CHAPTER 2

LITERATURE REVIEW

2.1 OVERVIEW

An extensive literature review has been carried out on the methodologies to thwart the sinkhole attack in the mobile ad hoc networks. All these existing methodologies in the literature are classified into the following broad categories.

- Network monitoring based detection
- Detection methods by modification of protocols
- Agent-based detection
- Anomaly detection
- Intrusion Detection Systems (IDS)
- Detection methods using cryptographic techniques
- Trust / Reputation based detection

This chapter provides the details of these existing methodologies and presents their merits and demerits.

2.2 NETWORK MONITORING BASED DETECTION

methodology is implemented in all the mobile nodes of the network. During Initialization phase, AODV carries out the route discovery; it propagates the RREQ to its neighbors. Methods for the attack detection in MANET by the internal attackers have been proposed in the literature. Vigna et al., (2004) proposed detection of attacks based on a stateful misuse detection technique. Specially designed sensor nodes are utilized. These sensors are designed in such a way that they either observe the behavior of the nodes or exchange the information among other sensors in the network. This method requires the deployment of huge such sensors in mobile nodes for the detection of various attacks. Further, these sensors exchange a lot of update messages among them. This causes devastating congestion in the network. Chris and Jack (2005) introduced few parameters to detect the sinkhole attackers in MANET. For detecting sinkhole nodes, a threshold-based methodology was also proposed. One of the parameters to detect sinkhole attack is 'route add ratio'. Route add ratio measures the ratio of routes which cross a specific mobile node to routes includes to the route cache of this node.

However, some nodes are susceptible to be faced with equivocal situation when they are positioned around the center of the network topology. The nodes which are nearby the center of the network have high route add ratio value though these nodes are not sinkhole attackers. The other parameter to detect sinkhole attack is 'sequence number discontinuity'. This parameter denotes the dissimilarity between sequence numbers of previous RREQ from the specific node to the sequence number of the current route request message of the node. However, an intelligent sinkhole attacker can increment the sequence numbers in such a way that it is larger to show that it has the fresh route and sufficiently smaller to get rid from the detection rule.
The method proposed by Gagandeep, A., and Kumar, P. (2012), utilizes the sequence number and the hop count of the on demand routing protocols to identify the sinkhole behavior of the mobile nodes and isolate them. During the storage phase, information of each RREQ such as sequence number, hop count & node id are stored in routing table. At the investigation phase, the source sequence numbers of current and the previous route request messages are compared and the difference between them is calculated. When source sequence number in the current route request is bigger than that of the previous request, then node from which current route request received is considered as malicious. The entry about this routing information is discarded from route routing table. The normal operation of AODV resumes at the resumption phase. The additional control messages used in this approach increases the routing overhead.

Padmanabhan and Simon (2002) emphasized the importance of ensuring robustness in packet forwarding. They proposed a protocol to enable the mobile nodes to locate the source node of routing misbehaviors. The protocol measures the performance of the paths. When the performance of a path drops beyond a threshold level, a linear search algorithm attempts to find out the link in that path responsible for dropping the path's performance. It uses probe packets which are similar to ordinary packets. It uses secret sharing to differentiate between individual losses and losses beyond a certain threshold. Because of the linear search algorithm, this method is slower to find a faulty link. Hence, it experiences larger detection time. B. Awerbuch et al., (2002) proposed a method where each of the route request packets include a weight list, a list of links, and the cost (metric) associated with each such link. These costs are derived from the node’s previous experience in sending packets over that specific link. When the route request packet reaches the destination node, it broadcasts a route reply packet. Each node forwards a route reply packet if it
has not previously forwarded a better route reply packet. Specifically, each node calculates the total cost of the recorded hops in a route reply sums up the cost of the hop between the previous node and itself.

If this total cost is less than the total cost of the previously forwarded reply, then the node also forwards this reply packet. This technique is vulnerable to the hop-drop attack. In hop-drop attack, a node forwarding a reply packet removes one or more nodes from the reply message that it forwards. Moreover, the number of reply messages sent in response to a single route request message is potentially exponential, even in the absence of malicious attacker. In the multidimensional feature vector based method proposed by S. Kurosawa et al., (2007), to detect the malicious attack in AODV, destination sequence number is used. During the normal operation, the sequence number of each node changes based on the traffic conditions of the network. When the attack takes place, regardless of the environment, the sequence number is increased largely. Further, the number of sent out RREQ and the number of received RREP is almost the same.

