it to construct a reply (REP) packet and unicasts it to S using the reverse path. Each node on the reverse path back to S validates its predecessor signature using the attached certificate, removes the signature and the certificate (if the certificate does not belong to the destination node D), signs the packet, attaches its certificate and forwards the packet to the next-hop. Eventually, S should receive the REP with the route it seeks.

ARAN has solution for some attacks but it is also silent about some attacks like black hole attack, denial of service attack etc. some research can be done to add functionality to ARAN that is also able to combat with above said attack (Mehla, 2010; Sanzgiri, 2002). The advantages of ARAN are that it is secure as long as CA is not compromised, confidentiality is guaranteed because of public key encryption, network structure is not exposed, and it is resistant to most of the attacks. The disadvantages are that it requires extra memory, it has high processing overhead for encryption, and does not use hop count, so the discovered path may not be optimal.

Byzantine Failure Resilient Protocol

It proposes to flood both route requests and route replies in order to defend against Byzantine failures (Awerbuch, 2002). There are five steps for route discovery. Request Initiation, the source creates and sings the request. Request Propagation, the request propagate to the destination via flooding. Request Receipt/Response Initiation, the destination verifies the authenticity of the request and creates and signs a response. Response Propagation, the node computes the total weight of the path. During Response Receipt, when the source receives a response, it performs the same computation and verification as the intermediate nodes as described in the response propagation step.

The Advantage of Byzantine failure resilient protocol is that, as long as there is fault free path, even in a highly adversarial controlled network, it will be discovered after bounded numbers of faults have been occurred. The disadvantage of the protocol is that it is difficult to design a scheme that is resilient to large number of adversaries.

Secure Position Aided Ad hoc Routing

The SPAAR protocol was developed with the classical managed-hostile environment in mind, thus meant to provide a very high level of security, and sometimes at the cost of performance. Among other things, SPAAR also requires that each device to use a GPS locator to determine its position, although some leeway is given to nodes using a so-called "locator-proxy" if absolute security is not required. In SPAAR packets are only accepted between neighboring nodes one hop away from each other, this is to avoid the "invisible node-attack". The basic transmission procedure is quite similar to ARAN, although the group neighborhood key is used for encryption in order to ensure one-hop communication only. Since all nodes also have information on their location they only forward RREQs if their position is closer to the destination position (Yasinsac, 2002). The only real security disadvantage currently discovered in SPAAR is that the usage of the certificate server and the extreme need to keep this server uncompromised. Also, issues still exist with compromised nodes already having valid certificates (Carter, 2002).

BLISS

Building Secure Routing out of an Incomplete Set of Security Associations (BISS) (Capkun, 2003), the sender and the receiver can establish a secure route, even if, prior to the route discovery, only the receiver has security associations established with all the nodes on the chosen route. Thus, the receiver will authenticate route nodes directly through security associations. The sender, however, will authenticate directly the nodes on the route with which it has security associations, and indirectly (by exchange of certificates) the node with which it does not have security associations. The operation of BISS ROUTE REQUEST relies on mechanisms similar to direct route authentication protocols. When an initiator sends a ROUTE REQUEST, it signs the request with its private key and includes its public key PKI in the request along with a certificate cl signed by the central authority binding its id with PKI .This enables each node on the path to authenticate the initiator of the ROUTE REQUEST. The ROUTE REQUEST message contains the id of the target node. The node that receives this ROUTE REQUEST authenticates the initiator (by verifying the signature on the message), and tries to authenticate the target directly through security associations that it has. Only if a node can successfully authenticate both the initiator and the target will the node broadcast the message further. In BISS, we use similar route request data authentication mechanisms as in Ariadne. BISS exhibits the same resilience as Ariadne, as the security of the route establishment in both protocols assumes authentication between the same entities at the same stages of protocol execution, but performed with different cryptographic primitives and communication assumptions.

Leash Mechanism

Hu *et al.,* (2003) presented a mechanism called packet leashes for detecting and defending against wormhole attacks. In wormhole attacks, an attacker receives packets at one point in a network, tunnels them to another point in the network and replays them into the network from that point. The authors proposed two types of packet leashes: geographical leashes and temporal leashes (Rai, 2008).

Geographical leashes require a node to know its own geographical location and all nodes must have loosely synchronized clocks, whereas temporal leashes require all nodes to have tightly synchronized clocks. The leash mechanisms add necessary fields to a packet—for example the time the packet was sent and the sender's geographical location (for geographical leashes)—which allows the receivers to validate whether a node is in its transmission range or not. The authors also proposed a secure broadcast scheme called TIK which can be used to secure the packet leash mechanisms.

