CHAPTER 1

INTRODUCTION

Development of technology is a keen interest for the researchers who work with new ideas and became a significant source to compete with mobile ad-hoc networks (MANET). The idea behind this technology is to take over spontaneous order into the network topologies, which has either a base station or having a fixed supporting structure. Without the fixed communication network infrastructure or human involvement, the MANETs could communicate with other mobile nodes by using wireless radio links. Many applications rose from this MANET technology, which mainly consists of Data Networks, Device Networks, Wireless Sensor Networks and Tactical Networks. Mobile ad hoc networks are a kind of technique which can develop themselves and are highly active through each node, that leads to this methodology which given way for security problems. The security problem happens due to the arrangement of networks by its own and absence of infrastructure, which the nodes present in the mobile ad-hoc networks acting as both a router as well as a host.

Figure 1.1 shows the basic structure of MANET, where each device is connected using the wireless network. Extending the cooperation between forwarding of data packets and exchanging of routing information is the primary motivation expected by the mobile devices. After deploying the mobile devices in a strategic environment, it compromises, or it is vulnerable to malicious attacks in every possible way.

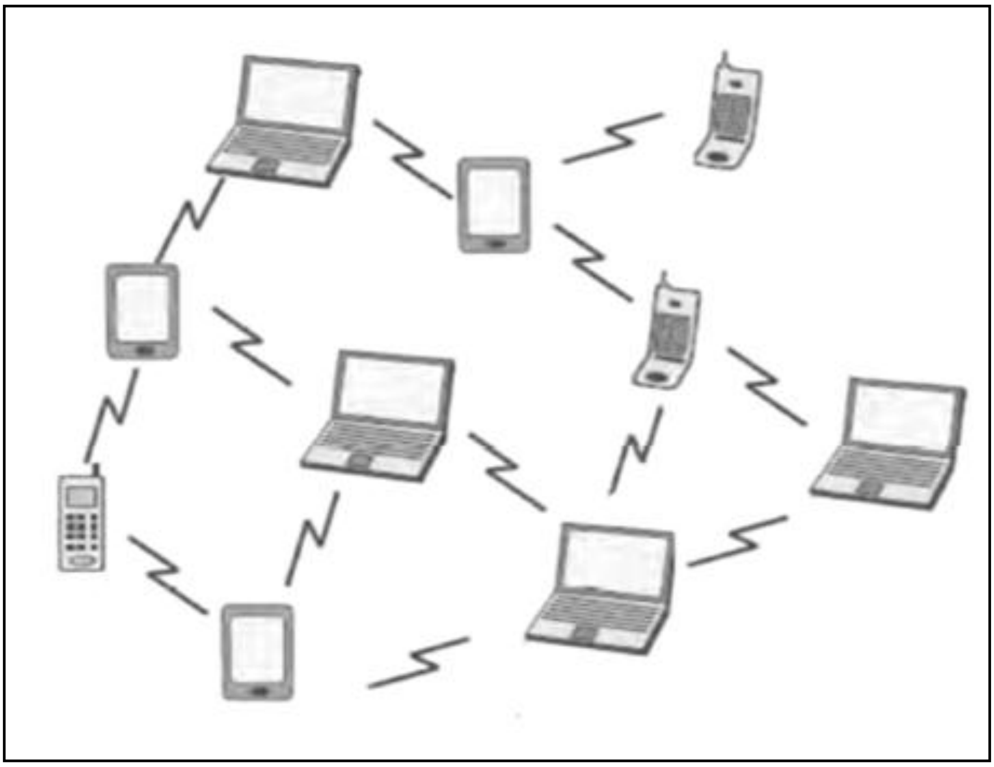


Figure 1.1 Architecture of Mobile Ad-hoc Networks

The whole network could be corrupted as the node behave vulnerably and disrupt even it seems to be permissible. So far, in all functional aspects, it is needful for each neighboring node should be a monitor for any suspicious activities. It is due to multiple attacks which can be organized at the same time by this kind of malicious nodes, and a trust metric is needed every time to monitor the feature of that particular node. A new technique called Trust metric, which is a mechanism to judge every node in the network by analyzing their information gathered is worth and about its integrity in the participation of data forwarding etc.

1.1 MANET Routing Protocols

The message packets, which sent from, source to the destination over a network using some set of rules called as routing protocols. According to network conditions, the mobile ad-hoc network obtains different kinds of routing protocols. Figure1.2 shows types of MANET protocols.