Hence, the number of sent out RREQ messages and the number of received RREP messages are calculated. Based on the difference in these values the malicious activity of the nodes are traced. The accuracy of the detection method can be improved by considering more features. Marchang N and Datta R (2008) proposed two algorithms to identify attacker nodes. Clique contains a group of mobile nodes where every two nodes are available within the communication area of other node. The proposed ADCLU algorithm detect malicious nodes in a cluster of nodes. The cluster is a collection of mobile nodes in which every nodes is one hop neighbor of others. In cluster, each of the nodes can be outside the communication range of others. Every cluster or clique has a
monitoring node observing the behavior of other nodes for misbehavior detection.

In the scheme proposed by Gisung Kim et al., (2010), When a mobile node is in the reception of route request message having the originator ID equal to that of receiving mobile node, it examines sequence number of message. If the sequence number in the route request message is higher to the present sequence number of the mobile node, the current node identifies the presence of sinkhole node; also it concludes that the RREQ message comes from sinkhole node. Hence, it is concluded that the route path of the request message contains sinkhole node. However, in practical scenario, not all the bogus route request messages reach the victim node and the sinkhole node will not be detected.

The OCEAN methodology proposed by Bansal and Baker (2012) extends DSR protocol to use Monitoring and reputation systems. This methodology gives substandard conclusions that results because of the wrong allegations. the assumptions made in the methodologies presented by Marchang N and Datta R (2008) are, when a malicious node receives a message, it is sent to a minimum of 50% of the remaining mobile nodes and monitor node is a legitimate node; malicious nodes are not aware of detection process. These assumptions seems to be unreasonable in real applications.

2.3 DETECTION METHODS BY MODIFICATION OF PROTOCOLS

Girish Kumar Verma and Rachit Jain (2016) proposed table driven approach for the detection of sinkhole attack in MANET. The routes learnt through the route request and route replay messages are stored in a buffer. This buffer is analyzed for the misbehaving node. These kind of approaches increase the latency in the network. Deng et al. (2002) presented a method which needs
intermediary node sending back route reply message having next hop details. At the instance the originating node gets this route reply message initiated by the intermediary node, it unicasts Further Request message to the next node to examine if it hold a path to the intermediary device and a path to target node. On the reception of this Further Request packet, the next hop node sends a Further Reply packet to originator node. As per the details available in Further Reply message, the originator checks the legitimacy of the path.

The methodology proposed by Lee et al. (2002) demands intermediary device to initiate confirmation request message to next hop present in the route towards the target. Next hop gets this message; checks with the cached routing information for a path to target. If a path leading to the target node is present in its route cache, it replies with confirmation message to the originator with the details of its route. The originator node decides if the route from the route reply message is legitimate. This is achieved by relating the details available in confirmation message. These approaches require modification in the underlying network layer protocols. Modifications in the network layer protocol increases the routing overhead. The increase in the routing overhead is not desirable in MANETs.

Marti et al., (2000) attempted to mitigate sinkhole nodes in MANET using Watchdog. The underlying protocol here is DSR. To identify the malicious behavior of a node, the node sending the traffic observes promiscuously the transmission of the neighboring node en route. If the neighboring node is inferred that it is misbehaving if it has not furthered the traffic. The watchdog maintains a copy of recently sent packets and compares each overheard packet with the packets it holds in order to find the similarity. If they are similar, the packet in the buffer is deleted. If a certain packet is in the buffer beyond certain time, the watchdog increments a failure tally for the node
which should have forwarded the packet by one. Once, that counter exceeds a
certain threshold value, it concludes that the node is malicious and sends a
notification to the source node. The trust calculation in this method is based on
the watchdog mechanism. The solution proposed by Park et al. (2004) to
identify the malicious node involves identifying the redundant path between the
source node and the destination. The source node sends the ping packet to the
destination node through three different routes by assigning different sequence
numbers. From the shared hops, the source node identifies the trusted route.
However in the practical scenario, due the mobility of the nodes, redundant
paths rarely exist. This method also increases the end to end delay of the traffic.

