CHAPTER 2

REVIEW OF LITERATURE

A new technique for securing the attacks and detection in mobile ad-hoc networks is developed. Some of the related works and survey related to the previous methods have described below.

- **Key Management System**

Ramkumar K.R et al. (2017) developed a Key Management for MANET using Chebyshev Polynomials. It performs key management that tested in various conditions which secret key shares symmetric key construction, generation, and key distribution. The recursive nature of this polynomial is the significance property. For implementing the overall system, the burden of mobile nodes is reduced by using Chebyshev polynomials.

Laurent E et al. (2002) have described a model for distributed network ensuring the authenticity by using a key management system. With capable of communication and limited computation of sensor nodes present in Ad-hoc mobile networks and Distributed Sensor Networks (DNS). Their work includes a key management system, which satisfies the operations of DSNs and its security requirements. Without communication capabilities and substantial computation, node re-keying, revocation of keys and selective distribution are included in this scheme.

Ricardo Staciarini P et al. (2003) have proposed a scheme for routing protocols of MANET to secure in new authentication way. It observed by the authentication service, which gives protection to the routing protocol.

Erdem O. M (2004) proposed a model using an efficient new Hierarchical Binary Tree (HBT) for the formation of grouped ad-hoc networks. It brings an alien

device for exchanging a secret key in a group using its new key distribution scheme at that time. This model is an Efficient Distributed Key Management (EDKM) having attributes, which self-organize by them where incrementally deploy in the network. This EDKM modify the membership by providing entire forward and backward security. Secret key cryptography and one-way hash function are used in this model. Therefore, MANET becomes practical and efficient by using EDKM model.

Sanyal S et al. (2010) proposed a security scheme for mobile ad-hoc networks from Distributed Denial of Service (DoS). Various attacks of DoS are possible in MANET due to limitations of the routing protocol. The misbehaving node of MANET identified by this proactive scheme, also, DoS attacks prevented by this method. Much better performance is given by this scheme than that of other existing approaches. Compromised nodes parameters monitored by this technique by shifting its responsibility on the neighbor's node.

Capkun et al. (2003) developed a method that users can leave centralized control and can join the networks using public key management system, which self-organized with trusted authorities are not relying on the user. The main advantage of this method is twofold. First, network data secured more, and second, shared key has agreed with established trust efficiently.

In this methodology, the node itself a pair of the private/public key generated using public key management. The certificate repository holds certificates to the neighboring nodes which issued by this scheme. This method to overcome trust establishment, which delayed, by using a secret dealer based on distributed trust model by initialization of trust accomplished in bootstrapping phase of the system. Each node contains some entries with a secret key, shortlisted by a mysterious dealer which provided by this scheme. The new thought was providing the robustness and redundancy using key management framework in between the nodes, which is paired with the establishment of Security Association (SA) in MANET.

- **Architecture Framework and Design**

Martin A (2017) analyzed a performance comparison of mobility models in MANET. The packet size, network size, and mobility of nodes are the factors that can deploy in any given situation. Random Waypoint and Manet_Down_left are the two mobility modes that are mainly compared in this paper.

Darren Hurley-Smith et al. (2017) proposed a protocol known as SUPERMAN, which communication security of unified mobile ad-hoc network problems addressed. Virtual Closed Network architecture implemented for protecting the application data in both networks.

Sankaranarayanan S and Murugaboopathi G (2017) used RSA algorithm for secure intrusion detection system in MANET. Here, before the attack processed to the node, the intrusion detection system finds the attacker. It is the first line of defense used in mobile ad-hoc networks.

Bin Sun et al. (2009) analyzed key management architecture and virtual infrastructure for mobile ad-hoc networks with three-layered. This scheme introduced two types of key management architecture of three-layered for analyzing the efficiency of communication between nodes in the network. The cost for the connection using three-layered key management scheme is lesser when compared to two-layered architecture. The virtual infrastructure protocol of mobile ad-hoc networks optimized using these two conditions.

Mansoor Alicherry et al. (2009) proposed enforcement architecture of distributed security policy approach, which designed especially for mobile ad-hoc networks. By implementing this approach, the network communication capabilities extended and controlled. The policy of hop-by-hop enforced in a distributed system for MANET nodes are restricted communication, which required in between the node by using this method. This scheme used a principal named deny-by-default, which authorized services only allowed for accessing by compromised nodes.

Frank Kargl et al. (2008) developed architecture for MANET named as security architecture for mobile ad-hoc networks (SAM), which work related to identity-based cryptography and use certificates for the identification.

Seongil et al. (2005) proposed architecture for mobile ad-hoc networks using self-organized authentication. It forms a secure overlay network using the concept of Neighbors for Authentication (NA).

Nagpal C.K et al. (2011) carried out a study on MANET's area shape and performance metrics like hop count, packet drop, throughput, and reliability. Various shapes like circular and equal area simulated by this study which rectangle and square followed by some nodes that less transmission range value required.

Jia et al. (2016) suggested an architecture using disturbance-adaptive platoons. It optimizes the distance and size of two platoons using disturbance scenario, which consists of traffic dynamics.

Buchegger and Boudec (2002) designed an architecture named CONFIDANT which misbehaving nodes detected, and responded by this protocol. Four components analyzed mainly in this method, path manager, monitor, reputation system and trust manager. For updating reports are the problem suffered by CONFIDANT due to conflict.