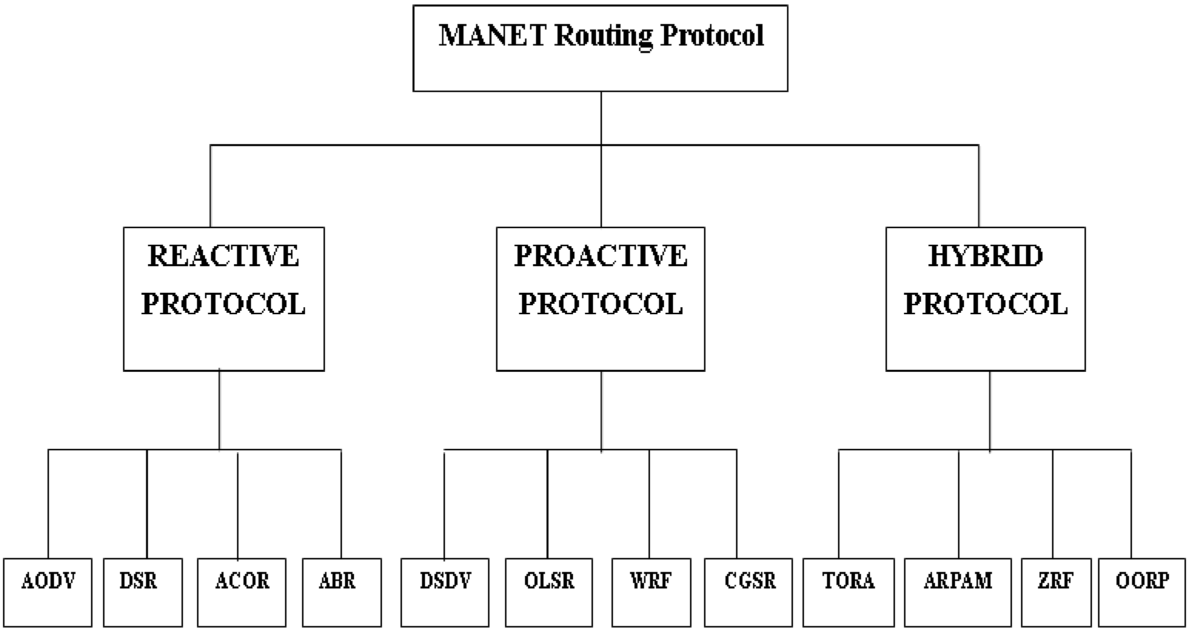


Figure 1.2 Types of MANET Routing Protocols

From Figure1.2, the different kinds of routing protocols in the mobile ad-hoc network shown, and it mainly consists of Reactive, Proactive and Hybrid protocol. Lakshit Prashar and Raj Kamal Kapur (2016) are given each of its example methods to work with MANETs. The Reactive protocols have several examples like Ad-hoc on demand distance vector (AODV), Dynamic source routing (DSR), Admission control enabled on-demand routing (ACOR) and Associatively-based routing (ABR).

Proactive routing protocol consists of four types of examples like Destination sequenced distance vector routing (DSDV), Optimized link state routing (OLSR), WRF protocol and Cluster switch gateway routing (CGSR). And some examples of hybrid protocols are Temporally Ordered routing algorithm (TORA), Ad-hoc *routing protocol* for Aeronautical mobile ad-hoc networks (ARPAM), Zone routing protocol (ZRP) and OORP.

1.1.1 Reactive Routing Protocols

On-demand routing protocols are the other name for this Reactive protocol. Nodes by on-demand basis initiate the route discovery whenever it is needed, and discovered by this protocol method. The route discovery procedure started when the source node is unable to obtain the route cache for getting the connection between the source and destination nodes. The two components of this protocol to process the method these are:

- Route Discovery
- Route Maintenance

- **Route Discovery**

Here this component mainly focuses on the path, when the sender does not know the destination route, then a Route request message is sent. The node, which received the signal from the source, will reply with Route Reply Packet (RREP) and obtain a link for connection to the destination node. After establishing the route, the data are sending through the particular path from source to destination.

- **Route Maintenance**

New links are formed in the network as well as it can also get broken due to its dynamic nature. Therefore, the transmission between two nodes will become a failure if the route link broke. For handling this kind of situation, route maintenance is needful, and it is the only mechanism to overcome this problem.

1.1.2 Proactive Routing Protocols

This controlling protocol is known as table-driven protocols that without having the information about the network topology, each node consists of the routing table to find the destination node. Because of power consumption and substantial signaling traffic, this kind of feature is useful for one-way traffic.

Whenever the network topology changes, every node updates the routing table from time to time. Unfortunately, for maintaining the routing table for each node, the proactive protocol becomes a drawback for large networks, which contain lots of information about the routes. By varying from protocol to protocol, it will preserve routing tables consistently.

1.1.3 Hybrid Routing Protocols

Here, the proactive and reactive routing protocols are combines to form a hybrid method. The concept behind this hybridization of two protocols is to decrease the latency caused by the route discovery in reactive routing and reduce the control overhead of proactive routing protocols. Some examples of hybrid routing protocols are ZRP and TORA etc. Figure 1.3 shows the hybrid routing procedure.

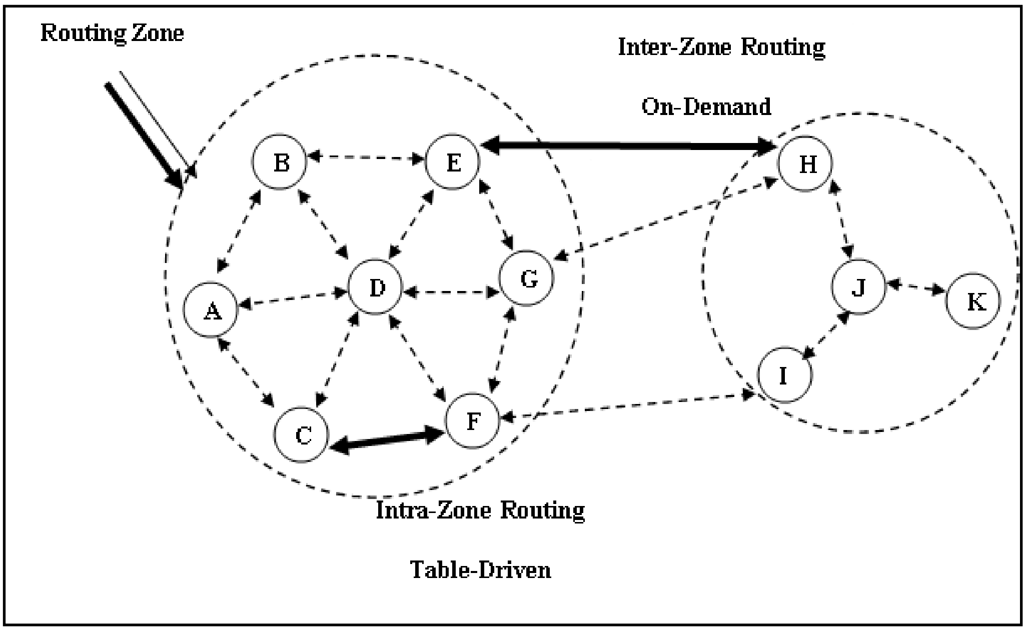


Figure 1.3 Hybrid Routing Protocol

1.2 Security Goals of MANET

Mobile ad-hoc network consists of some security goals that defined as shown in figure 1.4.