The second part of the solution requires each node to maintain two
tables; one table maintains the record of the sequence numbers of the packet
sent and the other table maintains the sequence number of the last packets
received from every sender. But the attacker node can monitor the sequence
numbers during the communication and update the table for last packet
sequence number. P. Kotzanikolaou et al. (2005) presents Secure Multipath
Routing protocol (SecMR), an on-demand, multipath routing protocol, secure
against colluding malicious nodes in MANET. SecMR discovers all the existing
valid paths between a source node and the destination node for the given
maximum hop distance. Authentication is the first phase of the SecMR protocol.
It involves the mutual authentication of the neighboring nodes. The second
phase of the SecMR, the route discovery and maintenance phase, involves the
establishment and maintenance of active routes.

Many methods have been proposed in the literature requesting the
destination or the intermediary mobile nodes to endorse the routing information
or provide supplementary information on the routes. SAODV, proposed by Lu
et al. (2009) is one of such methods. AODV protocol is suitably modified for
mitigation of the sinkhole attacks in the mobile ad hoc networks. This method uses new secure route request message and secure route reply packets with the secret code. When the originator node is in the reception of a minimum of two secure route reply messages, the shortest route among them is selected as the secure path to the target mobile node. Sun et al., (2006) proposed a method to mitigate the cooperative malicious attack. They presented a non-overlapping zone-based intrusion detection system. The nodes in the mobile network are grouped into various zones. Few of the nodes within the zones act as the gateway to other zones. The nodes in the zones use Markov Chains to detect the intrusions in the network. Alarm is sent to the gateway nodes in the event of intrusion using the proposed Intrusion Detection Message Exchange Format (IDMEF). This method uses an additional new message format. This increases the traffic in the network.

The method proposed by Sen et al. (2010) uses the genetic programming with multi-objective approach for the detection of malicious activities in the MANET. Flooding attack and the route disruption attacks are evaluated. The behavior of the malicious nodes in these attacks are different. For instance, in the flooding attack, malicious nodes continuously broadcast the bogus packets whereas in the route disruption attack, malicious node broadcast the routing packets containing bogus routing information. Hence, a general attack detection mechanism cannot be adopted for all kinds of attacks.

X. Li et al., (2010) proposed a trust-based reactive multipath routing protocol, ad hoc on-demand trusted-path distance vector (AOTDV) protocol. AOTDV uses the forwarding ratio of packets to detect the behavior of the nodes. In AOTDV, the first k shortest trusted paths are computed out as candidates during the route discovery process. AOTDV utilizes the trust values of next-hops and the number of hops to choose the best route to the destination node.
An adaptive hop-by-hop mechanism is proposed to select a forward path dynamically in terms of the trust requirement posed by a packet. AOTDV protocol performs better than AODV as it gives higher delivery ratio and lower end-to-end latency with the help of the trust model. Panagiotis Papadimitratos and Zygmunt J. Haas (2002) proposed a routing protocol for mobile ad hoc networks. This attempts to discover correct connectivity information in a network having malicious nodes. The proposed protocol uses a set of features, such as routing layer functionality, and the regulation of the query propagation. The resultant protocol does not require certification authority or the knowledge of keys of all network nodes. However, it requires that any two nodes that want to establish secure communication require to share a secret for the usage of their routing protocol modules. This is difficult to achieve in MANET environment.

Vishnu and Paul (2010) proposed the usage of backbone network. They assign constrained IP addresses to the afresh mobile nodes. When a node wants to send the data traffic to the destination node, it checks for an unused IP. The route request message is broadcasted for the destination and the RIP addresses. This IP address is unknown to the nodes which are other than the nodes in backbone network. If the originating node receives a route reply packet having the route for this constrained IP address, it denotes the presence of sinkhole node en route. This method requires a trusted third party, which is very difficult to achieve in MANET environment. Further this method requires all the nodes to be in the promiscuous mode to monitor the activities of the suspected node.

Raj, P. N. and P. B. Swadas (2009) proposed a method to defend against the security threats of blackhole attacks in the ad hoc networks. During the normal operation of AODV, the node that receives the route reply packet verifies the sequence number in its routing table. This route reply packet is
accepted if it has the sequence number higher than the one in routing table. In DPRAODV, the receiving nodes carries out additional verification to find whether the sequence number is higher than the given threshold value. This threshold value is dynamically updated during every time interval. If sequence number is higher than the threshold value, the node is suspected to be malicious and the processing node adds the node to the black list. Soon after the malicious behavior is detected, the node sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as one of the parameters. Therefore the neighboring nodes discard the further route reply packets from this node. The further route reply message packets from the blacklisted nodes are ignored. Hence, the malicious node is isolated from the network. This method considers only the sequence number as the parameter to detect the malicious node. Hence, this method exhibits higher false detection rate.