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 (Chatterjee, 2009).

SAR

Yi *et al.,* (2002) proposed a scheme called security-aware ad hoc routing (SAR) (Yi *et al.,* 2002). In SAR, nodes are categorized based on their security level. A secret group key is associated with each security level and it is shared amongst nodes which are classified at the given security level. SAR incorporates security attributes as route discovery parameters, such that a node can specify its preference with regards to the security level required for participation in the routing process. Yan *et al.,* (2003) proposed a trust evaluation based security solution (Yan *et al.,* 2003). The application of this scheme to MANET routing is similar in principle to the design of SAR (Yi *et al.,* 2002), in that the trust (or reputation) of a node is used as a routing metric when deciding the next hop of a packet (Lokulwar, 2012).

Trust Based DSR

Pirzada and McDonald presented a model for trust-based communication in ad hoc networks (Pirzada, 2004). 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 (Johnson, 1996) which incorporates the trust model and utilizes trust as an additional routing metric (Yong, 2007).

TAODV

Nekkanti and Lee presented a trust based adaptive on demand routing proto- col (Nekkanti, 2004). 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 (Perkins, 1999). It stipulates that one of three possible encryption levels be applied to a route request packets (RREQ). The encryption levels are high encryption which requires a 128-bit key, low encryption which needs a 32-bit key, and no encryption. The security level of a node and the security level of an application determine which encryption level is utilized. The general idea is that the more trustworthy a node is, the less need there is to hide routing information from this node during a route discovery operation. A summary of the route discovery operation is as follows: A source node S which desires a route to a destination D constructs a RREQ packet. The RREQ has a field where the application can set the security level it requires. The source then utilizes the public key of the destination node D to encrypt (with the appropriate security level) the source ID field of the RREQ packet and broadcasts it to its neighbors. When an intermediate node receives a RREQ packet it has not previously seen, if it is not the destination, it adds its node ID to the packet, signs it then encrypts it using the public key of D and broadcasts it to its neighbor. Eventually an RREQ packet should get to D. On receiving an RREQ packet, D verifies the signatures, decrypts the encrypted fields and verifies that the nodes in the path have the minimum required trust level. If these validation operations succeed, it constructs a route reply (RREP) packet and a flow-id and encrypts the RREP and the flow-id with the public keys of the nodes in the reverse path to S (in the order that the nodes should receive the RREP packet); then D signs the encrypted RREP and broadcasts it to its neighbors. When an intermediate node n_i receives the RREP it will attempt to decrypt it; if the decryption operation fails, n_i discards the packet; otherwise, it updates its routing table, removes its part of the RREP and broadcasts it to its neighbor. Eventually, the RREP should get to the source S which will verify the signature and decrypts the RREP to ascertain the route it seeks (Boukerche, 2004).

SDAR

Boukerche *et al.,* (2005) 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. When a node S desires to discover a routing path to a destination D, S constructs a routing request packet (RREQ), part of which is un-encrypted and the other part encrypted. The un-encrypted part of the RREQ contains necessary routing information such as the trust level requirement of the message and a one-time public key T P K. The encrypted part of the RREQ packet contains the destination ID, a symmetric key Ks generated by S and the private key T SK for the one-time public key T P K, plus other information. Part of the encrypted portion of the message is encrypted with the public key for the destination D and the other portion is encrypted with the symmetric key Ks. S then encrypts the entire packet with the shared key for the appropriate security level of the message and broadcasts it to its neighbors. When an intermediate node n_i receives the RREQ packet, it discards the message if it is not able to decrypt it. If n_i succeeds in decrypting the message, n_i adds its ID and a session key n_i then signs the portion it added and encrypts it with the one-time public T P K embedded in the un-encrypted portion of the RREQ packet; n_i then encrypts the entire message with the key (of the appropriate security) it shares with it neighbors and broadcasts the message. Eventually the message should get to D which decrypts the message with the appropriate keys. After verifying the signatures, D constructs a route reply (RREP) and encrypts it, first using the symmetric keyK_sS attached, then encrypts it again using the session keys K_i's in the order that the corresponding intermediate node should receive the RREP packet. D then forwards the RREP to its neighbor. The neighbor which is the intended next-hop will decrypt its portion of the packet and forwards it to its neighbors (one of which will be able to partly decrypt it). The process continues until the RREP gets to the source node S which will be able to decrypt the entire packet and ascertain the route it seeks (Boukerche, 2004).

