CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

Mobile ad hoc networks (MANETs) are vulnerable to attacks because of their dynamic topologies and bandwidth limitations. Establishing security measures and finding secure routes are the major challenges faced by MANET. Some of the security issues faced by ad hoc networks are node authentication, insider attacks and intrusion detection. Routing protocols attempt to mitigate attacks by isolating malicious nodes. A bird’s eye view of various security threats on each layer of MANET is presented in Chapter 1, Table 1.3. This chapter discusses various security threats against MANETs. It also gives a comprehensive description of various implementations of Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) routing protocols for intrusion detection and threat mitigation.

2.2 INTRUSION DETECTION SYSTEMS

Various IDS techniques available in the literature are briefly discussed in subsections 2.2.1 to 2.2.4

2.2.1 Decentralized IDS

A decentralized IDS based on network behavior is presented in (Da Silva et al 2005). The proposed method in (Da Silva et al 2005) tries to resolve the following attacks: message delay, repetition, wormhole, jamming,
black hole and selective forwarding. It also focuses on the following events: 
(i) data message listened by the monitor that is not addressed to it and 
(ii) message collision when the monitor tries to send a message. The 
proposed algorithm in (Da Silva et al 2005) is divided into three phases 
namely, (i) Data acquisition phase (ii) Rule application phase and (iii) 
Intrusion detection phase. In data acquisition phase, messages are collected in 
a promiscuous mode and important information is filtered before being 
stored for subsequent analysis. In the rule application phase, which is also 
called as processing phase, rules are applied on stored data. In intrusion 
detection phase, which is the analysis phase, intrusion detection is raised if 
the actual number of failures is more than the expected failures. The monitor 
nodes are distributed uniformly throughout the network for quick and 
effective detection of intrusion.

A Mobile Intrusion Detection System (MIDS) has been proposed in 
(Madhavi & Kim 2008) to detect misbehaving nodes, anomalies in packet 
forwarding, packet dropping and delaying. MIDS relies on overhearing packet 
transmissions among neighbor nodes. The intrusion detection algorithm 
proposed by (Madhavi & Kim 2008) designs simple rules to identify 
misbehaving nodes by a specially designated node called a monitor node. The 
work done in (Madhavi & Kim 2008) proposes that intrusion detection must 
be included in the security architecture for mobile computing environment.

Dhillon et al (2004) have integrated a distributed certificate 
authority mechanism in Optimal Link State Routing (OLSR) protocol. The 
proposed approach in (Dhillon et al 2004) couples the operations at the 
network layer level and thereby reduces the control traffic overload. The 
certificate authority is a RSA key pair which consists of a public key and a 
private key. The private key is distributed using Shamir’s secret sharing 
method by embedding it in the root of a polynomial. The proposed method
enables autonomous security by itself without any external administration. It
minimizes the signaling overhead by supporting security at the network layer
level. Future extension of this work includes benchmarking the performance
using a heavily loaded and large MANET, securing the MANETs against
wormhole attacks and generalizing the method to accommodate additional
MANET routing protocols.

2.2.2 Specification based Monitoring IDS

A monitoring system based on AODV is designed to detect attacks
on MANET is proposed in (Tseng et al 2003). The specification based
monitoring system captures the correct behavior by comparing the behavior of
objects with their associated security specifications. Thus, intrusions due to
incorrect behavior are detected without exact knowledge about them. The
proposed approach in (Tseng et al 2003) uses finite state machine for
describing a valid flow of AODV routing behavior. It is based on tree
structure and a node coloring scheme. Violations in the specifications are
detected by distributed network monitors. In this approach, a field is added in
the protocol message to enable monitoring. The IDS is built on the monitoring
system to trace the AODV request-reply flow.

Marti et al (2000) have proposed a watchdog mechanism
implemented using DSR by categorizing nodes in the network based on their
dynamic behavior. The proposed method complements DSR by having
watchdog and path-rater incorporated in it. The watchdog is used for detection
of malicious behavior. It runs on each node listening to all transmissions of
neighboring nodes. On the other hand, path-rater is used for trust management
and routing policy. Each possible path is rated by path-rater. A buffer is
maintained by the watchdog which contains details of recently sent packets.
When a packet is forwarded to the next hop, it's details are removed from the
buffer. If a packet remains in the buffer for a long time, watchdog isolates the
corresponding node as misbehaving node. The misbehaving nodes identified by the watchdog are avoided for packet transmission. On simulation, the proposed method (Marti et al 2000) performed efficiently, increasing the throughput by 17% in the presence of 40% misbehaving nodes. Further investigation needs to be carried out on conducting tests using watchdog and path-rater to determine optimal values to increase throughput in different situations. In addition to throughput, evaluation of watchdog and path-rater need to be done with respect to latency.

### 2.2.3 Multistage IDS

A multi stage classification system for network intrusion detection is presented in (Cordella et al 2004). The proposed method in (Cordella et al 2004) is made up of several stages. Each stage, considers different set of features to distinguish between normal and malicious traffic. As each stage considers only a reduced set of features, overall performance of the system is improved. The proposed system in (Cordella et al 2004) has low false alarm rate. Experiments are carried out using DARPA dataset and results achieved claim that the performance of the proposed system is significantly better when compared to other methods with low false alarm rate.