- **MANET Caching**

Raziel Carvajal Gomez et al. (2017) designed an evaluation of broadcast algorithms using mobility-driven and density in mobile ad-hoc networks. The algorithm helps to form informed the choice between protocols. In different scenarios, five different algorithms compared and then analyze regarding nodes mobility and its network density.

Liu Y et al. (2016) designed a cooperative cache model with the replacement of objects in mobile ad-hoc networks. Limited resources and topological changes are the additional constraints that differ caching of the network protocol in MANET. From this method, two schemes presented for caching, and the first one does Caching Data, which cache and objects checked by forwarding node when it is passed. An accessible object stored in a large number with the intermediate node is the main problem faced by this approach. Secondly, Cache Path method, here the paths of the objects found in closest node recorded by this scheme because the intermediate nodes cannot save the objects. From the intermediate node, it is concentrated only in passing the objects using these two approaches Cache Data or Cache Path.

Isuru U. Jayasooriya et al. (2013) have proposed a method for mobile ad-hoc networks web application which relied upon its designed protocol. Both Linux platforms and Android implemented by this iCache protocol. For the creation of MANET, this scheme used underlying Wi-Fi as part of its technology. Web data cache like web pages and images collected using the MANETs node correspondingly by different approach iCache. Data accessed on peer-to-peer when implementing iCache. Response time for fetching source data is higher when compared to iCache. Nodes density and requested object size increased with the implementation of iCache response. Internet bandwidth also preserved by this method.

Weigang Wu et al. (2013) developed an algorithm to improve the efficiency of network cache by exploring wireless communication property without having any meaning. A node can discover the packet within the transmitter range using MANET's wireless links. For optimizing cache discovery and placement, the proposed algorithm used, which includes data reply and request for overhead information. Using wireless connections, the messages, this sent and received for communication of nodes in the network.

Leo Sicard et al. (2012) developed a mobile ad-hoc protocol for a web application using a better approach. The network used a B.A.T.M.A.N algorithm for working with the nodes best path. All nodes in the network have information about

the next node. The neighbors get originator messages (OGMs) which broadcast periodically by the participating nodes in the B.A.T.M.A.N algorithm. Unique sequence number, sending node address and originator address is included in OGM. The sending address changed to its address by the neighbor nodes and messages re-broadcasted when OGM has received. After performing this scheme, the originator messages used in the network for flooding. In the network, data accessibility is provided to each node as a result.

Komal M. Sharma and Archana Raut (2013) specified that random movement of mobile ad-hoc network nodes. A Dynamic Group Caching scheme used to increase the efficiency of network caching data items. Group Head and Master manage group formed by mobile nodes.

Preetha Theresa Joy and K. Poulose Jacob (2012) improved information access efficiently, by the proposed approach of Cooperative caching used in the mobile ad-hoc network by reducing bandwidth usage and latency. It provides cache replacement policy comparison used in MANET. Coordinated and uncoordinated are two groups of replacement policies used in mobile ad-hoc networks. Using local access information, each node determines data item independently which is to be evicted using uncoordinated replacement policy. The decision for the replacement has taken by mobile nodes used cooperative caching policy, which collectively forms cooperative caching.

Shanmuga Vadivu K and Madheswaran M (2010) introduced Neighbor Group Data Caching (NGDC) to improve efficiency for accessing data in MANET. When destination node sending data object to a message host, the NGDC scheme proposes how and where to place the data object to a group member. Cooperative caching helps to improve efficiency for accessing and availability of data. Neighbor group nodes help to find communication cost of data sources which have lesser. This result in improvement of cache-hit ratio and average latency reduced.

- **Routing Protocol Concepts**

Chourasia R and Boghey R.K (2017) proposed a scheme for securing routing misbehavior of packet dropping using novel IDS in mobile ad-hoc networks. The attackers due to dynamic nature of MANET can easily modify the actual performance. This scheme analyzes the nodes activity and its performance and then blocks the node.

Ghaffari A (2017) developed a real-time routing algorithm based on Q-learning in mobile ad-hoc networks. The primary optimization objectives given here is link stability and route shortness. Lowest number of hops offered to the destination followed by a selection of a node within a group.

Adhvaryu K.U and Pariza Kamboj (2017) suggested the comparison of performance between multipath routing protocols in the mobile ad-hoc network. It is more difficult for group management when node speed increases in multicast routing and more likely to occur as tree link breaks.

Maleki et al. (2017) proposed a routing protocol for mobile ad-hoc networks that use a multi-agent RL-based. Markov Decision Process (MDP) captures the energy consumption and link delay for formulating the routing algorithm. Based on these metrics, the single-hop model is defined by the cost function.

Anirbit S et al. (2017) designed an algorithm for mobile ad-hoc networks using enhanced Zone Routing Protocol (ZRP). Here, it is mainly focused on the improvement of hybrid routing protocol constructed on the zone. Parameters like Bandwidth utilization, End-to-End delay, and Throughput are adapted as performance parameters. Based on the performance metrics like Data integrity, Jitter, and Sustention, etc., is used for comparison of ZRP and EZRP.

Nousheen Akhtar et al. (2017) proposed a method for congestion avoidance by efficient routing strategy in MANET. According to available bandwidth; its

estimation adjusts the current bandwidth consumption. The feedback of current network state is provided to source node according to its data rate.

Israel Martin-Escalona et al. (2017) designed a method for unreliable positioning impact in MANET for location-based routing protocols. Here, two methods are used namely, DYMOselfwd and AODV that implemented by OMNET++ for reducing the routing overhead. For evaluating the impact of positioning error, a uniformly distributed error has been added.