Li and Singhal (2006) proposed a secure routing scheme which utilizes recommendation and trust evaluation to establish trust relationships between network entities. The scheme uses a distributed authentication model which operates as follows: each network node maintains a trust table which assigns a quantitative trust value to known network entities. If a node S desires to know the trust value of a node n_i and n_i is not in S trust table, S sends out a trust query message—to ascertain n_i's trust value—to all the trustworthy nodes in S trust table.

When a node n_j receives the trust query message, if n_i is in its trust table, it sends the indicated trust value to S; otherwise it sends out a trust query message— requesting the trust value of n_i—to all the trustworthy nodes in its trust table. The process continues recursively until eventually a node which has n_i in its trust table forwards the trust value to the node which requested the info, which will in turn forward it to the node which sent it the trust query message; and so on, until eventually the response gets to S. S consequently uses the responses to compute a trust value for the node in question. This distributed authentication model is used to determine the trustworthiness of the network nodes. The end result being that nodes which are considered untrustworthy are excluded from routing paths.

SLSP

The Secure Link State Protocol (SLSP) (Papadimitratos, 2003) 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) (Koltsidas) 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. To operate efficiently in the absence of a central key management, SLSP provides for each node to distribute its public key to nodes within its zone. Nodes periodically broadcast their certified key, so that the receiving nodes validate their subsequent link state updates. As the network topology changes, nodes learn the keys of nodes that move into their zone, thus keeping track of a relatively limited number of keys at every instance.

SLSP defines a secure neighbor discovery that binds each node V to its Medium Access Control (MAC) address and its IP address, and allows all other nodes within transmission range to identify V unambiguously, given that they already have EV. Nodes advertise the state of their incident links by broadcasting periodically signed link state updates (LSU). SLSP restricts the propagation of the LSU packets within the zone of their origin node. Receiving nodes validate the updates, suppress duplicates, and relay previously unseen updates that have not already propagated R hops. Link state information acquired from validated LSU packets is accepted only if both nodes incident on each link advertise the same state of the link (Jawandhiya, 2010).

Incentive-based Schemes

Incentives are normally implemented using credits that are given to nodes that cooperate and forward packets. In turn network services such as routing is provided only to those nodes that have good credit. However, in an incentive based solutions, a node at an unfavorable location may not get enough packets to forward and thus may never be able to get credits to forward its own packets. Also in the absence of a central authority, ensuring tamper-proof manipulation of the crediting system may be complicated. 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 (Balasubramaniam) (Chen, 2004).

Buttyan and Hubaux (2003) 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. The operation of the scheme is as follows: when a node S desires to send a packet to a destination D, if the number of intermediate nodes on the path from S to D is n, then S's nuglet counter must be greater than or equal to n in order for S to send the packet.

If S has enough nuglets to send the packet, S decreases its nuglet counter by n after sending the packet. On the other hand, S increases its nuglet counter by one each time S forwards a packet on behalf of other nodes. The value of a nuglet counter must be positive; therefore, it is within a node's interest to forward packets on behalf of other nodes, and refrain from sending large number of packets to distant destinations.

Zhong, Chen and Yang presented Sprite: A Simple, Cheat-Proof, Credit- Based System for MANETs (Zhong, 2003).

Sprite provides incentive for MANET nodes to cooperate and report actions honestly. Sprite requires a centralized entity called a Credit Clearance Service (CCS) (Janzadeh, 2008; Kaushik, 2011) which determines the charge and credit involve in sending a message. The basic operation of Sprite is as follows: when a node receives a message, the node keeps a receipt of the message. Later when the node has a fast connection to a CCS, it reports to the CCS the message it has received/forwarded by uploading its receipt. The CCS then uses the receipt to determine the charge and credit involve in the transmission of the message.

Table 5: Summary of routing security analysis

Schemes	**Comments**
Schemes which do not address packet dropping	SRP (Papadimitratos, 2002), SEAD (Hu, 2002), SAODV (Zapata, 2001), Bliss (Capkun, 2003), Tiara (Ramanujan, 2000) Ariadne (Hu *et al.*, 2002), ARAN (Sanzgiri, 2002), Binkley and Venkatraman (2001) schemes do not address packet dropping. Byzantine Failure Resilient Protocol (Awerbuch, 2002), SPAAR (Yasinsac, 2002)
Trust-based Schemes	SAR (Yi *et al.,* 2002) requires shared group keys; therefore it is subjected to the key management issues outlined in Section 4.1.1. Pirzada and Nekkanti (2004) do not provide protection against packet dropping; SDAR (Boukerche, 2005) is subjected to the short comings indicated below for Marti et al scheme; Li *et al.,* (2006) 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	Buttyan *et al.,* (2003) requires tamper resistant hardware and Zhong *et al.,* (2003) 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.,* (2000) 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) limited transmission power, 4) false misbehavior, 5)collusion, and 6) Partial dropping. "Buchegger *et al.,* (2002) scheme does not provide protection against false accusations. The probing technique (Awerbuch *et al.,* 2002; Just and Patwardhan, 2003) schemes (Zhong, 2003) utilize, is ineffective against intelligent adversaries which selectively drop packets, since the probing packets are not completely indistinguishable from other data packets.