Intrusion detection is frequently used as a second line of defense in Mobile Ad-hoc Networks (MANETs). Mitrokotsa, A. & Dimitrakakis, C. (2013) have analysed the effective use of classification methods in intrusion detection for MANETs. Five supervised classification algorithms are evaluated based on various metrics in (Mitrokotsa & Dimitrakakis 2013). Their performance is measured for a dataset which includes varied traffic conditions and mobility patterns for multiple attacks. The work done in (Mitrokotsa & Dimitrakakis 2013) investigates the impact of using uniform and weighted cost matrices on the classifier's performance. It also examines the techniques for tuning classifiers when unknown attack subtypes are
expected during testing. A sequential cross-validation procedure is also developed in (Mitrokotsa & Dimitrakakis 2013) to make the classifiers more robust. The results achieved indicate that weighted cost matrices can be used effectively with statistical classifiers. It is observed that sequential cross validation can have a small, but significant effect for certain types of classifiers.

Figure 2.1 Various Attacks in AODV based MANETs

Table: Various Attacks in Mobile Ad Hoc Networks

<table>
<thead>
<tr>
<th>Category</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and non-repudiation attacks</td>
<td>IP spoofing, MAC spoofing, TCP spoofing</td>
</tr>
<tr>
<td>Availability attacks</td>
<td>Packet drop / gray hole attack, Tunneling / wormhole attack, Fabrication attack, Resource depletion attack, Selective existence attacks</td>
</tr>
<tr>
<td>Integrity attacks</td>
<td>False message propagation attacks, Modified sequence numbers, Modified hop counts, Detour</td>
</tr>
<tr>
<td>Confidentiality and privacy attacks</td>
<td>Sniffing, Location disclosure attacks, Content disclosure attacks</td>
</tr>
</tbody>
</table>

2.2.4 Real time IDS

A real time, AODV based IDS, Ad hoc On-demand Distance Vector State Transition Analysis Technique (AODVSTAT) is designed in Vigna et al (2004). Figure 2.1 summarizes various attacks on AODV based networks (Vigna et al 2004). Sensors based on AODVSTAT are deployed either on standalone or distributed basis on a subset of nodes in the network. The sensors perform real-time analysis on the packet stream to detect signs of
intrusions. Experimental results show that the proposed method successfully detects attacks against AODV routing protocol with less false positives and overhead (Vigna et al 2004). A novel knowledge-based intrusion detection technique, Real-time Intrusion Detection for Ad hoc Networks (RIDAN), is designed in (Stamouli et al 2005) to detect real-time attacks against the routing fabric of a MANET. The proposed system is designed to take countermeasures such as minimizing the effectiveness of an attack and thereby maintaining the performance of the network within acceptable limits. RIDAN does not have additional overhead and operates as an intermediate component between the network traffic and the protocol. RIDAN architecture utilizes Timed Finite State Machines (TFSMs) to define attacks against the AODV routing process. A prototype is developed to evaluate networks based on AODV using the network simulator (NS-2). RIDAN detects 81.2% of sequence number attacks and has 71.5% of packet drop rate and 74.8% resource consumption.

It is observed that the watchdog mechanism proposed in (Marti et al 2000) not only mitigate attacks but also improve the throughput of the network with a high number of misbehaving nodes. Though the work done in (Tseng et al 2003) is better in identifying various attacks, it does not provide a mechanism to mitigate the attacks.

2.3 SECURED ROUTING TECHNIQUES

Various mechanisms have been proposed in the literature for enhancing the security in MANET, which is based on authentication and encryption. Some of them are discussed in subsections 2.3.1 to 2.3.7.
2.3.1 **Authentication based Routing**

Paul & Westhoff (2002) have proposed a context aware inference scheme to identify malicious nodes in the network. It uses distributed certification authority by adding digital signatures of accused nodes in RREQ in order to reveal malicious nodes. Sanzgiri et al (2005) have proposed a public-key cryptographic mechanism called Authenticated Routing for Ad hoc Network (ARAN) which is used to offset or mitigate prospective attacks. Simulation results by employing ARAN indicate that in spite of increase in overall load, the proposed protocol provides improved security compared to DSR and AODV. Packet delivery fraction obtained using ARAN is 95% or higher in all scenarios and almost identical to that obtained using AODV. This suggests that ARAN is highly effective in discovering and maintaining routes for delivery of data packets, even with relatively high node mobility. Sen (2010) has proposed an integrated security solution for detecting the misbehaving nodes using key distribution.

Hu et al (2005) have presented a DSR based protocol called ‘Ariadne’ to provide secured routing. Several authentication mechanisms such as digital signatures, pair-wise secret keys and TESLA (Hu et al 2005) could be used with the proposed protocol. Hash chains are used to authenticate every route request protecting the network from overload and thereby preventing denial of service attacks. Attacks such as compromised nodes tampering the uncompromised nodes are also mitigated by employing Ariadne. It combines TESLA authenticators and hashing technique to protect the discovered routes.

Raffo et al (2004) have investigated security issues related to Optimized Link State Routing (OLSR) protocol for MANETs. Possible attacks against the integrity of OLSR network routing infrastructure is
investigated and a secured routing technique is presented in (Raffo et al 2004). A mechanism for routing message authentication i.e. digital signatures has been deployed. The proposed solution focussed on compromised nodes which could inject false, but correctly signed routing messages. It checks the authenticity of information injected into the network. The solution is based on recording recent routing information (HELLO messages) and reusing this information to prove the link state of a node at a later time. This is obtained using Advanced Signature (ADVSIG) control message.