Mitchell, R., and Chen, R. (2014) dealt also with network monitoring based attack detection. Each node maintains the audit data about the mobile nodes in the MANET. However, the attacker who knows the existence of the monitoring mechanism in the MANET can intelligently modify their audit data. Moreover, each of the mobile nodes require to carry out additional work in order to acquire the audit information about the neighboring nodes. Ramaswamy et al. (2003) proposed a methodology to identify the cooperative malicious attack in the MANET environment. The proposed solution uses the concept of Data Routing Information table. This table contains a trusted nodes list and Cross Checking. The originating node uses only the trusted nodes with good transmission history for the transmission of data packets. If the source node doesn’t possess adequate history of the intermediate nodes then the source node will send further a request message to the next hop after the intermediate node in order to identify the trustworthiness of the intermediate node. This methodology demands more number of routing messages exchanged before the
actual data transmission. These additional messages are undesirable in the bandwidth constrained MANET environment.

2.4 AGENT-BASED DETECTION

S. Stafrace and N Antonopoulos (2010) designed an agent based framework modeled over a military command structure and an agent behavioral model. This model uses adapted military tactics to police routes, and detect intruders in the network. The agents follow a risk-based approach such that the frequency of patrols is directly proportional to the risk factor of the route. In this study, a simulation-based model detect and recover from a Sinkhole attack in a Wireless Sensor Network, using the AODV is implemented. Krontiris et al. (2008) proposed an intelligent agent-based intrusion detection system for wireless networks. The authors proposed to design their solution to the resource constrained nodes of the network such as mobile ad hoc network and sensor network. The solution uses stationary agents, which are distributed throughout the network and collaborate amongst themselves. Each node audits the raw data traffic from their neighborhood. When a node suspects a malicious node, an alarm message is raised to all the nodes in the neighborhood. Each alarmed node participates in a voting process by exchanging detection reports from the other neighboring nodes.

Shafiei, H et al. (2014) presented distributed detection of sinkhole. Few of the nodes in the MANET are considered as trusted nodes. These trusted nodes act as monitoring nodes. Each of the monitoring nodes contains the local information about the network. Furthermore, the detection operation requires a base station. These assumptions and requirements are not suitable for the MANET environment. Moreover, the trusted node can be compromised. Kachirski and Guha (2003) proposed a multisensory intrusion detection system
for the detection of insider attack in the mobile ad hoc network using the distributed mobile agents. Each agent performs different roles: network and host monitoring, decision making and taking actions. The mobile nodes are divided into different clusters. Each cluster has a head node. The head node monitors the network and collects all the packets within a cluster. Based on the packets collected over the network, the decision agents in these nodes detect and classify the security violations in the network. The monitoring nodes deployed over the ad hoc network consume large amount of energy and the bandwidth. The monitoring nodes do not participate in the actual data transmission of the network. Further, details on how the detection process is performed is not given.

2.5 ANOMALY DETECTION

Sarika, S et al. (2016) discussed the anomaly based intrusion detection and misuse based intrusion detection methods which are infeasible in mobile ad hoc networks. Huang et al. (2003) proposed a technique for anomaly detection that is capable of detecting new attacks. The patterns presented by Huang et al., (2003) are used as normal profiles to detect anomalies caused by attacks. In this technique, the flow of packet is observed at each mobile node. Features related to the traffic and topology are defined. A data mining method that performs cross-feature analysis to capture the inter-feature correlation patterns in normal traffic is proposed. However, it is noted that the topology of the MANET changes rapidly and the differences in the network state grows rapidly with time.

Mitchell, R., and Chen, R. (2014) discussed the anomaly based intrusion detection. It looks for abnormal features of the network for the classification of normal nodes from the sinkhole nodes. The bigger drawback of the anomaly based detection is the higher false positive rate in detecting the
sinkhole nodes. Another drawback is the vulnerability posed by these approaches during the training phase of the method. Sun et al., (2004) proposed an anomaly detection method. The mobility of the nodes is taken into account. This method calculates the recent link change rate. But, mobility is not the only cause of the state changes in the ad hoc networks. The topology and the state of the ad hoc network can change due to the association or the disassociation of the mobile nodes in the network. Due to this fact, the methodology presented by Sun et al. (2004) is inadequate for anomaly detection in the mobile ad hoc networks.