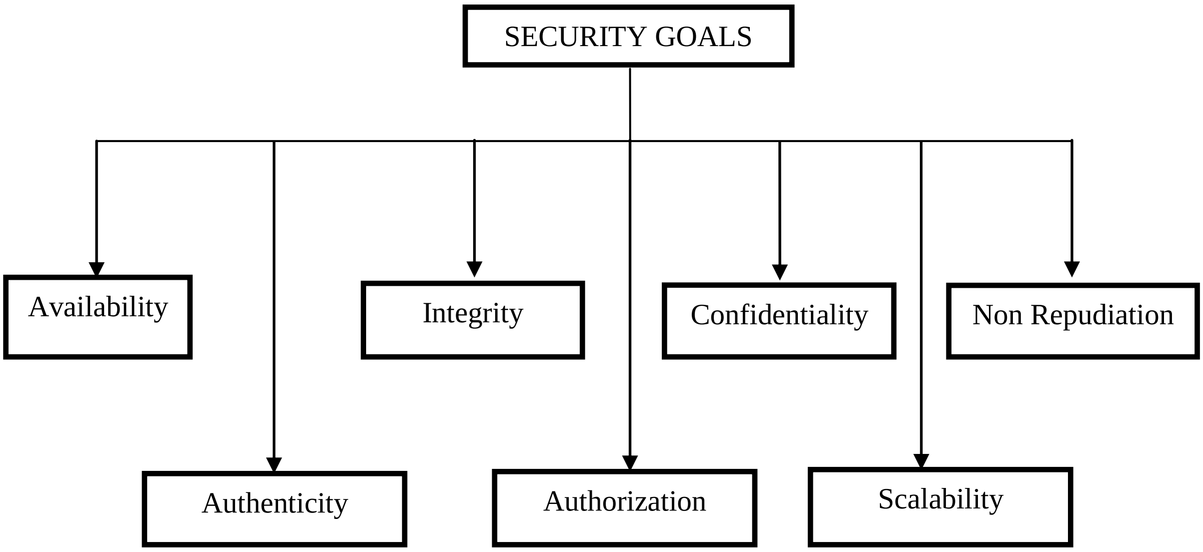


Figure 1.4 Security Goals of Mobile Ad-hoc Networks

- **Availability**

The appropriate times are open to approving the gatherings with benefits. Administration and information, which both applied from the accessibility. In any case, the administration assault refused even when system administration is guaranteed to survive.

- **Confidentiality**

By approved gatherings, the related resources of the computer guaranteed to be getting. The access from any individual for anything can be finished to get it. The private data kept with mystery from other information, which nobody can get the benefit of accessing it with a secret.

- **Integrity**

By approved gatherings, which altered the benefits, which implies trustworthiness. Erasing, making, evolving status and composing are incorporate by changes. Therefore, it is guaranteeing that the message exchanged is trustworthy, which never defiled.

- **Authentication**

The personality of associate hub guarantees by another corresponding hub, which empowers it with confirmation. The members in the correspondence are confirming to certify which are not impersonators, which known as validation.

- **Authorization**

The diverse sorts of clients relegate the property of various access rights. System overseer is helped to perform a system administration as an instance.

1.3 Attacks in MANET

The known fact is that MANETs does not have any central authority to control the network, it consists of only mobile nodes. For this reason, security is a significant problem, which initially not incorporated with routing protocols and assumed it does not fit. The data could be damaged due to vulnerable attacks, as routing protocols of MANETs are open and not secured. Mobile nodes can be easily prone to attacks in the network.