Schemes which Employ Detection and Isolation Mechanisms

This section contains a brief description of schemes which utilize detection and isolation techniques. We commence the review with an earlier proposal (Nadeema, 2013).

Marti *et al.,* (2002) proposed a scheme for militating 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 (Anitha, 2013; Marti, 2000). 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

Review Article

communications to and from even if those communications do not involve n_i. 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 n_i does not hear the transmission going from to then it is likely that n_i 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 assigns 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 (2002) 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 (Rajaram, 2010).

Awerbuch *et al.*, (2002) 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.

Just and Kranakis (2003) and Kargl *et al.*, (2004) proposed schemes for detecting selfish or malicious nodes in an ad hoc network. The schemes involve probing mechanisms which are similar in functionality to that of Awerbuch *et al.*, (2002) above.

Patwardhan and Iorga, 2005) presented a secure routing protocol called SecAODV (Uikey, 2013; Nayak, 2011). SecAODV is based on AODV but unlike the latter, it requires each node in the MANET to have a static IPv6 address. The scheme allows source and destination nodes to establish secure communication channel based on the concept of Statistically Unique and Cryptographically Verifiable (SUCV) (Montenegro) identifiers (Messerges, 2003) which ensures secure binding between an IPv6 address and a key, without requiring any trusted certificate authority (CA). Secured AODV also provides IDS (intrusion detection system) for monitoring the nodes' activities.

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 5 gives a summary of various types of secured schemes discussed above, their characteristics and examples.

Conclusion

Mobile Ad hoc networks (MANETs) have several advantages compared to traditional **wireless** networks (Tyagi, 2013). These include ease of deployment, speed of deployment and decreased dependency on a fixed infrastructure. There have been many studies done in this area to improve the quality and efficiency of the routing protocols in MANETs. However 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 examined the available secure routing protocols in MANETs such as Secure On- Demand Routing Protocol – Ariadne, Secure Ad hoc On- demand Distance Vector routing protocol – SAODV, Security Aware Routing Protocol – SAR, Secure Efficient Distance Vector Routing – SEAD, Secure Link State Routing protocol – SLSP, On-Demand Secure Routing Protocol Resilient to Byzantine Failures, Authenticated Routing for Ad-hoc Networks – ARAN, Secure Position Aided Ad hoc Routing – SPAAR. Thereby dividing the secured routing schemes into four different parts. We identify the advantages and disadvantages of each protocol as shown in the previous Tables.

A large number of on-demand routing protocols have already been proposed. Each protocol has its own key features, which may add positive or negative sides to the protocol. However, on-demand routing protocols 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 militate 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. However not all these security solutions provide complete security for MANETs.

ACKNOWLEDGEMENT
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.

REFERRENCES

Aad I, Hubaux JP and Knightly EW (2004). Denial of Service Resilience in Ad Hoc Networks. Proceedings of the ACM 10th Annual International Conference. (MobiCom-2004), Philadelphia, PA.
Aarti and Tyagi SS (2013). Study of MANET: Characteristics, Challenges, Application and Security Attacks. *International Journal of Advanced Research in Computer Science and Software Engineering*, Research Paper **3**(5) 252-257, Available at: www.ijarcsse.com.
Agrawal S, Jain S and Sharma S (2011). A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. *Journal of Computing*. Available: https://sites.google.com/site/journalofcomputing/www.journalofcomputing.org **3**(1) 41-47
Alam MR (2011). Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks. This thesis is presented for the Degree of Master of Philosophy of Curtin University of Technology.
Al-Shahrani AS (2011). Rushing Attack in Mobile Ad Hoc Networks. Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on Date of Conference: Nov. 30 2011-Dec. 2 2011 752 - 758
Al-Shurman M, Yoo SM and Park S (2004). Black Hole Attack in Mobile Ad Hoc Networks. ACMSE’04, April 2-3, 2004, Huntsville, AL, USA 96-97.
Anitha D and Punithavalli M (2013). A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS. *International Journal of Computer Science and Mobile Computing (IJCSMC)* **2**(3) 112 – 119.
Arya M and Jain YK (2011). Gary hole attack and prevention in Mobile Adhoc Network. *IJCA* **27**(10).
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).
Bala A, Bansal M and Singh J (2009). Performance Analysis of MANET under Blackhole Attack. Networks and Communications, 2009, NETCOM '09. First International Conference on: 27-29 Dec. 2009 141 – 145.
Balasubramaniam A, Ghosh J and Wang X (No Date). A Reputation Based Scheme For Stimulating Cooperation In Manets. University at Buffalo.