2.3.2 Location Aided Cluster based Routing

Improved Location aided Cluster based Routing Protocol (ILCRP) for MANETs with Global Positioning System (GPS) is proposed in (Mangai & Tamilarasi 2011). ILCRP makes use of location aided routing in the presence of cluster based routing protocol. The use of GPS prevents wormhole attack in ILCRP. Intrusion detection is done by all participating nodes and this collaborative intrusion detection leads to reduced energy consumption. Simulations are performed using NS2 and the results show that the ILCRP provides higher delivery ratio. Further investigation is to be done on key management and authentication which can result in better security.

2.3.3 Trust and Reputation Based Routing

Some of the trust and reputation based routing mechanisms for improving security in MANETs is discussed in this subsection. Buchegger & Boudec (2002) have proposed a scheme in which trust relationships and routing decisions are made based on routing and forwarding behavior of other nodes. The proposed scheme in (Buchegger & Boudec 2002) strengthens dynamic source routing against security threats while ensuring high throughput. Misbehaving nodes are detected and isolated. An ALARM
message is sent on detection of malicious nodes which are avoided during rerouting. Nodes learn not only from their own experience, but also by observing the neighbor nodes. Observable attacks on forwarding and routing can be thwarted by the suggested scheme of detection, alerting and reaction. Analysis has been done with respect to scalability, cost/benefit ratio and throughput. Further investigation is required for scenarios such as what happens to a node in a remote location, where friends might be located, use of rumor spreading and transitive trust etc.

A Trust Based Reliable AODV (TBRAODV) protocol is proposed in (Subramanian & Ramachandran 2012) to track, spot and isolate misbehaving nodes. Trust values are computed for each node based on which nodes are allowed to participate in routing. TBRAODV is implemented and simulated using (NS-2) and the simulation results show that TBRAODV provides consistent and reliable data transfer when compared to the conventional AODV.

An architecture for interdomain collaboration based on trust and reputation is proposed in (Perez et al 2011). The model Collaborative Intrusion Detection Networks (CIDN) proposed in (Perez et al 2011) improves the accuracy of detection when users move from one security domain to another. It uses a collaborative alert system where different domains participate. The proposed reputation model provides a better accuracy in computing the reputation of the mobile Host Intrusion Detection Systems (HIDS). This work can be extended further by calculating reputation of a mobile HIDS using security domain.

An extension of DSR, namely, the CONFIDANT protocol is proposed in (Buchegger & Boudec 2002). The watchdog listens into the transmission of neighboring nodes and observes the route protocol behavior. On detection of any intrusive activity, it sends an alarm message about
malicious nodes to other nodes on its friends list. On receiving the alarm message, other nodes update the reputation of malicious nodes if the source of alarm is a trusted node. Zapata (2002) has presented a secured routing technique which requires more power. A power aware secured routing is proposed in (Hu et al 2005) in which the end user can set the required level of security. Buchegger & Boudec (2002) have proposed a solution to overcome the additional processing overheads by introducing trust based systems. Trust based systems have lower overheads in terms of additional control packets and processor utilization.

A reputation-based protocol for Delay Tolerant Network (DTN) is proposed in (Dini & Lo Duca 2012). DTN relies on the implicit assumption that nodes cooperate towards message forwarding. But if malicious nodes such as black holes voluntarily attract and drop messages frequently, DTN cannot perform as expected. All nodes in the network maintain the reputation of the nearby nodes. Based on the reputation, it chooses highest reputation node for forwarding the packet. The Reputation protocol composed of three basic mechanisms: (i) acknowledgments, (ii) node lists and (iii) aging. Aging is the main factor which makes communication efficient and capable of adapting to the changing operating conditions of a DTN. The protocol has been extended to Context Aware Adaptive Routing (CAR) and results obtained using CAR has been compared with DTN routing protocol. Simulation results show that Reputation based CAR (RCAR) is effective and efficient for DTN and distinguishes black holes with less overhead. Moreover, RCAR is able to adapt dynamic topology of DTN and reduces false positive and false negatives using aging factor.

2.3.4 Cooperation based Routing

A trust model based on the non-cooperative game which uses a bacterial-like algorithm and allows the nodes to learn appropriate cooperation
behavior is proposed in (Mejia et al 2010). The proposed trust model in (Mejia et al 2010) exchanges genetic information between neighborhood nodes and thereby reduces the communication overhead. With local optimization, entire network is able to maximize cooperation and save energy by isolating selfish nodes.

Vilela & Barros (2006) have proposed a security solution that rewards nodes for their cooperation in exchanging the routing information. The proposed scheme correlates direct observation of transmissions with path information from successfully delivered packets mitigates security issues. The goal of (Vilela & Barros 2006) is to provide OLSR protocol with a security solution that defends the network against malicious nodes by rewarding proper routing behavior and thus assuring effective cooperation among communicating nodes. It combines two sources of traffic information i.e. (i) monitoring of neighbor nodes, whether they relay packets sent to them or not and (ii) the paths traversed by successfully delivered packets.