Prasanna Lakshmi G.S and ShantaKumar B Patil (2017) proposed a zone-based AODV routing protocol for signature intrusion detection in MANET. This routing protocol considers the security features like authentication, integrity, and availability. Better timing security is detected by this method.

Vimala S and Srivatsa S. K (2017) proposed a technique for securing MANET using data compression. For improving network lifetime, saving energy is the major concern for mobile ad-hoc networks. In this proposed scheme, it uses Modified Lempel Ziv Welch (MLZW) for compressing the data.

Hua YANG and Zhimei LI (2017) developed a routing optimization technology in mobile ad-hoc networks based on neural networks. For optimizing the route, Cooperative Hopfield Neural Network is used for finding a nearly optimal route for improving survivability and usability of MANET.

Usha R et al. (2017) analyzed the performance of mobile ad-hoc network routing protocols for military applications. Here, AODV, OLSR, DSDV, and DSR routing protocols are the best that used in military networks like NCMM, MARS, and RWPMM. There is no availability of such protocol that could be suitable for all mobility scenarios. The results were showing that concerning high throughput the AODV and DSR perform better, and concerning less delay, the OLSR and AODV perform well. DSDV provides the low overhead. NCMM gives the high throughput

and less latency with AODV. For low delay and high throughput, the RWPMM with DSDV gives a better result.

Bhargavi V. S et al. (2016) proposed a secured DSR algorithm for routing to form better network security. The algorithm used for dynamical routing with secure communication over routing in the network.

Sumaiya Vhora et al. (2015) proposed schemes for the availability of belief paths that drop out packet are perceived. The systematic view of network activities is precisely that identified by deploying RBDR scheme and network layers optimized in mobile ad-hoc networks when packet drop attack is put off. The network sleuthing deeds are analyzed and looked at the deployment of RBDR system where packet drop attack prevents network layer of MANET.

Venkataraman R et al. (2012) proposed link state routing (LSR) protocol and on-demand distance vector routing (ODVR) protocol as a trust model in MANETs incorporated over ad-hoc. From performance evaluations, the trust parameters set carefully for maintaining efficient throughput with minimum overhead. The ad-hoc routing protocol managed by confidence values and computed trust in their computation process of the path. Using this method, it observed that trade-off is routing traffic and end-to-end packet delay in the network for avoiding data loss, by taking trustworthy paths also by learning activities of a malicious neighbor node in the network.

Anuj K. Gupta et al. (2013) mainly proposed for the analysis of different routing protocols in mobile ad-hoc networks. The data packets sent by using mobile nodes in MANET using wireless medium. For establishing a connection between mobile nodes, a suitable routing protocol needed. Therefore, it shows property of topology changes dynamically. While determining the ad-hoc network performance, the important characteristics of routing protocols are mobility of nodes. For this reason, mobility models and effect of various routing protocols needed to know about

them. Moreover, it implemented various mobility models. It mainly focuses on two methods. First one is Random Mobility Models and the second one is Group Mobility models. Different routing protocol processed by routing technique properly by these mobility models.

Gang Ding and Bharat Bhargava (2011) proposed a concept using file sharing by peer-to-peer in mobile ad-hoc networks. Have different complexity; this approach gave five routing methods. The intermediate nodes used for communications with each other which take place between two nodes, as MANET has no structure characterized. Every node can do independent work, as it has no specific server with it. The reduction in internet bandwidth and accessing requested file quickly are the main result of this method.

Lee S et al. (2002) identified a solution for modifying routing protocol of AODV using two new packets namely route confirmation request (CREQ) and route confirmation reply (CREP). The source node got RREP when CREQ sent by intermediate node towards destination node with its next-hop node. Destination route looked up by the next-hop node using its cache when receiving CREQ. The source node gets CREP when it has a route. The source node confirms the validity of the path after receiving CREP when comparing RREP path as well as CREP. The appropriate route judged using the source node if both are coordinated.

Tamilselvan L and Sankaranarayanan V (2007) used a Fidelity Table for designing a solution that determines node reliability using fidelity level assigned to participating node. The level updates for each node using its behavior by assigning default fidelity for each node. The data forwarded to the destination by selecting a neighbor node that has fidelity level higher after receiving route replies from it when RREP received by the source node. The destination node sends ACK after it receives the data. The node in the network that has trusted participation relies on updating fidelity level. The forwarding nodes fidelity level is incremented or decremented by the source node when missing or receiving an ACK. The malicious node is marked

and eliminated from the network if fidelity level reaches zero. The high end-to-end delay is the main drawback of this proposed work.

Mi-Seon et al. (2012) proposed Mobility-Aware Hybrid Routing (MAHR) protocol. According to nodes mobility, the reactive to proactive approach changed using this routing process. When comparing with AODV, Tooska scheme, and OLSR protocol, this method is more efficient.

- **Trust Based Model**

Shima Asaadi et al. (2017) proposed a model TQOR in cognitive mobile ad-hoc networks. The acronym for TQOR is Trust-based QoS-oriented routing. Two cognitive processes are held by introducing and interacting cognition layer in parallel with the network layer. The first process is path learning (routing) that is based on machine learning algorithms and the second process is trust learning that is based on trust management.

Hansi Mayadunna et al. (2017) propose a method for identification of malicious nodes using reinforcement learning by improving trusted routing in MANET. Ad-hoc On-Demand Distance Vector (AODV) protocol is mainly focused and uses Reinforcement Learning (RL) for learning the detection of malicious nodes. It minimizes the limitations of the number of neighbors. In dynamic MANET environment, the proposed method detects the malicious nodes by reliable trust improvement and high accuracy.

