CHAPTER 2
LITERATURE REVIEW

2.1 INTRODUCTION

Efficient routing of packets is a primary challenging task for MANET because of its features like open medium, dynamic changing of its topology, lacks of central authority, limited transmission range and energy resources. Due to the limited transmission range multiple hops may be needed for one node to forward packets with another node across the network. In such an environment, each node operates not only as a host but also as a router to discover and maintain routes to the other nodes in the network. Each node participates in MANET routing protocol, allows it to discover multi-hop paths through the network to any other node. So, the primary goal of MANET routing protocol is to discover a correct and efficient path between source node and destination node in order to deliver a packet in time safely. Thus, the routing security plays an important role in MANETs. There are basically two categories of MANET routing protocols: proactive and reactive (Royer et al 1999, Ismail et al 2007). But, these protocols assume all the nodes trusted and cooperative. As a result, a malicious attacker (Kannhavong et al 2007, Mishra & Sharma 2010, Agrawal et al 2011) can readily become a part of routing process and disrupt network operations by intentionally disobeying the protocol specifications. To countermeasure the various routing attacks, there are various routing protocols have been developed in the past. These protocols are broadly categorized as secure routing protocols and anonymous secure routing protocols.
In the same way, routing is a challenging task when MANET is integrated with Internet (Chlamtac 2003, Rahman Khan et al 2008). The MANET routing protocols cannot be used directly for routing the packet from a mobile node form MANET to Internet. Because, the MANET routing protocols has been designed to discover and maintain multi-hop paths within the MANET. There are various techniques had been introduced to integrate MANET and Internet in the past but those techniques do not focusing privacy and security factors.

2.2 SECURE ROUTING PROTOCOLS FOR MANET

A number of secure routing schemes have been developed in the past to counter measure the various attacks and to improve the performance of routing protocols in MANETs. These protocols are discussed in this section.

Marti et al (2000) proposed a technique to mitigate routing misbehavior in MANETs. This technique uses two modules such as watchdog and pathrater. The nodes are in a promiscuous mode where the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. Based on the watchdog’s feedback the pathrater module rates every path in its cache and subsequently chooses the path that avoids the misbehaving nodes. Due to its reliance on overhearing raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power.

Hu et al (2003) proposed a secure efficient ad hoc distance vector routing protocol against multiple uncoordinated attackers creating incorrect routing state in any other node, in spite of active attackers or compromised nodes in the network. If the nodes are compromised in the network, then there is possibility of DoS attacks. This attacks attempts to consume network bandwidth or processing time. The proposed protocol used an efficient one-
way hash functions and don’t use asymmetric cryptographic operations in the protocol. This protocol is based on the Destination-Sequenced Distance-Vector routing protocol.

Zapata & Asokan (2002) proposed a securing ad hoc routing protocol, which has been designed to use a digital signature to authenticate most fields of a route request and route reply packets and uses hash chains to authenticate the hop count. This protocol countermeasure against certain impersonation attacks.

Hu & Peerig (2005) presented a secure on-demand routing protocol for ad hoc networks for node compromise attacks based on efficient symmetric cryptography. This protocol authenticate routing messages using any one of the three method such as shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication and digital signatures. The route discovery process of this protocol is based on dynamic Source routing protocol. Each mobile node helps using route maintenance to discover problems with each selected route.

Sanzgiri et al (2005) proposed an authenticated routing for ad hoc networks which is based on AODV routing protocol. In this protocol, every node has a certificate signed by a trusted authority, which associates its IP address with a public key. During a route discovery, the source node broadcasts a signed route request packet. This includes the destination node, certificate, nonce and timestamp. Each node that forwards the route request packet checks the signature because this protocol uses public-key cryptography for authentication. It is particularly vulnerable to DoS attacks based on flooding bogus control packets. If the nodes do not verify signature, an attacker can force some node to discard the control packets it receives.
Acs et al (2006) proposed a provably secure on-demand source routing protocol against security attacks in MANETs. This protocol works against active and passive attackers in MANETs. This framework focused on on-demand source routing protocols, but similar principles can be applied to other types of protocols.

Liu et al (2007) proposed an acknowledgement-based approach for the detection of routing misbehavior in MANETs. This protocol mainly focuses to identify and exclude the selfish nodes which are participating in en-route. The protocol is designed based on 2 acknowledgement scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The idea of using this scheme in this work is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged.

Zhao et al (2008) proposed a secure routing protocol in proactive security approach. This protocol use identity-based cryptography for encryption/decryption and signature/verification for its specific suitability for MANETs. The protocol is designed to start from a prerequisite secure status and fortifies this status by protecting packets using identity-based cryptography and updating cryptographic keys using threshold cryptography periodically or when necessary. This scheme can only be applied to pre-planned ad hoc networks such as those for policemen and fire-fighters.