Baras JS, Radosavac S and Theodorakopoulos G (2007). Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR. In: IEEE Military Communications Conference (MILCOM) 1-7.

Basagni S, Conti M, Giordono S and Stojmenovic I (2004). Mobile Ad Hoc Networking. IEEE Press, John Wiley & Sons, New York.

Binkley J and Trost W (2001). Authenticated ad hoc routing at the link layer for mobile systems. *Wireless Networks* **7**(2) 139–145.

Bonny J and Krichane M (2004). Securing Ad Hoc Networks Using Ariadne. Swiss Institute of Technology (EPFL) Lausanne, Switzerland.

Boora S and Ohri S (2013). A Survey of Layer Specific and Cryptographic primitive attacks and their countermeasures in MANETS. *International Journal of P2P Network Trends and Technology (IJPTT)* Available: http://www.ijpttjournal.org **3**(4) 192-198

Boukerche A, El-Khatib K, Xu L and Korba L (2004). SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks. University of Ottawa, *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)* 0742-1303/04 $ 20.00 IEEE.

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.

Brooke J and Hashmi S (2010). Towards Sybil Resistant Authentication in Mobile Ad-Hoc Networks. The International Conference on Emerging Security Information, Systems and Technologies.

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.

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.

Capkun S and Hubaux JP (2003). Building Secure Routing out of an Incomplete Set of Security Associations. WiSE'03, San Diego, California, USA.

Carter S and Yasinsac A (2002). Secure Position Aided Ad hoc Routing. Computer Science Department, Florida State University, This material is based upon work supported in part by the U.S. Army Research Laboratory and the U.S. Army Research, Office under grant number DAAD19-02-1-0235.

Carter SH (2002). Secured position aided ad hoc routing. Thesis submitted to Folrida State University, Major professor: AlecYasinsac, FALL SEMESTER 2002, Degree of masters, Computer science department.

Chandure OV and Gaikwad VT (2011). A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET. *IJCSIT* **2**(6).

Chatterjee P (2009). Trust Based Clustering And Secure Routing Scheme For Mobile Ad Hoc Networks. *International Journal of Computer Networks & Communications (IJCNC)* **1**(2) 84-97.

Chen K and Nahrstedt K (2004). iPass: an incentive compatible auction scheme to enable packet forwarding service in MANET. Distributed Computing Systems, 2004, *Proceedings of the 24th International Conference on Date of Conference* 534 – 542.

Chiu HS and Lui K (2006). DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks. In: *Proceedings of International Symposium on Wireless Pervasive Computing* 6-11.

De I and Barman Roy D (2011). Comparative study of Attacks on AODV-based Mobile Ad Hoc Networks. *International Journal on Computer Science and Engineering (IJCSE)* **3**(1) 313-322.

Deering S (1991). ICMP router discovery messages. Internet Request for Comments (RFC 1256).

Denko M K (No Date). Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme. In: *Systemics, Cybernetics and Informatics* **3**(4) 1-9.

Gagandeep, Aashima and Kumar P (2012). Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review. *International Journal of Engineering and Advanced Technology (IJEAT)* **1**(5).

Guan Q, Yu RF, Jing S and Leung VCM (2012). Joint Topology on Vehicular technology. *IJCNWC* **61**(6).

Guette G and Ducourthial B (2007). On the Sybil attack detection in VANET. IEEE International Conference on Mobile Adhoc and Sensor Systems Conference.

Hu Y, Perrig A and Johnson D (2002). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)* 3–13.

Hu Y, Perrig A and Johnson D (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks. In: *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking* (Mobicom 2002) 12–23.

Hu Y, Perrig A and Johnson D (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In: *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies* 1976–1986.

Hu YC, Perrig A and Johnson DB (2003). Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, September 19, 2003, San Diego, California, USA. Copyright 2003 ACM 1581137699/03/0009.

Hu YC and Perrig A (2004). A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security and Privacy* **2**(3) 28-39.

Hu YC, Perrig A and Johnson DB (2006). Wormhole Attacks in Wireless Networks. *IEEE Journal on Selected Areas in Communications* 370-380 **24**(2).