Kumar S et al. (2016) developed a model that satisfies the data security in WSN using a metric consisting of data forwarding ratio and energy consumption of sensor nodes. The proposed metric is applied by finding the best wireless link by using the broadcasting properties of wireless sensor networks.

Tan S et al. (2016) proposed a model for securing data plane using trust management system in Ad-hoc networks. Various attacks occur due to ad-hoc network characteristics like dynamic topology, openness. Here, the path trust value is evaluated by using the empirical knowledge using fuzzy logic. Then, a filtering

algorithm is used for harboring and slandering. For assuring the compatibility of trust management system with other security primitives, a feasible trust-factor collection approach is presented. At last, integration of OLSR and proposed trust management system is implemented.

Pirzada A. et al. (2004) proposed the establishment of trust model in pure ad-hoc networks. Heavy computation caused due to dependence between the nodes and central trust authority in ad-hoc networks. Spurious trust occurs due to nodes in the network, which inherits knowledge from different levels of computation trust. Nodes generosity helps to calculate the trusts.

Sam Harris et al. (2007), a concept of Belief, Neuro-imaging Uncertainty, and Disbelief proposed by them. Dempster-Shafer theory mainly dealt in this paper. Combination rule of Dempster helped for the exposing "Belief, Uncertainty, Disbelief" in neuro imaging. Therefore, this concept used anywhere which Trust evaluation is the main perspective.

Kumar Viswanath and Katia Obraczka (2006) designed a concept for multi-hop wireless ad-hoc networks known as flooding. Each node has packet reach ability that used the probability of analytical model lead to flooding. An efficient broadcasting method is used for reducing flooding overhead.

Renu Mishra et al. (2010) proposed a new trust method for security in mobile ad-hoc networks. The packet-forwarding ratio increased or decreased by maintaining every node trust. Nodes grade explained with positive or negative using trust counters threshold value. The intermediate node considered as malicious when the value falls for trust.

Soltysik DA et al. (2010) proposed a method for analyzing received RREP and a solution for it. For receiving RREP's multiple requests, it waits for MOS_WAIT_TIME seconds when receiving the first RREP from the source node. Stored RREPs analyzed by the source node from the table, and consider the sender as malicious and rejects it if the destination number very high. Nodes are having the

highest number selected according to destination sequence number that arranged in the table with remaining entries. The routing node is not maintained by this technique but only has suspected malicious record that discards nodes when any control packets are forwarded or received by that node. The high end-to-end delay introduced by this algorithm that nodes have to wait for multiple RREPs.

Choudhary N and Tharani L (2015) proposed a solution for a wireless channel based on sense. All neighbor nodes have maximum trust value assigned by this approach. When the min_trust value is higher than trust value, the communication cannot occur by the node with neighbor nodes. Routing table updated when RREP messages received by the source node and the transmitted data packet contains a unique number sequence and starts sending data. Time is set when data packets forwarded by the nodes and the promiscuous node is used for listening wireless channel for ensuring that packet of next-hop neighbor is forwarded. For the next-hop node, the trust value reduced for the node without hearing packet retransmission when the timer expires. Information of trust value updated and disseminated to neighboring nodes present in the network. All nodes in the network will be isolated when a decrease in min_trust value occurs for node than the trust value.

Zia H et al. (2011) proposed a novel method for trust management. It uses logic rule prediction for evaluating nodes trust. The untrustworthy nodes that were thrown by Fuzzy dynamic programming theory are used for obtaining dependable passage delivery route.

- **OLSR Routing**

Zhinan Li and Yinfeng Wu (2017) proposed a scheme using smooth mobility and link reliability-based optimized link state routing for MANETs. Semi-Markov flat and complexity restricted mobility model is used for the implementation process. This SMLR_OLSR scheme applies a twofold. Firstly, preventing the link property evaluation which is wrong. LR formulation based RLL estimation is utilized by

presenting SMS_CR mobility model. Secondly, based on the new LR metric, a modified MPR selection strategy is proposed.

Mushtaq Ahmad et al. (2017) suggested a protocol for secure, optimized link state routing in the mobile ad-hoc network. In this method, a breach is filled for security attacks when finding paths from source to destination by including the value of message authentication code (MAC) that use a signature technique to append messages by following encryption and global secret key in both Topology control (TC) and HELLO messages. The prevention of replay attacks is not possible by encryption and authentication, so timestamp mechanism is used to prevent the attacks.

Abdalftah Kaid Said Ali and U. V. Kulkarni (2017) compared and analyzed the reactive routing protocols like AODV, DSR, and TORA in QoS of MANET. The QoS metrics of these protocols are evaluated and differentiated. The AODV outperformed well when comparing other protocols regarding load delay, media access delay, retransmission attempts, and data drop entry.

Belhassen M et al. (2011) designed an OLSR routing protocol with some improved version. Cartography Enhanced Optimized Link State Routing (CE-OLSR) is the new name for the proposed method used in MANET. Three axes are mainly used as a solution by this technique. First, one is collection scheme of cryptography efficient network that based on signaling traffic of OLSR. Secondly, OLSR enhanced version is designed with node mobility impact to appropriate coped and collected cryptography. Third, the comparison with a set of simulations that proposed with CE-OLSR and original OLSR.

Ouacha A et al. (2013) proposed a method to avoid link breaks due to mobility between the nodes and MPRs. This method proposed Remaining Time to Quit (RTTQ) as a new metric for predicting the remaining lifetime of links between nodes and neighbor set using radio scoop and distance.