Nakayama et al (2009) proposed an anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals. This learning process involves calculating the projection distances based on multidimensional statistics using weighted
coefficients and a forgetting curve. This concept differentiates an attack state from its normal state.

Chauhan et al (2010) proposed a secure on-demand routing protocol to secure source routing in MANETs. The objective of this protocol is to authenticate the source, destination and intermediate nodes in route list of route request packet. Then to detect any kind of modification or fabrication in route lists from attackers. This protocol for mobile ad hoc networks allows intermediate nodes to authenticate its predecessor node, and then forward the route request message. Finally destination node authenticates all the nodes that make up route. This protocol is based on PKC algorithms require more calculation than the symmetrical algorithms. Therefore, it consumes much battery power than protocols based on symmetric algorithms.

Djahel et al (2011) discussed about mitigating packet dropping problem in MANETs. This paper discussed the proposals and challenges in MANETs. In this paper, a comprehensive survey investigation on the state-of-the-art countermeasures to deal with the packet dropping attack. Furthermore, this examines the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a sophisticated attack.

Gohari et al (2011) proposed reliability map routing for spatial routing through difficult terrains for MANETs. This protocol reactively discovers routes over spatial cells whose local reliabilities are distributed throughout the network via a fast dissemination algorithm. This protocol uses spatial approach where reliability and trust are attributed to space rather than to nodes. This protocol is mainly designed for high density and high mobility scenarios.
Lacuesta et al (2011) proposed a two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks. This protocol based on the computational cost such as the weak and the strong one. These computational costs based on the trust of the users and guarantee the secure protocol between the users and the mesh routers. Both protocols provide authenticity and integrity except anonymity.

Feng et al (2012) proposed a multicast routing protocol which is based on a priori creation of a multicast tree. This requires the individual nodes to maintain state information. This protocol uses a list of the multicast members' addresses, embedded in packet headers, to enable receivers to decide the best way to forward the multicast traffic.

Lacuesta et al (2013) proposed a secure protocol for spontaneous wireless ad hoc networks. This protocol uses a hybrid symmetric/asymmetric scheme in addition to the trust between users to exchange the secret keys. In addition, the trust between users has been used in order to exchange the initial data and also to exchange the secret keys that will be used to encrypt the data. Trust is based on the first visual contact between users. The protocol includes all functions needed to operate without any external support.

2.3 ANONYMOUS ROUTING PROTOCOLS FOR MANET

This section discusses the anonymous secure routing techniques that have been proposed to countermeasure various attacks and to improve the performance of the pouting protocols in MANETs.

Ko & Vaidya (2000) proposed a location aided routing in MANETs. This paper suggested an approach to utilize location information to improve performance of routing protocols for ad hoc networks. This protocol limits the search for a new route to a smaller zone by using location
information of the ad hoc network. This reduces the reduction in the number of routing messages. This protocol is designed based on two techniques such as location aided routing scheme 1 and 2 to determine the request zone and also suggest potential optimizations to the proposed algorithms.

Kong & Hong (2003) proposed an anonymous on-demand routing protocol which is based on “broadcast with trapdoor information” to achieve an untraceable and intrusion tolerant protocol for MANETs deployed in a hostile environment. This protocol uses a route pseudonym approach and a symmetric key boomerang type onion, a layered cryptographic structure on which appending and peeling off are performed by the same forwarding nodes. It prevents strong adversaries from tracing a packet flow back to its sender or receiver and ensures that adversaries are unable to identify local message-forwarding nodes. However, it has a trapdoor and anonymity issue.

Boukerche et al (2004) proposed a secure distributed anonymous routing protocol for hostile environment. In this protocol, the sender node initiate path establishment by broadcasting a path discovery message with specific trust requirements to neighboring nodes. The purpose is to ensure only trustworthy nodes construct routing paths to preserve node anonymity. It uses a public key cryptography, so it suffers from high computational complexity when the number of route request packets gets large for forwarding nodes. The long private key leads to high computational complexity when forwarding nodes create encrypted signature routing messages during path discovery. The part of the routing message may be deleted and modified by a forwarding node or adversary.

Zhu et al (2004) proposed an anonymous and secure routing protocol for MANETs. This protocol is based on asymmetric cryptosystems and is designed to ensure the security of discovered routes and preserve
sender, receiver, communications and location anonymity against known passive and active attacks. However, it has the disadvantages of large computational latency, key size, and power consumption and an inability to dynamically repair failed routes.

Boukerche et al (2004) presented an anonymity enabling scheme for wireless ad hoc networks. This is an anonymous routing protocol, similar to onion routing used in wired networks. This protocol establishes trust and avoids untrustworthy nodes during the route discovery process. The major objective of our protocol is to allow trustworthy intermediate nodes to participate in the routing protocol without jeopardizing the anonymity of the communicating nodes.