The trust as a security solution for OLSR protocol is focused in (Adnane et al 2013). Trust is present implicitly in protocols based on cooperation between the entities involved in routing operations. As the range of cooperating nodes in wireless environment is limited, the nodes mutually cooperate with their neighbors in order to extend remote nodes and the entire network. Explicit trust management allows entities to reason with and about trust and to take decisions regarding other entities. The technique in (Adnane et al 2013) contributes trust-based security in OLSR. Trust-based analysis of OLSR protocol is presented in (Adnane et al 2013) using trust specification language. Simulation shows that how trust based reasoning allows each node to evaluate the behavior of other nodes. The proposed approach can handle different attack scenarios and is compatible with the conventional OLSR.
Managing trust in a distributed Mobile Ad Hoc Network (MANET) is challenging when collaboration or cooperation is critical to achieve. In defining and managing trust in a military MANET, it seeks to combine the notion of social trust derived from social networks with Quality-of-Service (QoS) trust derived from information and communication networks (Cho et al 2011). Basic concepts and properties of trust are also discussed in (Cho et al 2011). The proposed method provides a survey of trust management schemes developed for MANETs. Trust metrics that captures aspects of communication and social network and corresponding trust measurement, distribution and management schemes are interesting research directions.

2.3.5  Secured AODV Routing

An overview of various approaches to secured routing protocols in MANET is presented in (Zapata 2002). An extension of AODV, Secure AODV, is also proposed in (Zapata & Asokan 2002). Digital signatures and hash chains are the two mechanisms used to secure the AODV messages. Digital signatures are used to authenticate the non-mutable fields of the messages. On the other hand, hash chains are used to secure hop count information. The route error messages generated or forwarded by a node are signed using digital signatures. Finally, the neighbor node verifies the signature before forwarding it to the intended destination (Panauousis et al 2009).

On-demand Tree-based Routing Protocol (OTRP) is proposed in (AlAamri et al 2013). It uses the concept of hop-by-hop routing with an efficient route discovery algorithm called Tree-based Optimized Flooding (TOF). Such protocol improves the scalability of ad hoc networks when there is no prior knowledge about the destination. Limited set of branching nodes are used to flood the network selectively in order to minimize route discovery overheads. Theoretical analysis and evaluation are done on OTRP based on
the following factors: (i) number of branch nodes, (ii) location of branching nodes and (iii) number of Route REQuest (RREQ) retries. The performance of OTRP is improved by increasing the number of branching nodes with a low number of RREQ retries. Simulation results show that OTRP achieves a higher level of data delivery and reduces routing overhead considerably. OTRP performs better than AODV with respect to Packet Delivery Ratio (PDR) for a network with 100 nodes, OTRP provides the packet delivery ratio of more than 80%, whereas, AODV is able to achieve only 50% PDR. Further investigation on the performance of OTRP needs to be carried out for heterogeneous network with high degree mobile nodes.

2.3.6 Distributed Trust Computation Mechanism

A highly scalable cluster-based hierarchical trust management protocol for Wireless Sensor Networks (WSNs) to identify and isolate malicious nodes is presented in (Bao et al 2012). The multidimensional trust attributes derived from communication and social networks are used to evaluate the overall trust of a sensor node. A heterogeneous WSN is described using a probability model. The WSN used in (Bao et al 2012) comprises a large number of sensor nodes with different social and quality of service (QoS) behaviors. This serves as a basis for validating the protocol design. The protocol validation is done by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of this hierarchical trust management protocol, trust-based geographic routing and trust-based intrusion detection has been applied on the system. For each application, the best trust composition and formation is identified to maximize application performance. Results indicate that trust-based geographic routing provides better delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, it has been discovered that there exists an
optimal trust threshold for minimizing false positives and false negatives. Trust-based intrusion detection performs well when compared to traditional anomaly-based intrusion detection, in both detection and false positive probability.

A class of trust management protocols for routing in Delay Tolerant Networks (DTNs) is proposed in (Chen et al 2010). The idea is to incorporate trust evaluation in the routing protocol. The main evaluation of trust is done by considering Quality-of-Service (QoS) trust properties such as connectivity and social trust properties such as honesty and unselfishness. There are two versions of trust management routing protocols: (i) Combination of equal-weight QoS and social trust management protocol called trust-based routing and (ii) QoS only trust management protocol called connectivity-based routing. The performance of these two routing protocols is analyzed in terms of message delivery ratio, latency and message overhead. A comparative performance analysis is also performed with epidemic routing for a DTN consisting of heterogeneous mobile nodes with different social and networking behaviors. The obtained results indicate that trust-based routing improves the delivery ratio. By properly selecting weights associated with QoS and social trust metrics, proposed trust management protocols can approximate to ideal performance by epidemic routing without incurring much overhead.

Trust and reputation models over distributed systems have been proposed in the last few years as an innovative solution for guaranteeing minimum level of security. Marmol & Perez (2009) have presented some of the most important and critical security threats that could be applied in a trust and reputation scheme. A thorough study has been made such as, how trust and reputation models solve the security problem in the network. The work
presented in (Marmol & Perez 2009) acts as a reference guide when designing secure trust and reputation models.