Huang Y and Lee W (2004). Attack Analysis and Detection for Ad Hoc Routing Protocols 1-21

Huang J, Seberry J, Susilo W and Bunder MW (2005). Security Analysis of Michael: The IEEE 802.11i Message Integrity Code. 01/2005; In: *Proceeding of Embedded and Ubiquitous Computing - EUC 2005 Workshops*, EUC 2005 Workshops: UISW, NCUS, SecUbiq, USN, and TAUES, Nagasaki, Japan, December 6-9, 2005, Source: DBLP.

Janzadeh H, Fayazbakhsh K, Dehghan M and Fallah MS (2008). A secure credit-based cooperation stimulating mechanism for MANETs using hash chains, Future Generation Computer Systems 25 (2009) 926-934, Contents lists available at Science Direct. *Future Generation Computer Systems Journal* Available: www.elsevier.com/locate/fgcs.

Johnson D and Maltz D (1996). Dynamic source routing in ad-hoc wireless networks routing protocols. In: *Mobile Computing*, Kluwer Academic Publishers 153–181.

Just M, Kranakis E and Wan T (2003). Resisting malicious packet dropping in wireless ad hoc networks. In: *Proceedings of ADHOCNOW'03*.

Kargl F, Klenk A, Schlott S and Weber M (2004). Advanced detection of selfish or malicious nodes in ad hoc networks. In: *Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)* 152–165.

Kaufman C, Perlman R and Speciner M (2002). Network Security Private Communication in a Public World. Prentice Hall PTR, A division of Pearson Education, Inc.

Kaushik R and Singhai J (2011). MODSPIRITE: A Credit Based Solution to Enforce Node Cooperation in an Ad-hoc Network, *IJCSI International Journal of Computer Science Issues* **8**(2) 295-302. Available: www.IJCSI.org .

Khirasariya HR (2013). Simulation Study of Jellyfish Attack. In: *Manet (Mobile Ad Hoc Network) Using AODV Routing Protocol*. *Journal of Information, Knowledge and Research in Computer Engineering* **02**(02) 344-347.

Koltsidas G and Pavlidou FN (No Date). Single-path and Multipath Routing Algorithms form Mobile Ad Hoc Networks.

Konate K and Gaye A (2011). A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile AdHoc Network. *International Journal of Future Generation Communication and Networking* **4**(2) 69-80.

Krawczyk H, Bellare M and Canetti R (1997). Hmac: Keyed-hashing for message authentication. Internet Request for Comments (RFC 2104).

Lai WS, Lin CH, Liu JC, Huang YL and Chou MC (2008). I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks. *International Journal of Multimedia Ubiquitous Engineering* **3**(4) 45-54.

Lamport L (1981). Password authentication with insecure communication. *Communications of ACM* **24**(11) 770–772.

Lamport L, Shostak RE and Pease M (1982). The Byzantine Generals Problem. *ACM Transactions of Programming Languages and Systems* **4**(3) 382-401.

Li H and Singhal M (2006). A secure routing protocol for wireless ad hoc networks. In Proceeding of the 39th Hawaii International, International Conference on Systems Science (HICSS-39 2006) 225–234.

Llewellyn-Jones D, Merabti M and Abbas S (2009). Signal Strength Based Sybil Attack Detection in Wireless Ad-Hoc Networks. International Conference on Developments in eSystems Engineering.

Lokulwar P and Shelkhe V (2012). Security Aware Routing Protocol for Manet Using Asymmetric Cryptograpy Using RSA Algorithm. *BIOINFO Security Informatics* **2**(1) 11-14.

Mahajan V, Natu M and Sethi A (2008). Analysis of wormhole intrusion attacks in MANETS. In: *IEEE Military Communications Conference (MILCOM)* 1-7.

Makkar A, Bhushan B, Shelja and Taneja S (2011). Behavioral Study of MANET Routing Protocols. *International Journal of Innovation, Management and Technology* **2**(3) 210-216.

Mamatha GS and Sharma SC (2010). Network layer Attacks and Defense Mechanisms in MANETs- A Survey. *International Journal of Computer Applications* **9**(9) 12-17.

Marti S, Giuli TJ, Lai K and Baker M (2000). Mitigating routing misbehavior in mobile ad hoc networks. In: *Mobile Computing and Networking* 255–265.

Maulik R and Chaki N (2011). A Study on Wormhole Attacks in MANET. *International Journal of Computer Information Systems and Industrial Management Applications* **3** 271-279 © MIR Labs. Available: www.mirlabs.net/ijcisim/index.html.