Kong et al (2005) indicates that the mobility changes anonymity so, the mobile ad hoc networks need efficient anonymous routing protocol. The authors indicates that the network needs more anonymity protections like (1) venue anonymity in addition to conventional identity anonymity, (2) privacy of node’s location and motion pattern, and (3) privacy of ad hoc network topology. So, an attention is needed to realize efficient and anonymous routing in mobile ad hoc networks.

Mu et al (2005) proposed secure anonymous mobile ad-hoc networks. This paper considers the following features such as any outsider can be convinced that the node is indeed in the group and any outsider can send a message back to the node in the group.

Song et al (2005) proposed an anonymous dynamic source routing protocol. This protocol is a combination of on-demand, MIX-net onion, no neighbor exposure, and crypto-protected receiver. It is composed of the security parameter route establishment, anonymous source/destination route discovery, and anonymous cryptographic onion data transfer protocols for
MANETs. In the route establishment protocol, an adversary performing an active modification or replay attack or executing the passive eavesdropping attack. In the route discovery process, an adversary cannot modify the public key, trapdoor or onion and a replay attack is detectable. In the data transfer phase, the onion protects all data communications.

Rahman & Mambo (2006) proposed an anonymous on-demand Position-based routing in MANETs. This protocol keeps routing nodes anonymous, thereby preventing possible traffic analysis. A time variant temporary identifier is computed from time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and temporary identity is used for establishing the route for sending data: a receiver hand shake scheme is designed for determining the next hop on-demand with use of the temporary identity.

Zhang et al (2006) proposed an anonymous on-demand routing protocol is a proactive routing protocol which is based on virtual circuit data delivery, no neighbor exposure and broken receiver anonymity. It offers sender, receiver, location and communication anonymity under a passive adversary model for large-scale theater-wide communications or small-scale tactical communications. It establishes sender receiver virtual circuits and uses dynamic pseudonyms for path presentations. It is resistant to message coding, flow recognition, replay and timing attacks, and offers high routing efficiency compared to classical AODV. The major weaknesses of this protocol are the final receiver is contained within every route request packet plaintext thereby breaking receiver anonymity.

Seys & Preneel (2006) proposed an anonymous routing for MANETs which is an on-demand routing protocol against cooperating nodes
inside the network and passive adversary that monitors all network traffic. It provides sender, receiver, and communication anonymity in both static and dynamic networks. The major problem with this work is, it assumes every node has a permanent identity known by other nodes; sender and receiver share a secret key and pseudonym. This is prone to various attacks.

Sy et al (2006) proposed an on-demand anonymous routing which uses bloom filters for storage processing and communication efficiencies. This protocol is based on asymmetric cryptosystems and provides sender, receiver, communications and location anonymity. A key management mechanism for distributing keys during source route construction provides strong end-to-end communication anonymity. But this protocol suffers from high overhead due to its key distribution technique.

Liu et al (2006) presented a Hierarchical anonymous on-demand routing protocol which is based on a hierarchical MANET architecture with multi-hop clustering. This protocol leverages the inherited group management security features to reduce the prohibitive computation and communication limitations of flat routing schemes. But the protocol is designed assuming a local, passive, and solitary adversary threat model instead of a much stronger global, active and multiple adversarial threat models.

Zhu et al (2006) proposed an anonymous routing protocol with local-repair mechanism is developed against active and passive attacks in mobile ad hoc networks. This protocol is designed to require neither asymmetric nor symmetric encryption/decryption while updating the flooding route requests; more importantly, once a route is broken, instead of re-launching a new costly flooding route discovery process like previous work, our protocol provides a local-repair mechanism to fix broken parts of a route without compromising anonymity.
Li & Ephremides (2006) proposed an anonymous routing in mobile ad hoc networks for providing anonymity by jointly considering the communication protocol and the security services. It depends on thus cutting across the traditional layer structure. Security services like authentication and key management are generally provided at the application layer. Two key components have formed. One is called trapdoor, a special token carried in the packet that only the designated receiver can open. Other users can neither open the trapdoor nor recognize who can open it. Such trapdoors can be implemented with cryptographic functions. The cost of constructing and opening the trapdoors depends on the type of cryptographic functions available at the application layer. The second key component is a routing protocol that sets up anonymous connections between source and destination.

Wu (2006) approached to applying pseudonymity for anonymous data delivery in location-aware mobile ad hoc networks. The node identities are kept anonymous. The positions of destinations are used for data-packet delivery. The anonymity for a destination relies on the difficulty of matching its position to its identity by any observer. Position servers that provide node position information act as trusted third parties and handle identity management. Node mobility makes the use of the pseudonym momentary, and therefore can further improve privacy. The anonymity for the source and intermediate nodes in the path is also achieved because they are not required to reveal any identity information. A receiver-contention mechanism is proposed so that a next hop can be generated without local position information exchange, which otherwise may lead to severe privacy degradation.