Different trust and reputation models have arisen in the last few years. All of them have certain key processes in common such as scoring, ranking, rewarding, punishing or gathering behavioral information. However, there is no standardization effort for these models. Such effort would be beneficial for distributed systems such as P2P, ad-hoc networks, multi-agent systems or Wireless Sensor Networks. Marmol & Perez (2010) have presented a pre-standardization approach for trust and/or reputation models in distributed systems. A global comparison has been done for the most relevant models in (Marmol & Perez 2010).

A subjective trust management MANET model called Analytic Fuzzy System (AFS) trust is built in (Xia et al 2011). AFS trust is contained with multiple decision factors based on Analytic Hierarchy Process (AHP) theory and fuzzy logic rules prediction method. These methods are used to reduce malicious node hazards. Various other multiple decision factors considered are direct trust, recommendation trust, incentive function and active degree. Weights are calculated for the above mentioned decision factors using AHP based weight mechanism. Prediction of nodes trust value is done using fuzzy logic rules prediction method. Weighted decision factors and node’s trust value made the proposed model more stable, adaptive and robust. Future work include the following directions: (i) Incorporation of other decision factors into the model. (ii) An adaptive trust level classification of nodes. (iii) Trust-based on-demand multipath routing.

An important and critical part of security is trust establishment and maintenance. A variety of schemes for distributed trust computation, strong connections with various components of random graph theory is established in (Baras & Jiang 2004). A description of distributed trust in MANET
framework consists of two major components, namely, (i) Trust document distribution and (ii) Distributed trust computation. The proposed work in (Baras & Jiang 2004) computes the trust values based on local interactions using random graph theory and cooperative game theory models. Phase transition phenomena appear in the trust computation and the effect of topology on the proposed scheme is described.

A key revocation mechanism to optimize the requirement of fast revocation propagation, complete coverage and low message complexity is proposed in (Reidt & Wolthusen 2007). Determining the efficiency of protocols in MANET environment depends on accurate characterization of the operating environment, particularly the message complexity. An extensible group mobility model is used to capture platoon-level light infantry operations. An algorithm is introduced for key revocation based on Trust Authority (TA) neighbors and real physical neighbors yielding a flooding algorithm. Different choices of the cluster message frequency of 2, 4 and 8 seconds yielded almost the same results in constantly arranged network. In simulation setup, the trust authority reaches a constant state after 30 seconds, i.e. after 5 rounds of cluster message exchanges.

A scheme proposed in (Inoue et al 2010) makes use of Attribute Certificates (ACs) for the evaluation of trust level for communication paths in MANET. Since a Mobile Ad hoc Network (MANET) is a distributed and self-organized network, there could be malicious nodes that intentionally falsify or drop packets. Many trust-based secure routing protocols have been proposed for evading malicious nodes in communication paths (Inoue et al 2010). Most of the time, the calculated trusts are not used and therefore expires. ACs can detect if the trust has been falsified. Moreover, the proposed scheme not only increases security level, but also reduces the number of trust expiries. Simulation results show that the proposed scheme in (Inoue et al 2010) provides improved packet delivery rate using trust.
Message security is of paramount importance in MANET applications such as crisis management, military and healthcare. However, because of the absence of a fixed infrastructure with designated centralized access points, implementation of hard-cryptographic security is a challenging prospect. A novel method for message security using trust-based multi-path routing is presented in (Narula et al 2008). Less trusted nodes are given lower number of self-encrypted parts of a message, making it difficult for malicious nodes to gain access to the minimum information required to break through the encryption strategy. Trust based multi-path routing allows network to operate with vital nodes and reduced redundancy. Simulation results, coupled with theoretical justification, affirm that the proposed solution in (Narula et al 2008) is much more secured than the traditional multi-path routing algorithms.

2.3.7 Event and Traffic-Load based Mechanism

Two main contributions are presented in (Cano et al 2009) namely, (i) Collective QoS definitions to measure event detection capabilities and (ii) A traffic-aware low power listening MAC to improve the network response to sporadic changes in the traffic load. To improve collective QoS, MAC protocols should react to sporadic increases in network load during event detection without compromising energy consumption. The protocol presented here combines an unscheduled access (low load) and a scheduled access (high load). The unscheduled access is based on the Low Power Listening (LPL) B-MAC protocol and a variation of S-MAC. With low traffic load, B-MAC protocol shows better performance as the energy consumption and delay are reduced. However, as traffic grows, continuous collision of preambles, specially in a multihop network, degrades the performance. But, S-MAC with adaptive duty cycle can provide low delay, low energy consumption and a better hidden terminal management in high load conditions. LPL with scheduled Wake up after Transmissions (LWT-MAC)
extends normal B-MAC operation by taking advantage of local synchronization of nodes that overhear transmissions. It can be seen that the energy consumption of LWT-MAC is slightly higher when compared to the B-MAC protocol except for high traffic loads.

2.4 MITIGATING ATTACKS

Various ideas have been discussed in the literature to mitigate attacks in MANETs. Some of them are briefly discussed in subsections 2.4.1 to 2.4.11.

2.4.1 Secured AODV based Routing to Mitigate Blackhole Attack

A thorough study has been performed in (Deng & Agrawal 2002) for security issues, in particular for blackhole attacks in MANET. AODV based routing solution is presented in (Deng & Agrawal 2002). To mitigate the blackhole attacks, it is proposed to disable the ability of intermediate nodes to reply. The reply messages can be sent only from the destination node, but the high routing delay made it infeasible. A more practical solution is proposed in (Deng & Agrawal 2002) which uses one more route to an intermediate node that replays RREQ message to check whether the route to destination exist or not. Simulation results show that the proposed method mitigates blackhole attacks and improves the throughput (Kurosawa et al 2007) considerably.