2.6 INTRUSION DETECTION SYSTEMS (IDS)

Mohanapriya, M., and Krishnamurthi, I. (2014) proposed a method to detect the sinkhole attack by modifying the underlying routing protocol. The proposed methodology assumes that all the links among the mobile nodes are bi-directional and all the nodes are authorized. The methodology is based on the number of messages exchanged among the nodes. This increases the overhead in the network and the assumptions here are not suitable for MANET environment. A cooperative intrusion detection system is proposed by (M.-Y. Su 2011). The mobile nodes monitor their neighboring nodes to detect the packets that are suspicious to be the malicious. This method estimates the suspicious value of a node by the amount of abnormal difference between RREQs and RREPs forwarded from a node. When the number of such packets sent by a node exceeds the given threshold, the node is designated as malicious node. The detector node broadcasts a block message to all the other nodes in the network. This block message is initially authenticated by the identification of the detector node. The block message also holds the identification of the malicious node. This indicates that the packets sent by the malicious nodes
should be ignored. This method uses only one feature to detect the malicious activity. Hence, the detection rate of this method is low.

(M.-Y. Su 2011) proposed an intrusion detection system to combat the malicious nodes in mobile ad hoc networks. The intrusion detection nodes are set in the promiscuous mode to calculate the suspicious value of a node within its communication range. The suspicious value is calculated based on the routing messages transmitted by the node. When this suspicious value exceeds a threshold value, the nearby intrusion detection system broadcasts a block message to inform the other nodes to isolate the malicious node. In this method, all the IDS nodes are functioning in promiscuous mode to sniff the routing messages. However, the value of the threshold is not discussed. P. Albers et al., (2002) proposed an adapted intrusion detection architecture for the MANETs by going through the requirements of intrusion detection systems. This proposed system is a simple trust-based mechanism with a mobile-agent-based intrusion detection system.

Mitrokotsa, A., & Dimitrakakis, C. (2013) used statistical classification algorithms for the intrusion detection in MANET. Statistical classification algorithms are largely automated. Hence, they are accurate. This methodology uses the training phase and then the classification method is used for the detection of abnormal behavior of the mobile nodes in the MANET environment. L. Venkatraman and D. P. Agrawal (2003) proposed an attack detection model for AODV. The Internal Attack Detection Model (IADM) is used to analyze local traces collected by the local data collection module and identify the misbehaving nodes in the network. When the IADM determines a malicious node, the response model (RM) broadcasts alarm messages to all the nodes in the network to isolate the malicious node. However, IADM exhibits high false positive rate.
Tseng et al., (2003) proposed specification based intrusion detection system in AODV. The specification technique is applied to monitor the AODV protocol. Initially the routing messages that are exchanged in the discovery of routes are monitored. This method places a monitoring node in the network. The monitoring node monitors the flow of the packets in the network to detect any attack. However, deploying the monitoring nodes or the sensors strategically in the network is very difficult when the topology of the network changes dynamically.

Gandhewar, N., and Patel, R. (2012) presented a methodology to detect and prevent sinkhole nodes in the mobile ad hoc network. The mobile nodes in the network monitor the behavior of the other nodes and observe the routing layer characteristics. The methodology presented in this paper works in four phases. They are initialization, storage, investigation and resumption phases. The increased number of messages exchanged contributes to the raise in the routing overhead. The inner-circle consistence concept Basile et al. (2007) is implemented for the detection of fake route reply in ad hoc networks. Each node present in the network finds its k-hop neighbor nodes. All these neighboring nodes create their inner-circle. This inner-circle takes the responsibility of voting the malicious outbound messages from any node. In specific, reply messages from the other nodes require to obtain approval of the inner-circle. Inner-circle nodes verify the legitimacy of the route reply messages. In case the reply message comprises of fabricated route information to lure the traffic, the malicious activity is traced by the way of voting carried out in the inner-circle nodes. However, this method has not addressed the problem of colluding attackers.