D. Kumar and S. C. Gupta (2013) presented a technique for the performance of routing protocols and mobility impact on the number of common paths. It used the comparison of network performances of routing protocols as OLSR, AODV, FISHEYE and LANDMark Ad-Hoc routing protocol (LANMAR).

Zheng L et al. (2008) proposed a method for OLSR routing protocol for MPR nodes improvement using Necessity First Algorithm (NFA). For reducing overhead and MPRs in the network, this method used a solution for addressing the problem of a greedy algorithm.

You L et al. (2011) proposed an algorithm for OLSR routing that Time Division Multiple Access (TDMA) performance improved by exploiting MPR method and gateway selection.

Chizari H et al. (2009) proposed a genetic algorithm based MPR selection method and a large number of nodes with maximal independent concept followed by MPR sets.

Dashbyamba N et al. (2013) extended the work with new protocol by OLSR improvement when the selection of MPRs taken into account by its signal strength and mobility of nodes. Hence, parameters of OLSR standard are not considered.

Banik S et al. (2010) designed an MPR algorithm with some improvement in it by using quality of service (QoS) parameters. These include end-to-end delay and bandwidth efficiency into a single numeric weight.

Johansson P et al. (1999) presented a study by comparing three routing protocols namely Ad-hoc On-Demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR). A new mobility metric can be functioned using this comparison using scenario-based performance analysis which relative velocity reflects from it.

- **Dynamic Key Management**

Ming Yu et al. (2009) designed key based secure routing. Here, Dynamic Key Management scheme is used about RSA. The RREQ and RREP bits formulate by every node that helps to decide about the packets reached the destination or not. The clusters each node distributed by public key using this key management. During broadcasting, promiscuous mode activated for cluster head. Consumption of resource is high.

Katrin Hoeper and Guang Gong (2006) proposed a bootstrapping security method for the mobile ad-hoc network. Two schemes developed by this method. First, IDentity (ID) based Authentication and the second one is Key Exchange (IDAKE). Unique features like efficient key management and parings of pre-shared secret keys are present in Identity-Based Cryptographic (IBC) scheme. MANET-IDAKE designed by employing IBC scheme to meet the requirements and unique constraints of mobile ad-hoc networks. The security of MANETs was bootstrapped by utilizing the merits of this scheme. Before joining the network, TTP initializes all devices which mentioned in this scheme. Moreover, central TTP is not required for MANET-IDAKE scheme that is entirely self-organized. Various types of applications, which are available in mobile ad-hoc networks that implemented by using this efficient IDAKE scheme. Security protocols like key exchange and authentication enabled by this scheme.

Fagen Li et al. (2005) proposed a method for ensuring the security protocols of mobile ad-hoc networks. A distributed key management approach was proposed by this method by using threshold secret sharing and self-certified public key system. The advantages of using this scheme are communication overhead, and storage space can be reduced which certificate is unnecessary and decrease in computational cost due to public key verification is not required. User's private keys not known by Certificate Authority (CA) due to key escrow problem is not available. By comparing

with IDentity-based (ID-based) public key system and certificate-based public key system, the proposed approach is much efficient.

- **Symmetric Key Management**

Aldar Chan and Edward Rogers (2004) described a method for the mobile ad-hoc network using distributed symmetric key management. Existing schemes of key management is not too efficient and not functional to unknown network topology, link failures or changing network topology. Hence, these are not applicable for ad-hoc networks. Before deployment, we are not known by this network topology. Key Pre-Distribution Schemes (KPS) is the scenarios practical option. Trusted Third Parties (TTP) relies on this scheme. Without having infrastructure support, it is realized as self-organized key pre-distribution and fully distributed constructed by DKPS prototype using Distributed Key Pre-Distribution Scheme (DKPS) approach. The drawbacks of previous works can be eliminated by using this DKPS approach.

Virgil D. Gligor (2004) proposed an approach for enhancing security in Ad-hoc networks. Ad-hoc networks have emergent properties, which is a common characteristic of this method. The network nodes individually cannot provide emergent properties spontaneously by themselves; instead, network nodes give result by collaboration and interaction with other nodes. Several fundamental ways used for protocol interaction for establishing traditional network properties which are different from security characteristics and emergent properties proposed by this approach? By this approach, distinguishing security implications and emergent properties are determined. Desirable and undesirable emergent properties presented by giving some examples by this method.

- **Certificate Revocation**

Park Y and Sungwook Kim (2016) proposed a method based on a weighted voting game approach for efficient certificate revocation scheme in mobile ad-hoc

networks. A new voting-based security scheme is designed based on the game theoretic model. The current system conditions are practically responded, and this game-based security paradigm provides ability that suitable real-time mobile ad-hoc network operations. Based on this weighted game model, the malicious nodes efficiently handled in MANET. The dynamic changing can be adaptable, flexible and able to sense for MANET environment.

Micali S (2002) presented a new model named NOVOMODO that enhanced and improved version of revocation techniques. This approach offers a mobile scenario, which has a valuable step for scalable revocation. Here, Certificate Revocation List (CRL) is used for controlling certificate approach. This list shared and managed among single or multiple CAs. Each node assigned with a digital certificate valid for some particular period by using the Certificate Authorization. The CRL is added with certificates of the suspicious node that revoked by CA. The entire network is broadcasted with updated accused node list with valid license into CRL.