2.4.2 Distributed Request Propagation Technique

A novel mechanism to resist creation of in-band wormhole attacks is proposed in (Su & Boppana 2007). The proposed method is based on distributed techniques and statistical profiling. The major advantage of the method is, it does not require network-wide synchronized clocks, at the same time it does not impose any additional control packet overhead and need only
simple computations by the source or destination in the network. The proposed approach is implemented using Ariadne and evaluated using the Glomosim simulator. Experimental results show that in-band wormhole creation and usage can be reduced by a factor of 2 to 10 with low false alarm rates.

2.4.3 Packet Leashes Mechanism

A protocol named TESLA with Instant Key Disclosure (TIK) is presented in (Hu et al 2003, 2006, Wang et al 2006) for detecting and defending against wormhole attacks. The proposed protocol introduces a general mechanism of packet leashes to detect wormhole attacks. Two types of leashes, namely geographical and temporal leashes are used to restrict the maximum transmission distance of a packet. The temporal leash is incorporated in TIK which provide instant authentication of data packets. The proposed solution protects the network against replays, spoofing and wormhole attacks. TIK requires public keys for nodes in a network and has relatively modest storage per packet size. A node needs to perform 3 to 6 hash function evaluations per time interval to maintain up-to-date key information. TIK imposes no more than 18% load on CPU time, even when flooded with packets at the maximum speed of the wireless network and normally uses less CPU load than that in normal operation. TIK does not require significant additional processing overhead at the MAC layer, since the authentication of each packet can be performed on the host CPU.

2.4.4 Attack Detection and Recovery based Mechanism

An efficient method to analyze and detect various attacks in MANET is proposed in (Viswanatham & Chari 2008). The proposed method modifies the conventional AODV routing protocol using an agent called MYAODV. It works in two levels. Initially, it detects nodes which drop data
packets, divert routes or consume extra resources. After detection, the recovery process is started where the malicious node is isolated from the network. Simulation results show that the performance of the proposed method improves significantly by reducing the number of packet drops in various attacks.

2.4.5 Cumulative Frequency, Behavior and Authentication based Detection Technique

A routing technique which mitigates MAC layer attacks is proposed in (Murugan & Shanmugam 2010). The proposed method uses three techniques simultaneously: (i) Cumulative frequency based detection technique for detecting MAC layers attacks, (ii) Data forwarding behavior detection technique for packet detection and (iii) Authentication code based technique for packet modification. Nodes are periodically checked whether they are malicious or not. Simulation results show that the proposed method provides improved security and reduces the packet drops.

2.4.6 Secure Route Discovery Mechanism in Cooperative Blackhole Environment

A detailed analysis on different types of attacks, such as black hole attacks, cooperative black hole attacks and other possible attacks on MANETs is presented in (Bhalaji & Shanmugam 2011). The proposed solution in (Bhalaji & Shanmugam 2011) mitigates cooperative black hole attacks by identifying and isolating black hole nodes. Evaluation is done through simulation and the results obtained are compared with that of the DSR protocol in terms of throughput, packet delivery ratio and latency.
2.4.7 Performance Comparison of Reactive Protocols for Blackhole Attack

A detailed investigation about the performance of AODV is done in (Dadhania & Patel 2013). The performance of AODV and DSR protocol is measured with and without black hole attacks with Constant Bit Rate (CBR) traffic under various network mobility. Simulation evaluates and compares it with standard protocols with respect to throughput, packet delivery ratio and end-to-end delay. Extensive experiments are performed using network simulator (NS-2) for 50 nodes in ad hoc network environment. It is observed that AODV protocol is more vulnerable to a black hole attack than the DSR protocol.

Detection, Prevention and Reactive AODV (DPRAODV) is proposed in (Raj & Swadas 2009). It detects black hole attack by isolating malicious nodes from the network. It stores incoming Route Reply Packets (RREPs) and destination sequence numbers in the routing table. It also calculates threshold value to evaluate dynamic training data in every time interval. The proposed solution makes the participating nodes to realize that malicious neighbor is not allowed to participate in packet forwarding operations. In conventional AODV, a node which receives RREP packet first checks its routing table sequence number value. The RREP packet is accepted if it has a RREP sequence number higher than the one in a routing table. DPRAODV also checks whether the RREP sequence number is higher than the threshold value in every time interval. When the value of RREP sequence number is found to be higher than threshold value, the corresponding node is thought to be malicious and is added to the black list. When an anomaly is detected, a new control packet, ALARM, is forwarded to neighbors which contains the blacklisted nodes. Neighboring nodes discard further RREP packets from those blacklisted nodes.
A routing protocol to handle single and cooperative black hole attack without degrading network performance is presented in (Weerasinghe & Fu 2008, Mittal & Taluja 2012). The proposed approach in (Weerasinghe & Fu 2008) detects the presence of a black hole in the network using reputation tables and assigning reputation values to participating nodes. It improves the security with existing association based DSR protocol using the concept of reputation node’s value and by identifying and isolating black hole nodes working in a group.