Huang (2006) introduced on measuring anonymity for wireless mobile ad-hoc networks. This approach is different from the traditional Shannon information theory based solutions where the measure is based on
hypotheses, i.e., predetermined probability assignments. Whereas this approach measures the anonymity from the views of the adversaries rather than the system designers; thus, our anonymity measure is scalable to the ability of adversaries.

Qian & Song (2006) proposed a secure anonymous routing for clustered multi-hop wireless ad hoc networks. This routing category belongs to intra-cluster routing and uses the common broadcast channel in wireless networks to provide anonymity, while inter-cluster routing uses a sequence of temporary public keys as the trapdoor information. Symmetric cipher is employed in most part of the proposed scheme to reduce computational complexity and maximize network efficiency. Public key is only used to distribute symmetric keys. Both privacy analysis including sender anonymity, receiver anonymity and sender-receiver anonymity and attack analysis show the effectiveness of the proposed scheme against a wide range of strong adversarial attacks.

Chou et al (2007) proposed an efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc networks. This protocol employs broadcasts with probabilistic-based flooding control to establish multiple anonymous paths between communication peers. It requires no hop-by-hop encryption/decryption along anonymous paths and, hence, demands lower computational complexity and power consumption than those MANET anonymous routing protocols. It builds multiple paths to multiple peers within a single query phase without using an extra route discovery process.

Boukerche & Ren (2007) proposed an efficient secure ad hoc routing protocol is designed to protect the anonymity and privacy information of the communicating nodes. In addition, it protects the security of the route
discovery and prevents some malicious behaviors during the two way conversation. In this protocol a source node does not need to collect and maintain the topological information of the network. Additionally, the mobile agent technique and the multicast mechanism used in our protocol protect the privacy of the sender and receiver of a message, while also providing protection for the message content as it traverses a network. They guarantee the anonymity of the sender node, receiver node, and their relationships.

Shokri et al (2007) proposed a chain-based anonymous routing for wireless ad hoc networks. This mechanism uses unicast-based broadcast data transfer to fulfill anonymous communication in wireless ad hoc networks. Through hiding identifiers of nodes inside the chain, CAR realizes sender, receiver, and relationship anonymity in addition to untraceability in the network. It also resistant to a wide range of passive attacks while adapting to implement other security mechanisms in the presence of active attacks. But this protocol suffers from high computational overhead.

Kao & Marculescu (2007) proposed a real-time anonymous routing for mobile ad hoc networks which is based on a symmetric cryptosystem. This protocol preserves the identity privacy, location privacy and route anonymity with only a negligible overhead in terms of processing requirements and packet size. Furthermore, this protocol does not rely on any trusted agent or centralized mechanism. Compared with other anonymous routing protocols, the protocol reduces the end-to-end delay by orders of magnitude, while performing comparably well in terms of packet delivery ratio. These features enable anonymity for applications with strict QoS requirements over mobile ad hoc networks.

Takahashi (2008) proposed an on-demand anonymous routing with distance vector protecting traffic privacy in wireless multi-hop networks. This
approach uses two anonymous routing algorithms such as randomized routing algorithm and probabilistic penalty-based routing algorithm. Both algorithms aim to differentiate routing paths to the same destination enhancing anonymity of the network traffic.

Zhu et al (2008) proposed anonymous misbehavior detection against DoS attacks in mobile ad hoc networks. This protocol provides anonymity for the witness who reports observed misbehavior. Together with a distributed trust mechanism, our protocol can identify malicious or selfish users in an anonymous manner. On the other hand, the misuse of witness anonymity is prevented in such a way that any malicious user who broadcasts multiple claims against the same user for the same reason can be identified.

Paik et al (2008) proposed anonymous and authentication routing protocol for mobile ad hoc network. This protocol focuses the anonymity properties such as entity anonymity, route anonymity and location anonymity. In addition, authentication is also provided by group signature for both nodes and packets during route discovery phase.

Shao & Huang (2008) proposed a trust enhanced anonymous routing in mobile ad-hoc networks. In this protocol the communicating parties are capable of choosing a secure end-to-end route free of any untrustworthy node during the anonymous route discovery process. The key features of our scheme are including of accomplishment of anonymity-related goals, trust-aware anonymous routing, effective pseudonym management and lightweight overhead in computation, communication and storage.

Nezhad et al (2008) proposed a V-routing which is based on proactive routing protocols. This routing protocol proposed for ad hoc networks of the type Mesh and MANET that conceals the locations and the identities of the communicating parties as well as the fact that they are
communicating. This protocol is especially for hiding the destination information. The protocol is designed based on a novel routing paradigm that puts the destination in charge of how packets should be sent to it.