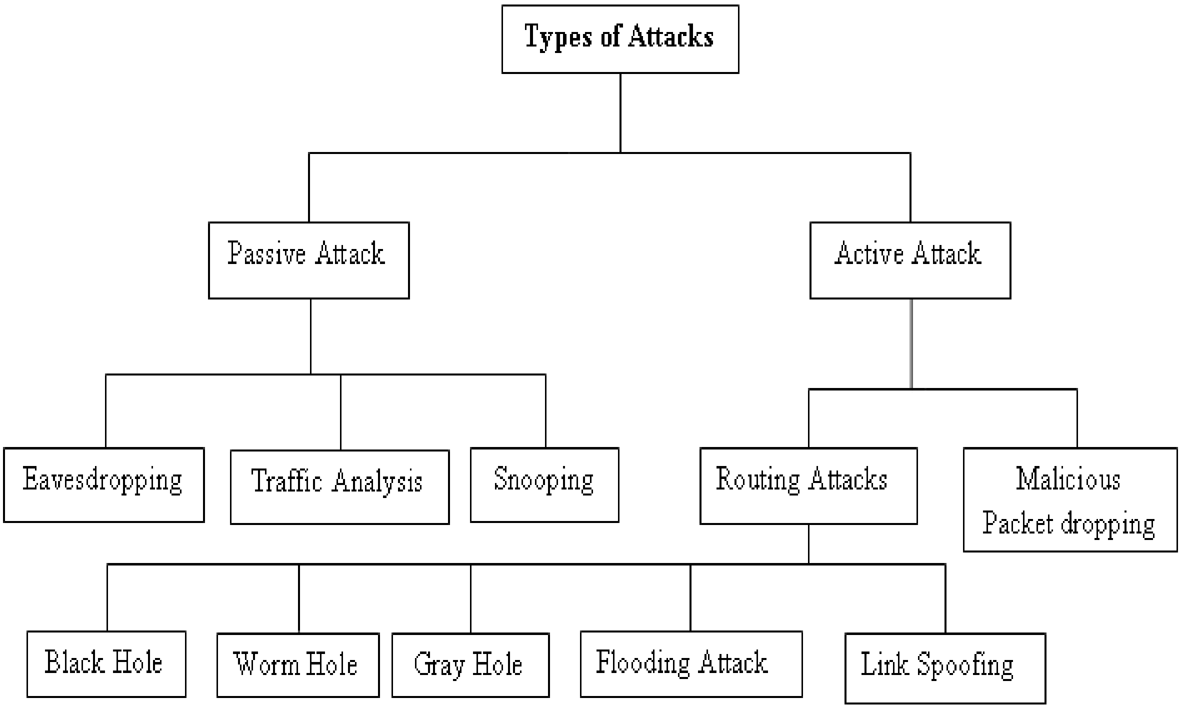


Figure 1.5 Types of Attacks in MANET

The attacks mainly classified into two categories as shown in Figure1.5. First one is Passive attack and second is an Active attack, and each of them has its classification of offenses as shown in figure1.5.

1.3.1 Passive Attack

Normal operations in the network are not affecting by this kind of passive attacks. It is a kind of attack, which snooping the data when exchanging from source to destination in a network without changing any information in the data. Here the secret messages can steal easily. During the operation over a network, we are not aware that our information been stolen; due to this reason, the passive attack cannot quickly detect. It overcomes by using the powerful encryption technique which during the transmission of data, the messages that encrypted. Passive attack is classified into three categories these are,

- **Eavesdropping**

It is one kind of passive attack, which acts as a node in a network, and its work is to observe merely the messages or confidential information passed between two nodes. This malicious node helps to retrieve the data later, which gathered from the network. Using this eavesdropper, lots of secret information like passwords, private key and public key and the location could take from them.

- **Traffic Analysis**

In mobile ad-hoc networks, competitors gave importance for both traffic pattern as well as data packets. For example, by analyzing the traffic patterns, we can derive network topologies important information. From the topology, we can gather valuable data by using traffic analysis, and it can act as an active attack, which is possible of eliminating nodes and motivate to be self-organization in the network.

- **Snooping**

It is another type of passive attack, which can access the third person's data or information without having any permission or access to it. During the transmission of data, it is not necessary to limit the gaining access, and it is similar to eavesdropping. This technique almost used for viewing the e-mail of someone is from his or her computer screen and observes the typing when the users are writing from their monitor. Moreover, some software programs which used for snooping, which they can access remotely from network or computer devices activity, by using observing their monitor.

The snooping techniques which are commonly used by the crackers who are known as malicious hackers for monitoring login information, keystrokes, viewing passwords and obstruct the email and data transmissions. Nowadays, many organizations and corporate companies use this kind of technique to monitor the workers and staffs to track the usage of internet and business computers. The general definition of snooping referred to a utility or a software program, which performs the function of monitoring.

1.3.2 Model of Active and Passive Attack

Figure 1.6 shows the active and passive attack in mobile ad-hoc networks. The attacker is given for each MANET and observed the possible attacks and seen the difference between the passive and active attacks.

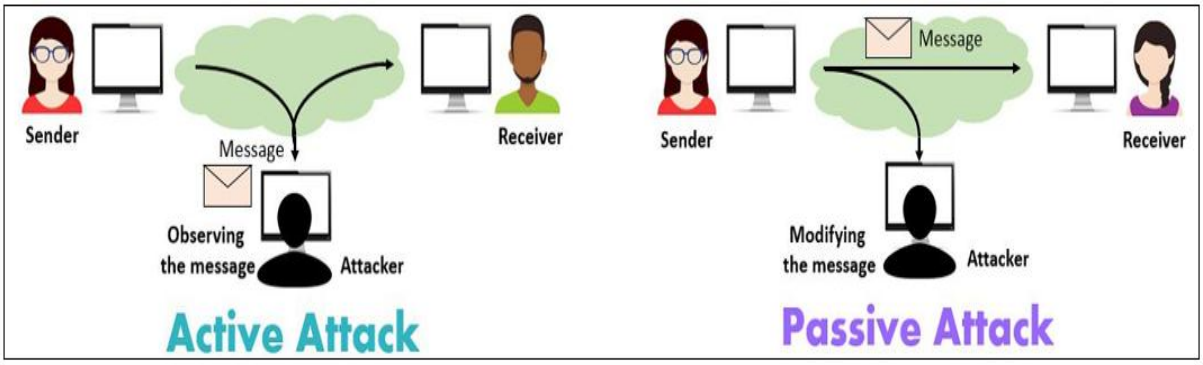


Figure 1.6 Active Attack and Passive Attack in MANET

1.3.3 Active Attacks

The central concept behind this attack is to alter or modify the data which is transmitting or exchanged over the network. This disturbs the functioning of the network and stops the transmission of data. This active attack obtains different features of the network to initiate the attack also it modifies the data packets, drops it or injects the packets. This kind of attacks is very vulnerable and most dangerous. Active attacks classified as Routing attacks and Malicious packet dropping.