Mehla S, Gupta B and Nagrath P (2010). Analyzing security of Authenticated Routing Protocol (ARAN). *(IJCSE) International Journal on Computer Science and Engineering* **02**(03) 664-668.

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.

Messerges TS, Cukier J, Kevenaar TAM, Puhl L, Struik R and Callaway E (2003). A security design for a general purpose, self-organizing, multihop ad hoc wireless network. In: *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*.

Milanovic N, Malek M, Davidson A and Milutinovic V (2004). Routing and security in mobile ad hoc networks. In: *IEEE Computer Society Journal* **0018-9162**(04) 61-65.

Min Z and Jiliu Z (2009). Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks, Information Engineering and Electronic Commerce, 2009, IEEC '09, International Symposium on: 16-17 26 – 30.

Montenegro G and Castelluccia C (No Date). Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses1-13.

Mukherjee B, Heberlein LT and Levitt KN (1994). Network Intrusion Detection, IEEE Network 26-41.

Muraleedharan R and Osadciw LA (2006). Jamming Attack Detection and Countermeasures. In: *Wireless Sensor Network Using Ant System,* Department of Electrical Engineering and Computer Science Syracuse University.

Murthy CSR and Manoj BS (2006). Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education.

Nadeema A and Howarthb MP (2013). An Intrusion Detection & Adaptive Response Mechanism for MANETs. Preprint submitted to Elsevier 1-28

Nayak SD and Gupta RK (2011). Sec, AODV for MANETs using MD5 with Cryptography. *International Journal of Computer Technology and Applications, IJCTA* **2**(4) 873-878. Available: online@www.ijcta.com.

Nekkanti RK and Lee CW (2004). Trust based adaptive on demand ad hoc routing protocol. In: *Proceedings of the 42nd annual Southeast regional conference* 88–93.

Papadimitratos P and Haas ZJ (2002). Secure Routing for Mobile Ad Hoc Networks. *Mobile Computing and Communications Review* **6**(4).

Papadimitratos P and Haas ZJ (2003). Secure Link State Routing for Mobile Ad Hoc Networks. *Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks*, IEEE Press 27–31.

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.

Perrig A, Canetti R, Tygar D and Song D (2002). The tesla broadcast authentication protocol. Cryptobytes (RSA Laboratories, Summer/Fall 2002) **5**(2) 2–13.

Perkins C and Bhagwat P (1994). Highly dynamic destination-sequenced distance- vector routing (dsdv) for mobile computers. In: *Proceedings of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications* 234–244.

Perkins C and Royer E (1999). Ad hoc on-demand distance vector routing. In: *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999)* 80–100.

Piro C, Shields C and Levine BN (2006). Detecting the Sybil Attack in Mobile Ad hoc Networks. This work was supported in part by NSF grants CNS-0133055, CNS-0534618 and CNS-0087639.

Pirretti M, Zhu S, Narayanan V, McDaniel P and Kandemir M (2006). The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense.

Pirzada AA and McDonald C (2004). Establishing trust in pure ad-hoc networks. In: *Proceedings of the 27th conference on Australasian computer science (CRPIT '04)* 47–54.

Rai AK, Tewari RR and Upadhyay SK (2010). Different Types of Attacks on Integrated MANET-Internet Communication. *International Journal of Computer Science and Security (IJCSS)* **4**(3) 265-274.

Rai AP, Srivastava V and Bhatia R (2012). Wormhole Attack Detection in Mobile Ad Hoc Networks. *International Journal of Engineering and Innovative Technology (IJEIT)* **2**(2) 174-179.

Rajaram A and Gopinath S (2010). Efficient Misbehavior Detection System for MANET. *International Journal for Advances in Computer Science* **1**(1) 12-16 © IJACS 2010 - All rights reserved.

Ahamad A, Bonney J, Hagelstrom R and Thurber K (2000). Ranga Ramanujan | Architecture Technology Corporation, Eden Prairie MN, USA, MILCOM 2000. *21st Century Military Communications Conference Proceedings* **2** 660-664.

Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J and Nygard K (2008). Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, *IJSEIA* **2**(3). Available: www.sersc.org/journals/IJSEIA/vol2_no3_2008/4.pdf.

Rangara RR, Jaipuria RS, Yenugwar GN and Jawandhiya PM (2010). Intelligent Secure Routing Model for MANET. 978-1-4244-5539-3/10/$26.00 ©2010 IEEE.

Razak SA, Furnell SM and Brooke PJ (No Date). Attacks against Mobile Ad Hoc Networks Routing Protocols. Network Research Group, University of Plymouth.