Mitchell, R., and Chen, R. (2014) discussed also the reputation based intrusion detection methodology. These methods are applicable to bigger
networks where creating the trust among nodes apriori is not possible. However, reputation maintenance in the mobile ad hoc network is difficult to achieve because of the mobility nature of the mobile nodes. An intrusion detection architecture is given by Manikopoulous and Ling (2003) for MANET. The intrusion detection system (IDS) runs on every mobile node. This IDS collects local data from its host node and neighboring nodes within its communication range. It processes raw data and periodically broadcasts to its neighborhood node for classifying normal or abnormal behavior based on processed data from its host and neighbor nodes. K. Nadkarni, and A. Mishra (2003) proposed intrusion detection system based on misuse detection that can accurately match signatures of known attacks. Anomalous characteristics of the mobile nodes was utilized by the IDS proposed by Partwardan et al. (2005). The traffic activities of the mobile nodes are monitored by other nodes. Audit log collected from neighbor nodes are utilized for attack detection.

Methodology proposed by Hlavacek, D. T., and Chang, J. M. (2015) for sinkhole identification has two phases. Initially, during the detection phase, the nodes present in the MANET are alarmed on the existence of the sinkhole node in the network. Then each node computes the reliability value of their neighbor. When the reliability value exceeds the threshold value, the neighbors are alerted on the presence of sinkhole nodes. The existence of the sinkhole node is confirmed by the nodes communicating with their neighbors. This methodology imposes higher routing overhead.

Garcia-Teodoro et al. (2009) used the Intrusion Detection System to determine the potential existence of the sinkhole nodes in the mobile ad hoc networks. A distributed and cooperative scheme for the detection of intrusion is introduced by Zhang et al. (2003). Each mobile node in the ad hoc network runs a SVM-based intrusion detection system agent. This agent observes the mobile
nodes, collects the local information within their radio range. Each node is responsible for the detection of the traces of the malicious activities locally and independently. If any anomaly is detected from the locally collected traces, neighbor IDS agents collectively analyze in broader area. Two modules are responsible for carrying out the response action: the local and global response modules. The computational overhead incurred by these machine learning approaches makes them unsuitable in the resource constrained mobile ad hoc networks.

2.7 DETECTION METHODS USING CRYPTOGRAPHIC TECHNIQUES

Vennila, G et al. (2014) proposed cryptography based methodology for the detection of blackhole nodes in the mobile network. It utilizes the RSA algorithm for secure communication among the nodes. The route request message is encrypted and sent from the sender side. The receiver knowing the key value is able to decrypt the routing messages. Hence, the legitimate sender and receiver nodes exchange route request messages securely. The usage of cryptographic functions is not recommended for the MANET environment. Z. Xia, and J. Wang (2006) proposed DIMH (detect and isolate malicious host) model to detect, isolate the malicious nodes and provide the integrity and authentication mechanism for routing protocol information for the requirement of secure routing. The process of detecting and isolating the (i+1)\textsuperscript{th} malicious node is carried out by the cooperation between the i\textsuperscript{th} node and (i +2)\textsuperscript{th} node. Three additional message types are included in DIMH. They are DIMH\_request, DIMH\_confirm and DIMH\_ACK messages. These three messages operate between node i and node i+2. This proposed DIMH model assumes the following conditions.
• A key management center exists which holds the public key and other information of all hosts. All the nodes register their information such as IP address, and public key, etc. to the key management center. Before any node associates with the ad hoc network, the registration process includes the authentication process between key management center and mobile host.

• Any node can request and obtain the public key of other nodes from key management center.

However, in practical MANET scenario where no central authority is possible, these assumptions are invalid.

(Zapata 2006) proposed secure AODV (SAODV) to add security to AODV Perkins et al. (2003). Two mechanisms are used to secure the AODV messages. Digital signatures are used for the integrity of route request and route reply messages. Every field in the request and reply messages are digitally signed but the hop count field of the AODV message. Hash chains are used to authenticate the hop count of the route request and route reply messages. A node which prepares the routing message signs the message with its private key.