Li et al (2009) proposed an efficient anonymous routing protocol for MANETs. This protocol introduces a localized trust management which can primarily remove malicious nodes and encrypts entire message with trust key and says hello to its ancestor within expiration time. It makes malicious node can be detected and isolated from the network. In this way, a anonymous and secure route path can be established in a hostile environment. Meanwhile, it is able to efficiently against the DoS attack.

Choi et al (2009) proposed an anonymous and secure reporting of traffic forwarding activity in mobile ad hoc networks. This mechanism developed for a civilian ad hoc network, in which the source and destination collect reports from intermediate nodes on the routing path. Every data packet initiates a report from one intermediate node that is randomly chosen by a source node. Through a symmetric cryptographic construction, it has been ensured that the node selection is not disclosed to other intermediate nodes. Furthermore, an efficient report wrapping scheme is proposed to prevent eavesdropping nodes from learning the reporting node selection by analyzing the report field going in and out of a node.

Song & Korba (2009) proposed a robust anonymous ad hoc on-demand routing to provide better services for strict military environments. This protocol is based on the anonymous neighborhood trust model, trapdoor, and onion routing technologies. The anonymous neighborhood trust model is based on the public key infrastructure and a master key mechanism, and can be easily implemented on military ad hoc networks. The trust model provides an anonymous trust environment for the ad hoc network through
authenticating nodes with their master key and pseudonym certificates without disclosing their real identity and the organization's information to outside observers. The trapdoor uses symmetric key cryptography and secret sharing to protect the source and destination nodes from identifying the shared communications. Onion routing combines symmetric and public key cryptography to provide secure and anonymous protection for the routing packets and communication data between source and destination nodes.

Pan & Li (2009) proposed an effective strong anonymous and secure shared key negotiation protocol in MANETs. This protocol is designed identity-based encryption to negotiate the shared key. It constructs the trapdoor using bilinear map to hide the destination identity and the source node can randomly generate and update the pseudo public key and private key to hide itself true identity.

Wan et al (2009) proposed a technique for anonymous user communication to protect privacy in wireless metropolitan mesh networks. This technique adapts two schemes; the first scheme relies on group signatures, together with user credentials, to deliver security and privacy protection. In the second scheme, the user is kept anonymous to mesh routers. This paper analyzes these two schemes in terms of security, privacy, and performance.

Dang et al (2010) proposed a distributed anonymous secure routing with good scalability for mobile ad hoc networks. This protocol addresses the problems of anonymous routing and later anonymous data transmission via a dynamic identity pseudonymity approach based on incomparable public keys. In this work, good scalability is achieved by using Diffie-Hellman key exchange scheme and symmetric key cryptography, instead of public key cryptography. In comparison with other previous anonymous secure routing
protocols, this protocol provides better security and anonymity protection, but also provides better scalability.

Siguang & Meng (2011) proposed an anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. This protocol provides identity anonymity, location anonymity, data and traffic anonymity based on cryptography technology and secret sharing in MANET communication. In addition, this work also considers hash function to detect active attacks in our data transmission process. This protocol effectively thwarts the various passive attacks and reduces the successful probability of active attacks such as intercept and physical destroy attacks.

Sun et al (2011) proposed security architecture to achieve anonymity and traceability in wireless mesh networks. This architecture strives to resolve the conflicts between the anonymity and traceability objectives, in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non repudiation. The major contributions in this paper is to design of a ticket-based anonymity system with traceability property and bind of the ticket, pseudonym which guarantees anonymous access control and simplified revocation process and adoption of the hierarchical identity-based cryptography for inter-domain authentication avoiding domain parameter certification.

Singh & Leavline (2011) proposed an anonymity threat avoidance routing protocol architecture against the anonymity threat such as traceability, intrusion, observability and linkability. This architecture has been designed with the principle of reactive routing protocol. It provides strong security with anonymity protection and scalability.

Defrawy & Tsudik (2011) proposed an anonymous location-aided routing in MANETs. This protocol uses nodes' current locations to securely
disseminate and construct topology snapshots and forward data. This protocol provides security and privacy with the aid of advanced group signature techniques. In addition this protocol provides node authentication, data integrity, anonymity, and untraceability. It also offers protection against passive and active insider and outsider attacks.

Jiang & Xing (2012) proposed an Anonymous on-demand routing and secure checking of traffic forwarding for mobile ad hoc networks a comprehensive anonymous communication protocol. This protocol consists of anonymous routing, which is based on identity-based encryption pseudonym and single-round onion, and secure checking of traffic forwarding in data transmission phase, to achieve strong route anonymity and improve reliability of packet delivery in the data transmission phase.

Shen et al (2013) proposed an anonymous location-based efficient routing protocol in MANETs. This protocol is proposed to offer high anonymity protection at a low cost. This protocol dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a untraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, this protocol offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks.