Resnick P, Kuwabara K, Zeckhauser R and Friedman E (2000). Reputation systems. *Communications of ACM* **43**(12) 45–48.

Reyzin L and Reyzin N (2002). Better than biba: Short onetime signatures with fast signing and verifying. In 7th Australian Conference on Information Security and Privacy, *LNCS* **2384** 144–153.

Saha HN, Bhattacharyya D and Banerjee PK (2010). Semi-Centralized Multi-Authenticated RSSI Based Solution to Sybil Attack. *International Journal of Computer Science & Emerging Technologies* **1**(4).
Sahu M and Lal RC *et al.*, (2012). Controlling ip spoofing through packet filtering. *International Journal of Computer Techology & Applications, IJCTA* **3**(1) 155-159, Available: online@www.ijcta.com 2229-6093.
Sanzgiri K, Dahill B, Levine B and Belding-Royer E (2002). A secure routing protocol for ad hoc networks. In: *Proceedings of 10th IEEE International Conference on Network Protocols (ICNP)*.
Schütte M (2006). Detecting Selfish and Malicious Nodes in MANETs. Seminar: Sicherheit, In: Selbstorganisierenden Netzen, Hpi/Universität Potsdam, Sommersemester 1-7.
Shanmuganathan V and Anand T (2012). A Survey on Gray Hole Attack in MANET. *IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC)* **2**(6) 647-650.
Smaha SE and Haystack (1988). An Intrusion Detection System. In Fourth Aerospace Computer Security Applications Conference, Tracor Applied Science Inc., Austin, Texas 37-44.
Sofi S, Malik E, Baba R, Baba H and Mir R (2012). Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation. *ICCIT*.
Templeton SJ and Levitt KE (2003). Detecting Spoofed Packets.
Thalor J and Ms Monica (2013). Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering* **3**(2) 137-142.
Uikey C (2013). Performance Evaluation of Routing Protocol for Mobile Ad-Hoc Network. *IJCSN International Journal of Computer Science and Network* **2**(4) 59-65 2277-5420, Available: www.ijcsn.org.
Ullah I and Rahaman SU (2010). Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols. In *Master Thesis Electrical Engineering Thesis* no: **MEE 10 62**.
Venkatraman L and Agrawal DP (2001). An optimized inter-router authentication scheme for ad hoc networks. In: *Proceedings of the Wireless* 129–146.
Vishnu K and Paul AJ (2010). Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks. *IJCA* **1**(22).
Wang X, Feng D, Lai X and Yu H (2004). Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Cryptology ePrint archive: Report 2004/199, Available: http://eprint.iacr.org/2004/199.
Wu B, Chen J, Wu J and Cardei M (2006). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Springer.
Xiao Y and Shen X (2006). Wireless/mobile network security.
Yan Z, Zhang P and Virtanen T (2003). Trust evaluation based security solution in ad hoc networks. In Proceedings of the 7th Nordic Workshop on Secure IT Systems (NordSec 2003).
Yan Z (No Date). Security in Ad Hoc Networks. Networking Laboratory. Helsinki University of Technology.
Yasinsac A and Carter S (2002). Secure Position Aided Ad hoc Routing. Florida State University, Available: http://www.cs.fsu.edu/~yasinsac/Papers/CY02.pdf.
Yang H, Luo HY, Ye F, Lu SW and Zhang L (2004). Security in mobile ad hoc networks: Challenges and solutions. UCLA.
Yi S, Naldurg P and Kravets R (2002). Integrating quality of protection into ad hoc routing protocols. In: *Proceedings of the 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002)* 286–292.
Yong C, Chuanhe H and Wenming S (2007). Trusted Dynamic Source Routing Protocol Wireless Communications, Networking and Mobile Computing, 2007, WiCom 2007. International Conference on Date of Conference 1632 – 1636.

Zapata MG (2001). Secure ad hoc on-demand distance vector (soadv) routing. INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt.

Zapata MG (2002). Secure ad hoc on-demand distance vector routing. *ACM Mobile Computing and Communications Review* **6**(3)106–107.

Zapata M and Asokan N (2002). Securing ad hoc routing protocols. In: *Proceedings of the ACM Workshop on Wireless Security (WiSe'02)*.

Zhang Z (2011). Mobile Ad-Hoc Networks: Protocol Design. Chapter 22: A Novel Secure Routing Protocol for MANETs, University of Southern Queensland, Australia 455-466. Available: www.intechopen.com, Publisher InTech, Published online 30, January, 2011, Published in print edition.

Zhong S, Chen J and Yang Y (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks. In: *Proceedings of IEEE INFOCOM*.