The nodes that receive this signed message verify the signature using the public key of the sender. It facilitates every node receiving the message to verify that the hop count has not been decremented by an attacker. With the usage of the asymmetric cryptographic mechanisms, whenever a node generates a message, it has to generate the signature. If a node receives a message, it has to verify the signature. In addition to this, SAODV messages are significantly bigger because of the digital signatures. Helena R., and Jordi H. (2007) presented Secure Dynamic MANET On-demand (SEDYMO) routing protocol. This is a new security protocol that claims to offer integrity, authenticity and
non-repudiation. Its security mechanisms are based on digital signatures and hash chains. The proposed protocol assumes that a distributed Certificate Authority (CA) issues authorization certificates to control the access to the resources of the network. Certificates are extended only to the authenticated users that hold a correct reputation history. Authentication is performed using identity certificates from recognized external CAs.

Local authorization certificates bind the user identity with its IP address and cryptographic keys. They are meant to be renewed in short periods of time to guarantee malicious node ejection and isolation. SEDYMO uses public key cryptography. Hence, secret keys need not be shared among the participating node. It also does not rely on synchronized clocks. During the route discovery process of SEDYMO, intermediate nodes must always append routing information to the routing messages they forward. Also, information from previous nodes cannot be removed from the packet even if it is stale or disregarded. D. Cerri and A. Ghioni (2008) demonstrated a simpler implementation of SAODV called as Adaptive SAODV (A-SAODV). A-SAODV is a multi-threaded application. One thread is dedicated for the cryptographic computation. The other thread takes care of the other function such as processing of routing messages, routing table management, message generation and data transmission. These two threads communicate via a First In First Out (FIFO) queue having all the messages which are to be signed and verified. RSA (Rivest et al., (1978)) algorithm is used as the cryptographic algorithm and SHA1 (Fastlake et al. (2001)) is employed as the hash algorithm.

Yih-Chun et al, (2005) proposed Ariadne that withstands node compromise. This method relies only on symmetric cryptography. Ariadne authenticates the routing messages using one of three methods: shared secret keys between all pairs of nodes, shared secret keys between communicating
nodes, or digital signatures. This approach prevents the compromised mobile nodes tampering the uncompromised routes. Usage of the pairwise shared keys avoids the need for synchronization, but at the cost of higher key setup overhead. In addition to this, the encryption mechanism can be used when a small set of nodes that trust each other want to create an ad hoc network where the messages are only routed by nodes of the network. All the nodes in the network know the encryption key and, therefore, it can encrypt and decrypt every single message exchanged across the network. However, this does not scale well and the nodes in the MANET have to trust each other. So it can be only used for a very small subset of the possible scenarios.

Mohanapriya, M., & Krishnamurthi, I. (2014) presented trust based routing protocol for the detection of malicious nodes from the MANET. The detection process used in this methodology uses the route request and route reply messages. Each node monitors the neighboring nodes for malicious activities. The assumptions made in this methodology are not suitable for MANET environment. Several security schemes have been proposed for mobile ad hoc networks in literature. In the method proposed by Zhou and Hass (1999), to build a highly available and highly secure key management service, usage of threshold cryptography to distribute trust among a set of nodes is used. In the proposed distributed key management method, transmission of routing information is carried out in a redundant way such that if any route fails or any node is compromised, the network is not critically affected.

To alleviate the attackers who tries to find out the secret key of the certificate authority within a short span, the share refreshing is used. But it is assumed that the shared signature of private key of key management service cannot be disclosed to adversary. This assumption will not be true if the internal node is compromised. The proposed key management service employs share
refreshing to achieve proactive security and to adapt to changes in the network in a scalable way.

The authenticated routing for ad hoc networks (ARAN) is proposed by Sanzgiri et al., (2005). This method uses public key cryptosystem on AODV protocol. It uses the authentication mechanism and a trusted certificate server. In ARAN, every mobile node that forwards the route request or the route reply messages needs to sign it. This procedure consumes higher computing power and makes the routing messages to increase in size at every hop. These methods protect the ad hoc networks from the external attackers.

However, the attacks from the internal attackers and the malicious nodes or the compromised mobile nodes still have impact on the regular operation of the network and the network performance. The intrusion prevention methods to mitigate malicious attacks in mobile ad hoc networks includes key management, encryption and authentication ((Kurian 2004); Akosan and Ginzboorg (2000); Khalili et al. (2003); Herzberb et al. (1997); Frankel et al. (1997); Zhou and Haas (1999)). Any route request message or route reply message from one node in MANET must have been encrypted ahead of sending them over the network to the target. For the encryption, a secret key should have been shared well ahead of time.