2.4 MANET-INTERNET INTEGRATION APPROACHES

A number of routing schemes have been proposed in the past to integrate MANET and Internet and to route the packets from each of the networks. In addition, there are various security mechanisms have been introduced to countermeasure the various attacks and to improve the
performance of routing protocols in integrated MANETs. These protocols are discussed in this section.

Jonsson et al (2000) proposed a Mobile IP for mobile ad hoc networks for integrating ad hoc networks to the internet based on Mobile IP. This mechanism provides mobile nodes in ad hoc networks with access to the Internet and the mobility service of Mobile IP. The FA is used as an access point to the internet. The AODV routing protocol is used to route packets between the FA and the ad hoc nodes. When a new node wants to access the Internet, it registers with the FA using its home address. The mobile nodes in the ad hoc network tunnel the packets to the FA in order to send them to the Internet. The FA simply sends any packet coming from the Internet to the mobile node in the ad hoc network. Routing the packet inside the ad hoc network is based on the ad hoc routing protocol used, which in this case is AODV. This mechanism uses the route discovery mechanism of the AODV routing protocol to search for the destination. If the route to destination is not found within the ad hoc network, the mobile node establishes a tunnel to the FA according to the FA default route the mobile node registers with it.

Belding-Royer & Perkins (2001) proposed an internet draft for global connectivity between MANET and IPv4. This method enables MANET to obtain Internet connectivity. This draft is integrates the Mobile IPv4 and AODV, such that a mobile node outside the FA transmission range can get a COA and connect with the internet through other hops in the MANET. The mobile node can roam to another MANET subnet without disconnection using Mobile IP.

Benzaid (2002) proposed a global connectivity for IPv6 mobile ad hoc networks. This method describes a method to enable MANET nodes to communicate with the fixed internet. The connection between the MANET
nodes and the internet is through nodes called internet-gateways, which are connected to the Internet using a wired interface and connected to MANET using a wireless interface. The author has proposed two methods to enable MANET nodes to find the Internet gateway and obtain the global prefix information, so that the MANET node can generate a global IPv6 address, which is used for sending/receiving packets from/to the Internet.

Ergen & Puri (2002) proposed a Mobile IP enriched wireless local area network architecture. In this work two protocols have been used to extend Mobile IP capabilities to ad hoc networks. Three types of domains such as the Internet domain, the FA domain, and the ad hoc are considered. This protocol uses the destination sequenced distance vector routing protocol to route packets between the FA and mobile ad hoc nodes. It is used to route packets between ad hoc mobile nodes and the FA. In this protocol, the routing table in every node has two types of entries. The first type is established when the mobile node receives a periodic beacon from the FA, which refers to the default route to the FA (uplink port). The second type is established when the mobile node receives registration request message from low-level mobile node.

Ratanchandani & Kravets (2003) proposed a hybrid approach to internet connectivity for mobile ad hoc networks. The authors propose a hybrid scheme to enable the MANET nodes to obtain Internet connectivity using Mobile IP. The FA periodically broadcasts agent advertisement messages. The agent advertisement messages are flooded in the MANET in an n-hop neighbor. Any node, nhops far from the FA, can receive up-to-date information about the FA. Mobile nodes more than nhops away from the FA and wanting Internet connectivity broadcast a solicitation message to discover the FA. The intermediate node, which receives a fresh agent advertisement
message and has a correct route to the FA, can reply to the mobile node with a unicast advertisement.

Tseng et al (2003) proposed an integration of a MANET with the Internet. In this integration one-hop wireless networks are extended to multiple MANETs. Every MANET is served by an FA and it represents a subnet of the internet. The proposed architecture consists of multiple MANETs connected to the Internet using different access points called gateways.

Xie & Kumar (2004) proposed an integrated connectivity framework for internet and ad hoc networks. This protocol is an enhancement for the destination sequenced distance vector protocol to solve the link break problem due to high mobility, which decreases the performance of the standard protocol. It proposes bidirectional connectivity for ad hoc networks and the internet based on efficient destination sequenced distance vector. Three simple communication scenarios are presented for integration of MANET and Internet such as reactive integration routing solutions, micro-mobility within wireless Ad hoc Networks and towards hybrid wireless multi-hop networks hybrid integration routing solutions.

Kock & Schmidt (2004) proposed dynamic mobile IP routers in ad hoc networks to integrate between cellular system and an ad hoc network is presented using Mobile IP. The basic idea in the integration is using mobile routers as a gateway between the HA and ad hoc mobile nodes. It is assumed that gateways in the ad hoc network are multi-interfaced. One interface is connected to the cellular system and the other connected to the ad hoc network using the ad hoc routing protocol. The mobile router sets up tunnels to every mobile node for which it is serving as gateway, and another tunnel to the HA using second interface.
Benzaid et al (2004) proposed an integration of Mobile-IP and optimized link state routing protocol for universal mobility. The author proposes a hierarchical mobility management architecture which is used to interconnect MANET nodes to the internet. The access network of the proposed integrated network architecture is called optimized link state routing IP access network.