- **Link Spoofing**

This method of attack indicates that it interrupts the routing operations by advertising some fake links by the malicious node which is not a neighboring node. Take OLSR protocol as an example, here it target the two hop neighbors and the attacker send some fake links to them. After posting this kind of attack to that particular node, it becomes a victim and selects that malicious node which it thinks as its MPR. Late, this attacker gathers information or modify the routing traffic and perform Denial of Service attack.

- **Flooding Attack**

Network resources like bandwidth, computational and battery power are drained by the attacker also to consume the resources of each node and humiliate the network performance by interfering the operations over routing. This process is known as flooding attack. It classified into two types based upon the types of packets used for flood and shown in figure 1.7.

(i) RREQ Flooding

(ii) Data Flooding

(iii) Syn Flooding

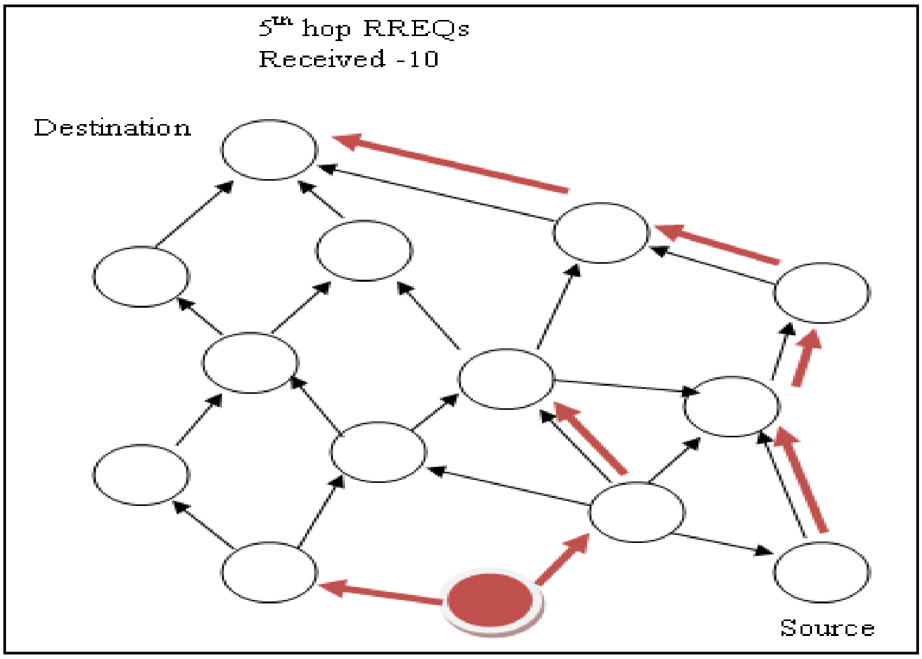


Figure 1.7 Example of Flooding Attack

(i) **RREQ** – In this attack, it will send many packets of RREQ for the particular IP of the network which does not exist. A parameter named as RREQ_ratelimti which is deactivated by the intruders for attempting the RREQ attack. The effects of performing this kind of attack consume the nodes battery power, network bandwidth, and the rightful user cannot use this network for authentic communication. Figure 1.8 shows the route request in AODV.

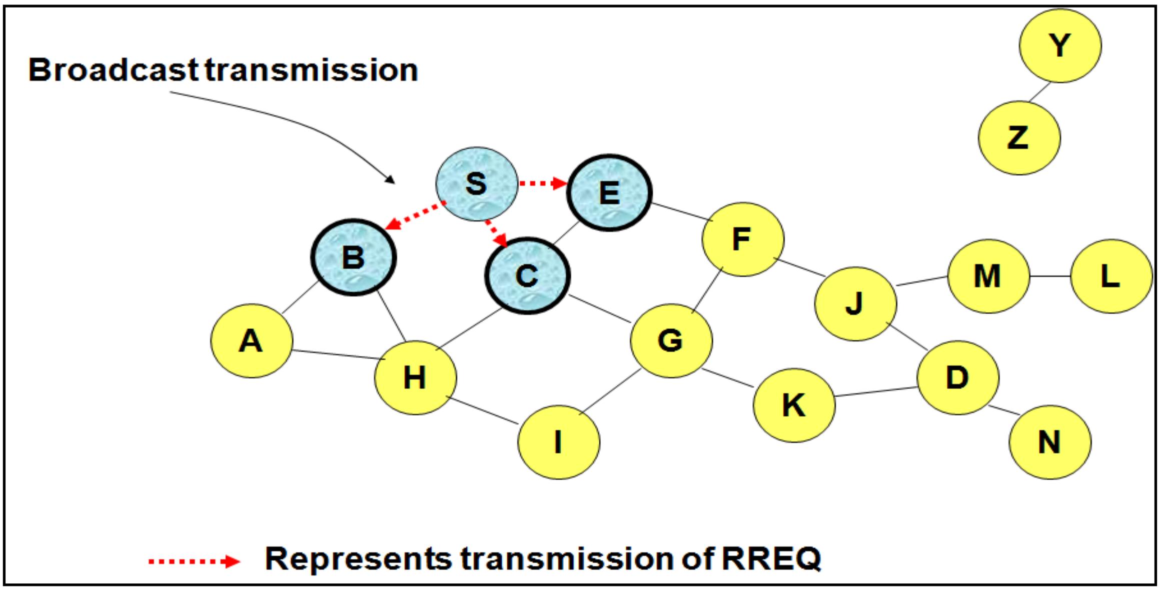


Figure 1.8 Route Requests in AODV

(ii) **Data Flooding** – Its primary target is to consume all the network resources by first creating a malicious node and then it will create a new path to every node and then sending unwanted or bogus data packets in a considerable amount. The effects caused by this attacks are exhausting the resources of networks and very difficult to detect such kind of attack. Figure 1.9 shows the attack from source to destination.