Kocher P. C et al. (2004) proposed a system using asymmetric cryptography that presents existing requirements for a cryptosystem. The essential aspects include reliability, performance/scalability, security, and simplicity. The author proposed three revocation techniques likely to be online revocation, revocation trees, and revocation lists.

Perlman R (1999) showed several PKI models in a different manner that are compared and discussed previous techniques. The crucial design of PKI in this system has efficient and scalable with revocation mechanism that preserves security and supports the system.

Housley R et al. (1999) proposed a certificate for status information of certificate (CSI) which to be handled. Certificates and status handling are dealing with previous work like RFCs. For this reason, one active mechanism like Online Certificate Status protocol is provided for the updating CSI.

Elwailly F et al. (2004) designed an approach named as QuasiModo schemes in which Merkel Trees are used to provide certificate revocation and verification into single and multiple methods.

Luo H et al. (2004) proposed URSA method which certified tickets which are used and nodes are evicted from the network that is locally managed. Third-party trust systems like CA were not used in URSA. Neighbors, issue tickets for newly joined nodes. The votes from the neighbors were used for revoking ticket of a malicious node due to centralized authority is not available. In URSA, one-hop monitoring performed for each node. The identification of malicious node allowed by neighbor's monitoring information, which exchanged within. Successfully, revocation of tickets from the accused node is done when certain threshold exceeds the number of votes. Without having valid tickets from node then it cannot communicate with each other. Isolation of particular node indicates by revoking nodes ticket. For false accusation attacks, URSA is strong against it. However, collision attacks by multiple malicious attackers are the issue of coping.

Arboit G et al. (2008) proposed a voting-based scheme that allows voting by every node present in the network. The network has no CA existed like URSA. Instead, neighbor’s behavior is monitored by each node. Variable weight with nodes vote is the primary difference of this scheme with URSA. Using the past practice, the reliability of nodes derived which used for calculating weight. The weight will be more significant when reliability is higher. A predefined threshold of nodes exceeds or reaches when summing weights of votes are against it and revoked the suspicious node's certificate. Certificate revocation accuracy improved by doing the same. For revoking the certificate, increase in time is needed that is due to a participant of all nodes for voting is required and communication overhead required as exchange voting information is higher.

Clulow J and Moore T (2006) described a decentralized suicide-based approach. With just an accusation, certificate revocation completed quickly by using

this approach. Accuser's certificate and certificate of accused node revoked using this proposed method. In other words, the attacker removed from the network by sacrificing one node by itself. Both communications overhead and node eviction time reduced for certificate revocation procedure dramatically by using this strategy. The approach is limited to the application by owing suicide-based policy. For differentiating correctly, accused malicious nodes by falsely accused legitimate nodes by proper mechanism are not provided by this scheme.

- **Cluster-Based Techniques**

Gomathy D and Sathiya D (2017) proposed techniques using clustering and without clustering methods in mobile ad-hoc networks for scrutiny of broadcasting efficiency. High overhead which caused by brute force attitude is avoided using this cluster-based broadcasting scheme. For maximizing the NRL and packet delivery ratio, this method is used that reduces delay and overhead.

Farooq Aftab et al. (2017) proposed a method using zone-based group mobility in MANET for self-organization based clustering. The bio-inspired behavioral study of birds flocking algorithm is used for maintaining and forming of clusters in mobile ad-hoc networks for improving stability and scalability of the overall network. Network congestion is reduced by taking cluster size managements efficient mechanism, and it enhances the performance of group mobility in MANET. For handling isolated nodes, an algorithm is proposed by proper usage of resources.

Nirwan Ansari et al. (2013) proposed a method in which clusters formed by organizing nodes, is known cluster based certificate revocation scheme. Blacklist and Warning list are maintained by nodes to revoke their certificates and certification authority issues revoked by this scheme. Certification Authority (CA) is accused of neighbor the node if node acts maliciously and the nodes are placed in the blacklist. To confirm that blacklisted nodes are malicious or not this scheme uses CA for sending accusations to CH. The certificate of malicious nodes revoked when

confirmed by CH. When the confirmation by CH that it is not confirmed then nodes recovered from the malicious list and sends to the waiting list. The nodes are taken part in certificate revocations that are on the warned list for improving reliability and enhancing accuracy. This scheme has high communication overhead.

Noman Mohammed et al. (2011) proposed a method; here the reputation is formed by each node where incentives are provided. For election process, nodes encourage for participating honestly using incentives. For any node, truth-telling is a dominant strategy that each node computes reputation using VCG mechanism.

Chen G et al. (2002) proposed an algorithm for constructing k-hop clustering scheme. The neighboring nodes, which are present in the network, process flooding request message which used for starting clustering. Each node knows K-hop neighbors. For becoming CH, it creates a cluster by broadcasting the decision message using k-hop neighbors that has lowest ID among them. Increase in resource consumption and cluster head occasionally occurs by bottleneck problem.

Ya Xu et al. (2003) designed an algorithm named as Enhanced Cluster based Energy Conservation (ECEC). Minimum connectivity provided for nodes by using this algorithm and lifetimes of huge networks are increased, and energy conservation is provided. CH is assigned to that node which value of estimation energy is higher in the network. In connection with other clusters, gateway nodes are selected using ECEC algorithm when cluster head selected. It provides extensive network lifetime and low power consumption. The main drawback of this scheme is for selecting CHs and gateways use high overhead.