Shin et al (2004) proposed a protocol for MANET-Internet integration access. Periodic gateway discovery mechanism is used based on periodic HELLO message. HELLO scheme is extended as e-HELLO to contain the reachable gateway sets information over the ad hoc networks to inform its neighbor node when HELLO message is broadcasted and updates route entries for the gateways. NAT-based table for source node and proxy RREP (P-RREP) scheme is used to maintain the connectivity with the gateway. Mobile node can change its current gateway only when current session is over when node moves away the range of the default gateway.

Ammari & El-Rewini (2005) proposed a mobile gateway based on three-layer approach using both Mobile IP protocol and destination sequenced distance vector routing protocol. The first layer contains Mobile IP foreign agents; the second layer includes mobile gateways and mobile Internet nodes, which are one-hop away from Mobile IP foreign agents; the third layer has all MANET nodes and visiting mobile Internet nodes that are at least one-hop away from mobile gateways. The second layer is to provide Internet connectivity to MANET nodes and, thus to help establish interaction between MANET nodes and the Internet. Mobile gateways are powerful MANET nodes and are designed in a way to use both Mobile IP protocol when they communicate with the Internet. The destination sequenced distance vector routing protocol is used for routing within the MANET. The integration framework considers using some border MANET nodes to connect the rest of
MANET nodes to the Internet. These MANET nodes are referred as mobile gateways. A mobile gateway selects a closest and/or a least loaded foreign agent based on the distance and the load criteria. MANET nodes select a closest and/or least loaded mobile gateway.

Hamidian et al (2005) extended the AODV routing protocol to the Internet to achieve the interconnection between the MANET and the Internet. The paper discusses and evaluates three approaches for gateway discovery. The authors implement these three schemes in network simulator 2 (ns-2) and compare them by means of simulation study. They also discuss the advantages and disadvantages of the three approaches. The gateway discovery method follows a similar approach based on. However, those approaches have a fixed TTL for proactive gateway advertisements and do not reflect dynamic network conditions.

Rakeshkumar & Misra (2006) proposed an efficient mechanism for connecting MANET and internet through complete adaptive gateway discovery. The authors implemented “Complete Adaptive” scheme to discover internet gateway in an efficient manner for AODV and compared it with an existing approach. This approach sends periodic advertisement at long interval and adaptive advertisement performed whenever it detects mobility in the network. To decide the time-to-live of next message this approach use the maximal benefit coverage algorithm. We propose a heuristic algorithm to decide whether to perform an adaptive advertisement or not. Our “Complete Adaptive” approach results in an efficient solution especially it reduced overhead compare to an existing approach.

Abduljalil & Bodhe (2006) proposed an integrated routing protocol for integration of cellular IP and mobile ad hoc networks. This work mainly focuses to integrate MANETs to Cellular IP access network and Internet
proposed. The authors implemented this work to support mobile nodes mobility between different overlap and none-overlap MANETs with multiple access points.

Trevino-Cabrera et al (2006) proposed a mechanism that integrates the mobile ad hoc networks into the internet without dedicated gateways. The authors introduced this mechanism and deployed at the edge of the internet, to get connectivity with the IPv6 hosts located on the internet. The mechanism proposes the use of mobile multiple gateways for this purpose and allows any ad hoc node, either directly connected to the internet or via one or more intermediate nodes, to configure its interfaces with globally routable unique IPv6 addresses and exchange packets with host on the Internet. This is achieved by configuring and properly managing, which indeed is an important issue for such networks, one or more ad hoc nodes as mobile internet gateways.

Mo et al (2006) proposed a MANET node based mobile gateway with variety of MANET nodes can possess internet connectivity. The problem of load-balance for multi-gateway can be alleviated through the select strategy, and the performance of networks can be improved. And also routing and gateway information can be directly obtained with the gateway registration, discovery, advertisement and invalidation algorithm, which makes Manet routing not rely on any specific Manet routing protocol. Any packet will be forwarded to gateway and gateway forwards the packet to the Internet or other nodes in the MANET.

Wakikawa et al (2006), proposed an approach to global Internet connection over the IPv6 MANET environment, where mobile nodes in the ad hoc network are configured with new globally routable IP addresses based on the neighbor discovery protocol of IPv6 or route searching procedure of on-
demand routing protocol. This paper defines two different mechanisms to discover Internet gateways: periodic flooding of gateway advertisement messages from the gateways and reactive flooding a gateway solicitation message from nodes. The periodic flooding using gateway advertisement is completely proactive, whereas the reactive flooding using gateway solicitation is completely reactive. Gateway advertisement and gateway solicitation messages can be implemented by simply adding an ‘T’ flag to existing route request and route reply messages. However, this proposal does not give any metric to select a gateway.