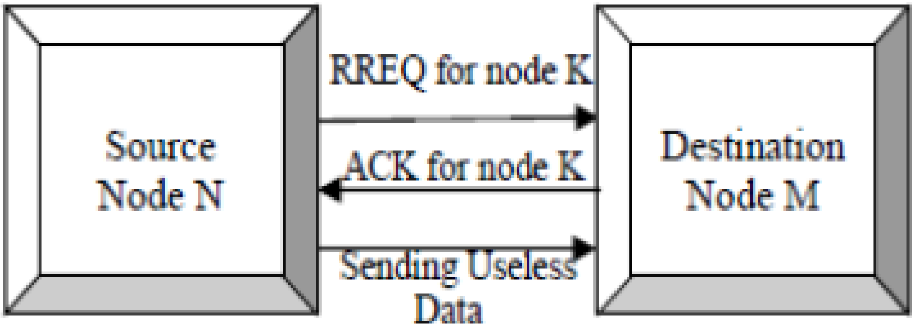


Figure 1.9 Data Flooding Attack

(iii) **SYN Flooding** – Here synchronization packet is sent to the destination node by the flooder or attacker which consumes a massive amount of memory when this attack occurs. Figure1.10 shows the concept of syn flooding.

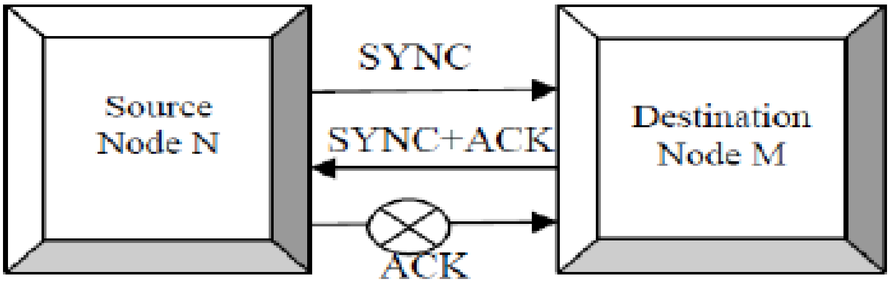


Figure1.10 Synchronization Flooding Attack

- **Black Hole**

Vaishali Gaikwad and Lata Ragha (2015) explained about the attacker that creates its malicious node which advertises the false route by replying to the route request node sending false information about the path to the destination and make use of routing protocol and admit of having the shortest route to the particular destination. After processing this attack, the victim node starts sending information or data through that black hole node and become as an active route to the victim. Figure 1.11 shows the cooperative black hole attack.

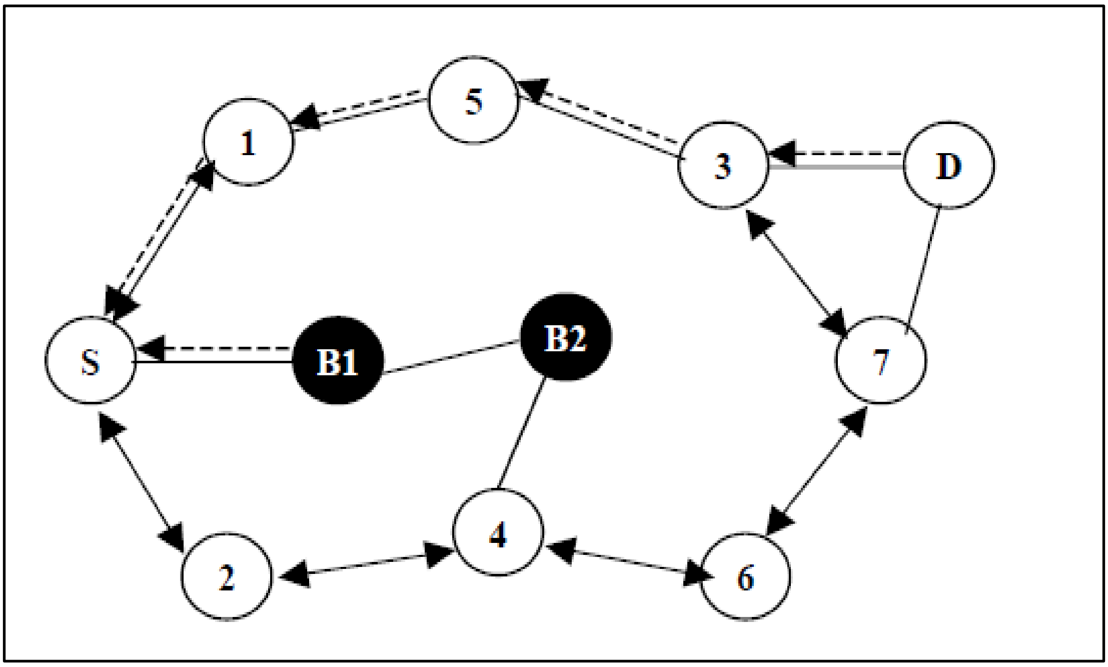


Figure 1.11 Cooperative Black Hole Attack

- **Worm Hole**

The recorded packets of one location are tunneled by the attacker from one site to another. The secret understanding of two attackers who created the tunnel is known as a wormhole. The attackers tunneled the routing control messages which interrupt the routing in a network. On-demand routing protocol could prevent the attack used by the wormhole attacker from finding any routes. Figure1.12 shows the initial demonstration of attack proposed by a wormhole.