- **MANET Attacks**

Muhammed Saleem Khan et al. (2017) proposed an approach for analyzing packet loss using fine-grained in MANET. The network parameters such as forwarding node queue, MAC layer information, and node mobility are admitted to

packet loss in MANET. For isolating the malicious nodes, this paper proposes a trust-based security model based on the fine-grained analysis. FGA scheme increases the data rate, node degree, and node speed regarding detection rate, false positive rate, and packet loss rate.

Lawal Bello et al. (2017) designed a model using mobility adaptation for computational power conservation technique in MANET. Here, the power model is added with existing on-demand ad-hoc routing protocols that used this method. The mobile nodes evaluate the power status is the unique feature of this technique that decides if they fit for forwarding and reception of the packet.

Hicham Amraoui et al. (2017) suggested a survey and challenges faced by MANET and mechanism of security and cooperation. IDSs and point detection mechanism are two security solutions noticed in this research. Also, different kinds of attacks are analyzed with this method. Network performances are improved by this cooperative solution for detecting non-cooperative behaviors.

Mohammed B. M. Kamel et al. (2017) proposed a model to mitigate Blackhole attack using a secure and trust-based approach on AODV based mobile ad-hoc networks. The routing protocol security of AODV is improved by using STAODV method. Depends upon previous information gathered by the network it isolates the malicious nodes. Each participating node attached with a trust level for detecting its level of trust. Blackhole attack is prevented by examining each incoming packet.

Danista Khan and Mah zaib Jamil (2017) reviewed the Blackhole attack detection and preventing in MANET. This attack performs the closest path and indicates to the node itself. The routing protocol exploited and absorbed all data packets of the network by the node. The performance becomes degraded after this process occurs in the network. Various techniques were discussed for preventing Blackhole attack.

Swapnil Bhagat et al. (2017) proposed an algorithm based on generic request/ reply for detection of Blackhole attack in the mobile ad-hoc network. Mutual trust between nodes is needed for data transmission and interdependent for communication. By injecting malicious node in the network, different kinds of attacks are performed. This proposed approach improves time and performance.

Deny J et al. (2017) proposed a cooperative bait detection approach for protection against the malicious node. Here, Collaborative Bait Detection Scheme is used to detect vindictive hubs that affect gray hole community oriented Blackhole assaults. CBDS arranges the proactive distinguish proof in the beginning stride and touchy response at those subsequent strides.

Vijayakumaran C and Adiline Macriga T (2017) proposed a method for detecting misbehaving nodes in MANET using an integrated game theoretical approach. The relay packets of other nodes used for the payoff that gained by selfish nodes. Then, punished and gradually isolated the reluctant nodes from the network. For maximizing the bonus value, the relay packets are cooperating with other nodes. Optimal probability is provided based on incentive mechanism using its multi-stage rating game to maximize the payoff for working players, and timely delivery packets are ensured for the destination.

Jhum Swain et al. (2017) proposed a study regarding routing issues in MANET and analyzed it. The improved methods are compared is studied, and extent of the work with various parameters are examined. Also, the network performance parameters are packet delivery ratio, power consumption, and average delay.

Afroze Ansari and Mohammed Abdul Waheed (2017) presented a method of preventing and detecting flooding attack based on a cross-layer link quality assessment in MANET. Signal properties are analyzed the MAC layer of the nodes and cross-layer of MAC interface used to incorporate the features into the routing

table. Through the cross-layer MAC/Network interface, the MAC is communicated when the node is marked with flooding node and blacklisted in the routing table.

Jyoti Prabha Singh et al. (2017) proposed a technique for MANET's multipath approach to prevent riddance and hindrance of Grayhole attack. Due to vulnerabilities of AODV routing protocols, severe threat occurs in MANET. Eliminating the gray hole attack have been implemented with this multipath approach.

Schweitzer N et al. (2017) designed an approach using fictitious nodes for reducing the denial of service attacks in optimized link state routing (OLSR). This scheme used the reverse technique or same tactics as attacker used for isolating the victim from the network. The attack itself returned against the attacker for protecting the nodes and preventing exploitation of knowledge about the network.

Kannhavong Bounpadith et al. (2007) explained about link spoofing, colluding attack, flooding attack, black hole attack, and prevention form these attacks in mobile ad-hoc networks. Routing operations are disturbed by sending fake messages or links from malicious party to non-neighboring nodes using the link-spoofing attack. Denial of Service (DoS) attack is a form Flooding, in which destination node gets a large number of requests from malicious nodes in a short period, these connections cannot be completed and not a genuine offer. Black hole attack sends fake information to malicious nodes for routing which claims it is an optimum route.

Ebinger P and Bucher T (2006) analyzed mobile ad-hoc network attacks and designed a generic attack by tree-based model. Also, it examined how to launch attacks like warm-hole, black hole, Sybil and rushing in AODV using their method. They are not able to gather any real-time or simulation-based results by performing and analyzing semi-formal modeling method.

Ning P and Sun K (2005) proposed a method using AODV for studying insider attacks against MANET. Two-dimensional systematic analysis schemes are composed

by using this approach. The routing messages misused by inside attacker, which is a set of possible atomic misuse actions. Ones routing message is an indivisible manipulation by each atomic misuse action. A collection of misuse goals wants to achieve by using insider attack is the second dimension handled by this approach. Through attacker and other nodes, the number of packets is sent for the evaluation criteria which performed by simulations.

- **Authentication Management in MANET**

Salman et al. (2017) compared the tactical issues and commercial purposes of MANET. The deployment of communication platforms and type of transceivers are considered to be essential for tactical space for military applications. The specific environment characteristics and unique attributes of MTNs are discussed and have a significant impact on the adoption of mobile ad-hoc networks for military use.