A comparative analysis of the black hole attack is presented in (Gupta et al 2011) using both proactive routing protocol (OLSR) and reactive routing protocol (AODV). The impact of attack on the performance of MANET is evaluated by finding which protocol is more vulnerable to attack. The protocol is analyzed on various performance metrics such as throughput, network load and end-to-end delay. In a network, it is important for a protocol to be redundant and efficient in terms of security. The percentage of severances in delay under black hole attack is 2 to 5 percent in OLSR, whereas it is 5 to 10 percent for AODV. The throughput of AODV is effected twice as compared with OLSR. In case of network load, there is less effect on AODV when compared to OLSR.

2.4.8 Sequential Probability Ratio Test Detection Scheme

A intrusion detection scheme to detect in-band wormhole attack is proposed in (Zheng et al 2008). The detection scheme uses the Sequential Probability Ratio Test (SPRT). The SPRT has been proven to be an optimal detection test when the probability distributions of both normal and abnormal behaviors are given. Furthermore, non-parametric methods are introduced which are more adaptive to mobile scenarios and require no training. The performance and detection accuracy of various schemes are compared, in the presence of congestion. A tradeoff analysis among detection latency and
probabilities of false alarms and missed detection is also presented in (Zheng et al 2008). Simulation shows that the proposed detection schemes use delay measurement to detect wormhole attacks with great accuracy.

A simple lightweight protocol, called LITEWORP is presented in (Khalil et al 2005), to detect and mitigate wormhole attacks in ad-hoc and sensor wireless networks. LITEWORP uses secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. Different ways of launching wormhole attacks and how LITEWORP handles them are illustrated in (Khalil et al 2005). The solution detects the wormhole and isolates malicious nodes in the network. The results show that the fraction of packets lost due to the wormhole, when LITEWORP is applied, is negligible when compared to the loss encountered when the method is not applied. The lightweight features of LITEWORP make them suitable for sensor networks. The cost analysis shows that LITEWORP has low storage, processing and bandwidth requirements.

A neighbor discovering scheme, Mobile Secure Neighbor Discovery (MSND) is presented in (Stoleru et al 2012). MSND offers a measure of protection against wormholes by allowing participating mobile nodes to determine neighbor nodes in a secured manner. The proposed scheme determines valid neighbours with the presence of wormholes in network, with correct localization and proper control over the network. MSND leverages concepts of graph rigidity for wormhole detection.

2.4.9 Secure Central Authority Position Tracking System

A countermeasure for wormhole attack, called MOBIWORP is presented in (Khalil et al 2008) which efficiently mitigates the wormhole attack in mobile ad hoc networks. MOBIWORP uses a secure central authority (CA) for global tracking of node positions. Local monitoring is used
to detect and isolate malicious nodes locally. Additionally, when sufficient suspicion builds up at the CA, it enforces a global isolation of the malicious node from the whole network. The effect of MOBIWORP on the data traffic and the fidelity of detection is brought out through extensive simulation using ns-2. The results showed that as time progresses, the ratio of data drop comes to zero with the capability of MOBIWORP to detect, diagnose and isolate malicious nodes. MOBIWORP is shown to completely eliminate framing of a legitimate node by malicious nodes, at the cost of a slight increase in the drop ratio. The results also showed that increasing mobility of the nodes degrades the performance of MOBIWORP.

2.4.10 Game Theoretic Framework

A game theoretic framework proposed in (Li et al 2010) is used to analyze the strategy profiles for legitimate and malicious nodes in MANET. The situation is modelled as a dynamic Bayesian signalling game. Regular nodes consistently update their beliefs based on the opponent’s behavior, while malicious nodes evaluate their risk of being caught to decide when to flee. Some possible countermeasures for regular nodes that can impact malicious node’s decisions are also presented. An extensive analysis and simulation study showed that the proposed equilibrium strategy profile outperforms other pure or mixed strategies and proved the importance of restricting malicious node’s advantages brought by the flee option.

A game theoretic trust model called Distributed Emergent Cooperation through Adaptive Evolution (DECADE) is presented in (Mejia et al 2012). The main purpose of introducing DECADE is to prevent selfish nodes in MANET. Selfish nodes are those nodes that use resources from other nodes to send their own packets, without offering their own resources to forward other node’s packets. Thus, rational nodes (those nodes willing to cooperate if deemed worthy) must detect and isolate selfish nodes in order to
cooperate only among themselves. The design of DECADE is shown by first, analyzing a simple case of packet forwarding between two nodes and then the results are extended to bigger networks. In DECADE, each node seeks individually to maximize its chance to deliver successfully their own packets, so that the cooperation among rational nodes and the isolation of selfish nodes appear as an emergent collective behavior. This behavior emerges as long as there is a highly dynamic interaction among nodes. DECADE includes a sociability parameter that encourages nodes to interact among them for faster learning and adaptability. Additionally, DECADE introduces very low overhead on computational and communication resources, achieving close to optimal cooperation levels among rational nodes and almost complete isolation of selfish nodes.