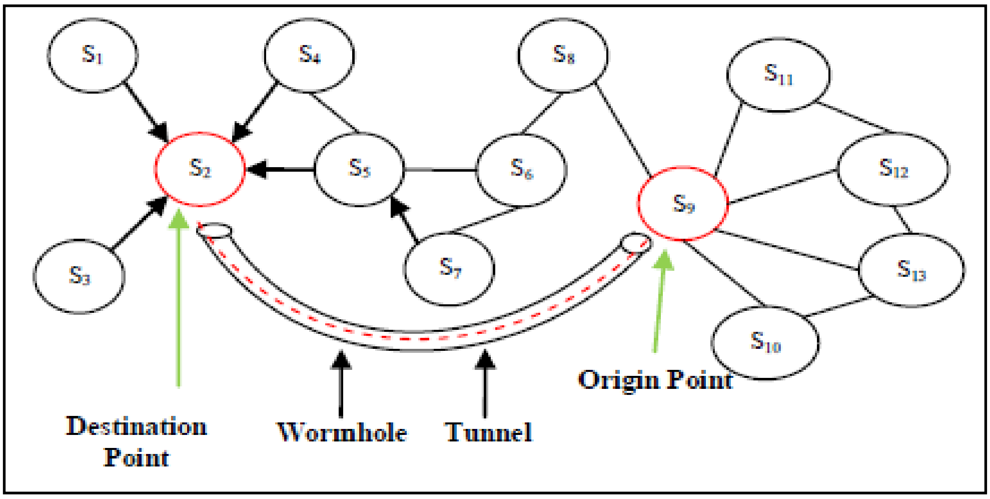


Figure 1.12 Wormhole Attack Demonstration

- **Gray Hole**

This attack leads to messages to drop out from the node by misbehaving of the route in the network. Two phases are available during this attack, the first phase of attack implies to the destination node that it has a valid way and in the second phase, using a specific probability it drops intercepted packets from the nodes. Figure 1.13 shows the gray hole attack.

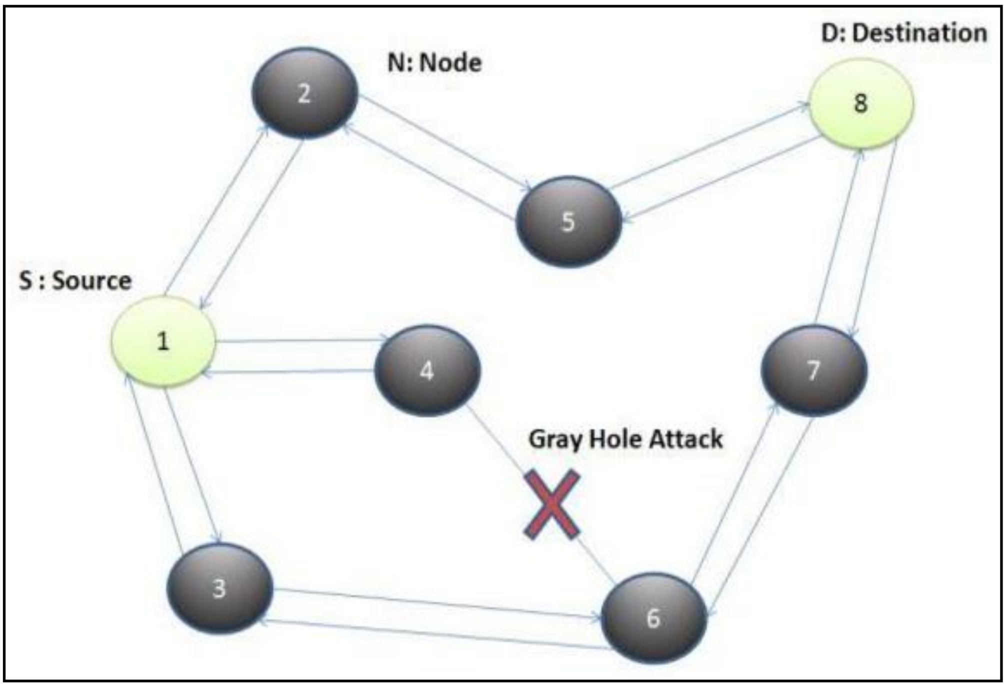


Figure 1.13 Gray-hole Attack

- **Malicious Packet Dropping**

This attack mainly applied to the user application and operating systems of a computer by using malicious attacks like Worms, Spywares, Viruses and Trojan horses.

1.4 Key Management Schemes

Mobile ad-hoc networks are having many security problems due to the infrastructure it made off. Which overcome by using a key management scheme, which is high for security purposes. Energy constraints like dynamic topology, variable capacity links, and limited physical security made the critical task to MANET for managing and usage of keys for security. Depends upon the applications speed of the mobile ad-hoc networks vary. Such example for this kind of situation is military application speed is low whereas commercial rate is high. The unique feature helps MANET to work in standalone intranet and connect with large networks.

Methods like the public key, group key, symmetric key and hybrid key are the different kinds of cryptographic keys used for encryption. These referred to symmetric and asymmetric key management. The sender and receiver use same keys, which later is used for encrypting the data as well as for decrypting, known as symmetric key management. Here, k number of keys required to n number of nodes to communicate with mobile ad-hoc networks. Then, the formula defined as $n(n-1)/2$.