Rajesh Babu M and Usha G (2016) proposed an approach for detection and isolation of Blackhole attack using a novel Honeypot technique in mobile ad-hoc networks. For detecting malicious nodes, a fake RREQ packet is broadcasted. The invalid Destination Sequence Number (DSN) is contained by a spoofed packet that is a maximum number of all nodes. For reducing the overhead the live value to time is set to 1. Therefore, this fake packet sent to the network and check which node responds to it and results in that node to be malicious attacker. Then, all other nodes in the network get the address of the attacker node, which broadcasted by this Honeypot technique and blacklists it from routing tables.

Hongmei Deng et al. (2004) proposed a method for wireless ad-hoc networks using identity-based key management and authentication based on self-organized MANET. Because of fully distributed nature of the protocol, high computational complexity is required for distributed key management and authentication approach.

Bin Lu et al. (2006) proposed a protocol for the mobile ad-hoc network known as the lightweight authentication protocol. It is based on a one-way hash chain.

Ngai C. H et al. (2004) proposed cluster and trust-based authentication services for mobile ad-hoc networks. Trust relationships are made by monitoring behavior of nodes when intrusion detection component is equipped.

Tomasz Ciszkowski and Zbigniew Kotulski (2006) propose a method based reputation using anonymous authentication protocol in MANET. Tunnels are created between receiver and sender at the cost of storage by providing robust security by this approach.

Nachiketh R. Potlapally et al. (2006) proposed a technique concerning various cryptographic methods for a tradeoff between battery power and security protocols.

- **Sink-Hole Attacks**

Mohammaed Yasin N et al. (2017) proposed a method for preventing sinkhole attack using anomaly detection scheme in wireless sensor networks. The DDMS ides is used for dealing the attacks separately. By its effective design, multiple server attacks can be handled using this DDMS.

Chris H et al. (2005) proposed an approach for analyzing sinkhole problem in the context of DSR using two sinkhole detection indicators for MANET. First, Sequence number discontinuity and secondly Route add ratio. If the node is not seen the packet already, then it processes an RREQ for limiting the number of RREQs communication, and route record of the packet does not have its address. From each node, the overall average difference between the last and current sequence number is used for measuring sequence number discontinuity also proportion of duplicate sequence numbers are observed for the penalty. The route overriding effect caused by the attacker that uses a sequence number, which is not high is a drawback of this

indicator. The proportion of routes to the total number of routes added to particular traverse node to the nodes routing table is known as the route-add ratio. The routes are added to the network using nodes to pass through the sinkhole is caused by sinkhole attack. The calculation of route-add ratio is implemented each time when source route is found. Before intrusion alert issued by the system, the values of two variables must be higher than corresponding value.

Marchang N. and Datta R. (2008) proposed a collaborative technique for mobile ad-hoc networks. By using this method, nodes are used as monitor node. Also, for detecting malicious node, this monitor node is responsible, and nodes voting do it. After receiving votes from the nodes, the malicious nodes detach by monitor node from mobile ad-hoc networks. After a fair bit of power consumed by monitor node, it fails that caused by this approach.

Gisung Kim et al. (2010) presented a cooperative technique that uses three types of packets. Firstly, Sinkhole Alarm Packet (SAP) and the second one is Sinkhole Detection Packet (SDP), and third, Sinkhole Node Packet (SNP). The sequence number of bogus RREQ, current sequence number, and sinkhole route are present in SAP within the node itself. Network id, RREQ sequence number, and standard path contained in SDP itself.

Woochul Shim et al. (2010) suggested a cluster analysis technique. In which, false RREQs are separated from regular RREQs also indicators are verified for detection. There may more than two groups of healthy and false RREQs, so for this reason, this approach is used. Differences among cluster are examined by this cluster analysis that requires measurement of distance.

Krontiris I et al. (2008) specified launching of sinkhole attack in Multi-Hop LQI and Mint Route protocol. For wireless sensor networks, these experiments are conducted.

Nguyen H. L. and Nguyen U. T (2008) performed attacks using study of simulation-based on mesh-based multicast in mobile ad-hoc networks. They implemented black hole attack, rushing attack, jellyfish attack and neighbor attack on ODMRP routing protocol.

Abdelshafy M and King P. S (2013) analyze security perspective on AODV. Selfish, Blackhole, Flooding and Gray hole are four attacks implemented on AODV protocol. Four parameters of the lens are used to observe the impact of attacks mentioned above. These parameters are the end-to-end delay, routing discovery, network throughput and routing overhead. As compared with Gray hole and Selfish attacks, the impact of Flooding and Blackhole attacks are severe on network performance.

Patel D. N et al. (2014) presented a survey on the comparison of performance on AODV, AOMDV, DSR, AODV-UU and DYMO protocols. They established the working performance in some specific cases that works well. The assumption about the properties of the network, the suggestion of their work has some drawbacks. Also, improvement in scalability and traffic overhead control are discussed in AODV, DSR, AOMDV, and DYMO.

Table 2.1 Comparisons of Different Attacks in MANET

Attacks	Type of Attack	Techniques used for Prevention
Wormhole Attack	Active	SAW DAW, HMTI, Packet Leases, DELPHI
Sybil Attack	Active	Robust and light weight detection technique
Black Hole Attack	Active	SADOV
Denial of Service (DoS)	Active	LMAC and Evasion
Misrouting Attack	Active	Watchdog Mechanism
Eavesdropping	Passive	SSL
Traffic Analysis	Passive	Transmission Schedules