2.4.11 Secure and Reliable Broadcasting Scheme

An authentication scheme called Collaborative Rateless Broadcast (CRBcast) is presented in (Ayday & Fekri 2012). The CRBcast is built on top of a reliable and energy efficient broadcasting protocol to improve efficiency and reliability. Reliability and security of broadcasting is critical in Wireless Sensor Networks (WSNs). Since reliability and security compete for the same resources. A typical attack called byzantine attacks in which the adversary can compromise nodes and then drop or modify the legitimate packets or inject its own packets into the network. For reliable and efficient multihop broadcasting, it is critical to reduce the energy consumption and latency. To prevent the adversary from consuming network resources, each receiver node should make sure that packets it receives are authentic and it filters out malicious packets immediately. The CRBcast scheme is resilient with respect to Byzantine and flooding attacks. Moreover, the scheme outperforms in terms of efficiency and data availability (Ayday & Fekri 2012).
Key management (KM) and secure routing (SR) are two most important issues for Mobile Ad-hoc Networks (MANETs), but previous solutions tend to consider them separately. This leads to KM–SR interdependency cycle problem. Zhao et al (2013) proposed a KM–SR integrated scheme that addresses KM–SR interdependency cycle problem. By using identity based cryptography (IBC), this scheme provides security features including confidentiality, integrity, authentication, freshness and non-repudiation. Compared to symmetric cryptography, traditional asymmetric cryptography and previous IBC schemes, this scheme has improvements in many aspects. Also provide theoretical proof of the security of scheme and demonstrated efficiency of the scheme with practical simulation.

2.5 OPTIMIZING MANET ROUTING USING SWARM INTELLIGENCE

Wide range of optimization techniques have been proposed in the literature for attaining optimal and secured routing in MANET, which is inspired by Ant Colony Algorithm (ACO), Genetic Algorithm (GA), Swarm Intelligence (SI) etc. Some of them are discussed in subsections 2.5.1 to 2.5.3.

2.5.1 Performance Comparison of ACO Algorithm

The most challenging task in MANET is finding an efficient and secured routing in spite of mobile and dynamic nodes in MANET. In ACO routing algorithms, artificial ants are used to establish an optimal route between source and destination. One artificial ant could communicate with others indirectly by depositing pheromones. The performance analysis of Ant Colony Optimization (ACO) algorithms for MANETs is presented in (Sebastian 2013). The results obtained in (Sebastian 2013) have proved that ACO algorithms are suitable for MANETs where nodes are moving mobile and dynamic with frequent topological changes.
2.5.2 Cellular Robotics System using Swarm Intelligence

Swarm Intelligence (SI) was first introduced in the context of cellular robotics system in (Beni & Wang 1989). SI makes use of relatively simple biological agents for communication with the environment. SI based methodologies, techniques and algorithms draw their inspiration from the behavior of insects, birds and fishes and their unique ability to solve complex tasks in the form of swarms, although the same thing would seem impossible at individual level. Indeed, single ant, bee or even bird and fish appear to have limited intelligence as individuals, but when they operate as community, they seem to be able to accomplish hard tasks such as finding the shortest path to a food source, organizing their nest, synchronize their movement and travel as a single coherent entity with high speed etc. This achievement becomes even more significant if it is taken into account that they accomplish such tasks without the presence of a centralized authority dictating any of this behavior. Applications of this can be found in NP-hard optimization problems such as the travelling salesman problem, assignment problem, job scheduling, vehicle routing etc.

2.5.3 Public Key Infrastructure(PKI) over Ant Colony based Routing Algorithm

An ant-colony based routing algorithm, namely, AntPKI, is presented in (Kadri et al 2013). AntPKI is a simplified implementation of PKI for MANETs over swarm intelligence routing. ACO routing algorithms use two different types of artificial ants for discovering and establishing routes, namely, Forward Ant (FANT) and Backward Ant (BANT). FANT searches the entire network to find possible routes from source to destination and deposits an artificial pheromone in intermediate nodes. This pheromone values are used by BANT to select a final route. While constructing the solution, pheromone table is updated with new pheromone value. The
pheromone values are increased by FANT during its forward movement and decreased by BANT if the route is not optimal. AntPKI algorithm presented in (Kadri et al 2013), guaranties data confidentiality by establishing session key along with certificate publishing.

2.6 CONCLUSION

This Chapter discusses various Intrusion Detection Systems (IDS) that are available in the literature. It also discusses some of the secured routing techniques. It presents different mechanisms available to mitigate various threats in MANETs. It can be seen that most of the attacks that have been detected are modifications of infrastructure based wireless networks and wired networks. Various types of IDS, such as decentralized IDS, mobile IDS, distributed certificate mechanism, monitoring based IDS, watchdog, realtime IDS etc. are used to detect different types of security threats against MANET. Various mechanisms have been discussed for enhancing the security issues in MANET, which is based on authentication, encryption, location aided cluster based, reputation, cooperation based routing etc. Finally it discusses some of the work done on applying swarm intelligence for MANET routing. It is evident that PDR and End-to-End delay play a very significant role and has been found to decrease in the presence of malicious nodes. It can also be seen that metaheuristic algorithms including Genetic Algorithm (GA), Swarm Intelligence (SI), Ant Colony Algorithm (ACO) play a significant role in improving QoS, even when they suffer from local minima problem. MANET routing must also consider other aspects such as bandwidth constraints, mobile nodes, dynamic topology and power consumption due to limited battery life. In order to improve the QoS in MANETs, selection of secured optimal route is of paramount importance.