Subsequently, decryption is required at the destination for using the information in route request or route reply messages. However, MANET lacks central coordination or authority. Hence, cryptography and authentication - centered security solutions are difficult to be implemented in the MANET. Similarly cryptography based methods consume more energy which is undesirable in the energy-constrained mobile ad hoc networks.
2.8 TRUST / REPUTATION BASED DETECTION

Several trust models have been developed for trust management in mobile ad hoc networks. These trust models are classified into two groups. They are centralized models and decentralized models. In centralized models, a common central node or an authorized third party maintains the trust values of each of the nodes in the MANET. In decentralized models, each node assigns the trust values for other mobile nodes. Several trust models (Xiong L., and Liu L. (2004), Song S., et al. (2005), Liang Z., and Shi W. (2008)) have been proposed in the literature. Although these models can be applied to routing in MANETs, information exchange among the mobile nodes will incur significant traffic in the network.

A methodology based on the sequence numbers for detecting sinkhole nodes in MANET is recommended by Sanchez-Casado L et al., (2015). The proposed methodology is based on the postulate of presence of contagion border. Nodes in the border are denoted by the genuine nodes influenced by sinkhole attackers and also holding genuine neighboring node. This permits estimation of the malevolent characteristics of nodes pretending as sinkhole nodes. This proposed methodology increases the overhead; also, only the sequence number are used as the feature to identify the sinkhole nodes. Including additional features improves the detection ratio.

In the trust model proposed by Asad Amir Pirzada et al., (2004), the trust agent of every node calculates the trust level of its neighbor. The trust calculation is carried out based on multiple observed events including the link-layer and the network layer acknowledgements, gratuitous route replies, blacklists and packet precision. These acknowledgements are requested explicitly. Hence, it introduces unwanted delay and the heavy traffic in the
network. The mobility of the nodes in the network affects the trust calculation. It is also possible that the nodes are unable to forward the acknowledgements due to heavy traffic or low battery power. Though they have obtained promising simulation results, these promising effects can be obtained with a simplified trust model.

CONFIDANT protocol specified by Buchegger and LeBoudec (2002) discourages misbehavior activities. In addition to watchdog, the node also works on details obtained through trusted mobile nodes for the identification of malicious activity of a node. The route having the malicious node is eliminated by path manager in the event of identification of malicious activity. Other trusted nodes are intimated by the path manager about malicious activity. Further, it also sends ALARM message about this misbehaving node to other trusted nodes. The CORE mechanism demonstrated by Michiardi and Molva (2002) is reputation based. It imposes cooperation among the nodes. Similar to CONFIDANT, CORE has monitoring and reputation system. Every node keeps a table for route discovery and forwarding; collected information for each node is preserved in another table. Non-cooperating nodes are given negative rating which depreciates the reputation of node. Other nodes are given positive ratings to improve the reputation. Requests from nodes with negative reputation are rejected. Malicious node is isolated from the network in this way.

Thanachai et al. (2006) demonstrated a distributed sinkhole detection method which uses trust-based calculations. Primarily, all the node allots trust value to the nodes in their neighborhood. For the duration of the transfer of messages, if a neighbor node does not send message to a designated node or the destination node, the trust-weight value it has assigned to its neighbor is brought down. This reduction in trust value is propagated in the network. If trust value of any neighboring node decreases below the given threshold value, then the
neighboring node is considered to be malicious. No centralized control mechanism is demanded by this methodology for taking decisions. It permits the mobile node to arrive at a conclusion exclusively by itself. However, this approach increases the message overhead in the network and thus results in excess bandwidth usage. Further, the nodes need to work in promiscuous mode which is not desirable in terms of energy.

2.9 SUMMARY

This chapter provides a comprehensive literature review of the existing methodologies to mitigate sinkhole attacks in MANET. The intrusion detection systems, cluster based intrusion detection and cryptographic based detection systems either require centralized authority in the MANET or poses higher computational and routing overhead. Other methodologies require either the underlying routing protocols to be completely modified or the mobile nodes to be working in promiscuous mode always. These decline the performance of the mobile ad hoc network in terms of routing overhead, packet delivery ratio and end-to-end delay. Hence, efficient methodology to detect and isolate sinkhole nodes in MANET is required.