Kumar et al (2007) proposed an efficient gateway discovery in ad hoc networks for internet connectivity. The focus of this paper is on devising an efficient proactive gateway discovery algorithm that takes into account the size of interface queue in addition to the traditional minimum hop metric to select an efficient gateway. In the MANET domain, AODV routing protocol has been used. This approach also allows an efficient handoff from one gateway to another gateway and still maintains a seamless connectivity to a fixed host. In this work, impacts of this new metric on the gateway discovery performance are investigated.

Domingo& Prior (2007) proposed hybrid gateway discovery scheme with modified AODV routing protocol for routing in ad hoc domain. Scheme differentiates between the best-effort and real-time services. QoS are also discussed for real time services. Threshold is discussed for end-to-end delay to improve the QoS for real time services. QoS model is proposed to improve the real time flows. QoS parameter is defined to assume packet lost is end-to-end delay cross the threshold. Ratio between the number of real time sources having latency problem and total number of real time sources using gateways and a threshold parameter is also discussed. Destination keeps track of the lost messages and inform to real time source traffic. Also suggest that
to reduce the end-to-end delay of the lost message the message will be forwarded as broadcast packet.

Trujillo et al (2008) proposed a stability approach to improve MANET-internet connection. The authors consist of presenting and testing an algorithm to automatically adapt certain parameter to the network conditions so that the network performance can be improved, regardless of its mobility pattern. This scheme dynamically adjusts the frequency of messages and improves the conventional proactive schemes. In addition this scheme makes use of the mobility and connectivity properties of the network to tune the control system that sends the messages.

Rahman Khan et al (2008) proposed an integrating Mobile ad hoc networks and the internet: challenges and a review of strategies. The author reviews the characteristics of ten proposed solutions with their relative merits and de-merits in the light of a few specific parameters. It concludes with a discussion on the suitability of the solutions under different scenarios.

Hoon (2009) proposed a tree-based approach for the internet connectivity of mobile ad hoc networks to efficiently extend the scope of mobile internet protocol. In this approach the mobile nodes form a number of small trees named, each of them growing from anchor node which can communicate directly with an internet gateway. A new node registers with foreign agent and home agent along the tree path without resorting to an inefficient flooding. In addition this approach sets up a routing path efficiently by exploiting the tree information without relying on flooding.

Zhuang (2009) proposed a hybrid internet gateway discovery scheme in mobile ad hoc networks to remove unidirectional links and enhance internet connectivity simultaneously. In this work the author modifies AODV routing protocol to set up multi-hop paths to the internet gateways in the
MANET. The simulation results shows that this approach can provide better performance to avoid unidirectional links and can achieve good connectivity while keeping overhead costs low.

Li & Li (2009) proposed a MANET accessing internet routing algorithm based on dynamic gateway adaptive selection. This mechanism considers candidate gateways’ connecting degree, load degree, residual energy, and movement rate synthetically and uses the idea of group decision-making method for reference. The algorithm employs the methods of multi-paths and query localization technique based on old path information to maintain routing adaptively.

Iqbal & Kabir (2011) proposed an internet gateway discovery and selection scheme in mobile ad hoc network. In this work, the gateways advertise gateway advertisement messages only on-demand. In addition, it contains the advertisements within a limit in order to make our scheme scalable. The author considered the interface queue length and the total number of neighbors along a route in addition to the hop count to bypass the loaded and dense route to the gateways in order to reduce the delay and packet loss.

Saluja & Srivatsava (2012) proposed a scenario approach for route discovery using MANET routing protocol. In this work, the gateways act as bridges between the two different protocols architectures such as MANET and Internet. The AODV reactive routing protocol is extended to support the communication between the MANET and the Internet. This work carried out a systematic simulation based performance evaluation of the different gateway discovery approaches under different network scenarios. The performance differentials are analyzed on the basis of three metrics - packet delivery fraction, average end-to-end delay and normalized routing load.
Yan et al (2013) proposed a QoS-based gateway selection in MANET with internet connectivity based on three QoS metrics such as traffic load of gateway, path quality from MANET node to the gateway and hop count to the gateway for integrating MANET and the Internet. This method adapts simple additive weighting method, which used to combine these three QoS metrics to outrank the optimum gateway. Gateway with the smallest weight has been selected as a gateway. The simulation results show that the proposed scheme can improve packet delivery ratio and end to end delay.

2.5 SUMMARY

In this chapter the plethora of routing protocols that have been proposed in the past for MANET and integrated MANET-Internet networks. These protocols are compromised in many ways and prone to different kinds of insider and outsider attacks. These protocols considers either security issues or privacy issues, in other words none of the protocols provides privacy and security completely for both the environment. There is a need of privacy and security related techniques to safeguard the MANET and MANET-Internet networks.