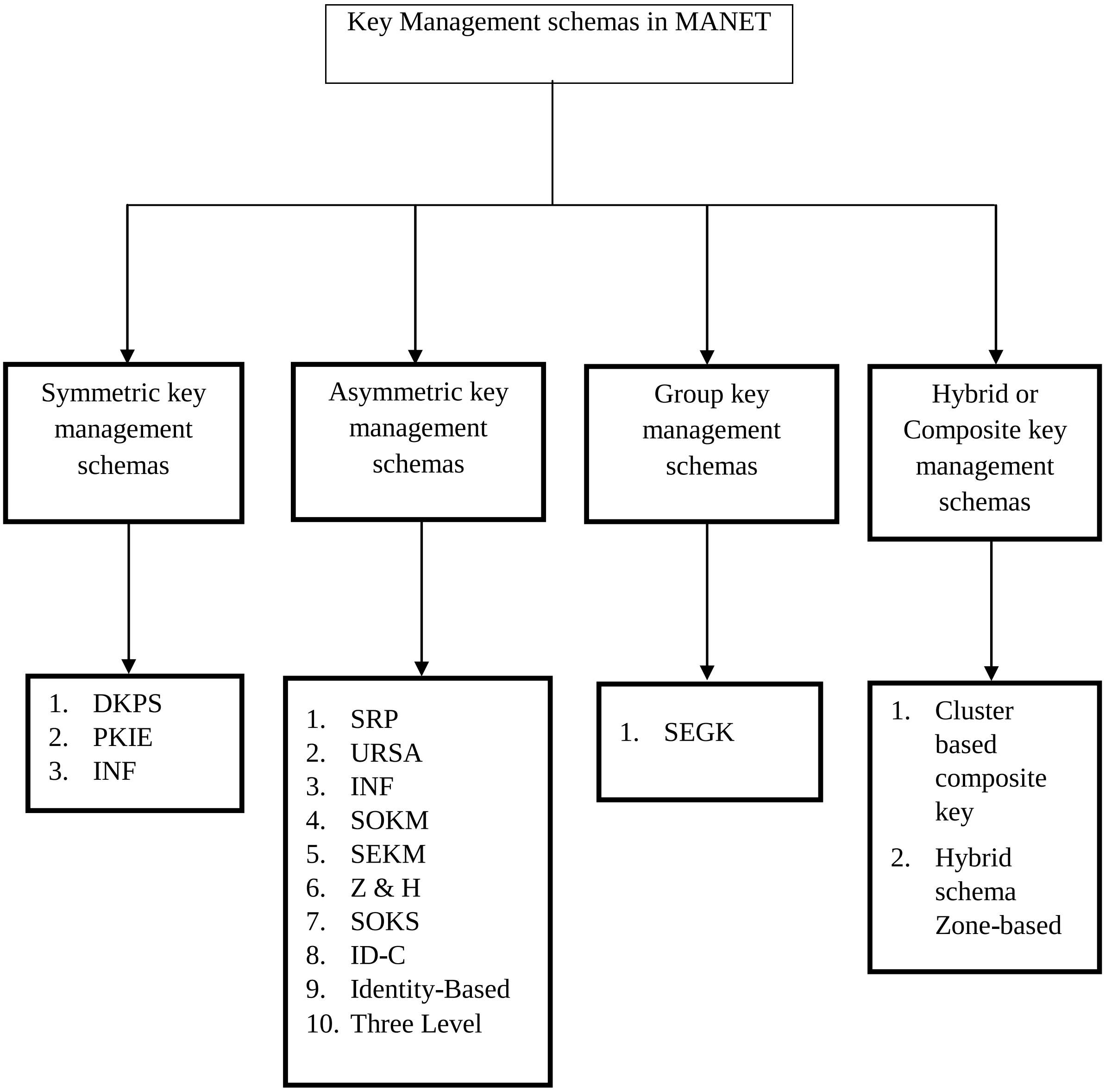

Key Management schemas in MANET
Symmetric key management schemas
Asymmetric key management schemas
Group key management schemas
Hybrid or Composite key management schemas
1. DKPS
2. PKIE
3. INF
1. SRP
2. URSA
3. INF
4. SOKM
5. SEKM
6. Z & H
7. SOKS
8. ID-C
9. Identity-Based
10. Three Level
1. SEGK
1. Cluster based composite key
2. Hybrid schema Zone-based

Figure 1.14 Key Management Schemes in MANET

The public and private are two keys used in public key cryptography method, where, public key defined for encryption and private key for decryption. The individual source node has the private key, which used for decryption and the destination nodes have public key used for encryption. A new pair of private and public keys created for every communication. Like symmetric key cryptography, this scheme needs keys lesser. For more extended messages, the symmetric key scheme used and for short messages, asymmetric keys are used. Mobile nodes, which form as the group use a single key that assigned by group key cryptography technique. For group members, secretly a key is generated and distributed by group key scheme.

Networking system has essential security services when initialization occurs in the network for the users. These are installation, generation, distribution, revocation, control, storage, destruction, backup, bootstrapping, archival and maintenance of trust in keys. Figure 1.14 shows different types of schemes for key management in mobile ad-hoc networks.

1.4.1 MANET Schemes for Symmetric Key Management

- **DKPS**

The acronym for DKPS is Distributed Key Pre-Distribution Scheme. Three critical phases used in this technique. First, Distributed Key Selection (DKS), Using exclusion property, this stage generates a random key for each node from the universal set. Cover Free Family (CFF), in this concept, the exclusion property evaluated and a probabilistic method used to make it in a distributed manner. MANET could be dynamic by using this technique as it removes Trusted Third Party (TTP). The second phase is Secure Shared-key Discovery (SSD), a shared key generated for each node. SSD uses the insignificant method. This method evaluated even if it is not providing security while DKS phase can be eavesdropping. The last stage consists of Key Exclusion Property Testing (KEPT). For constructing a matrix, binary values used which is a relationship between shared keys and mobile nodes keys. CFFs exclusion properties used for testing the KEPT phase, whether it fulfills the mobile nodes. As compared to group key management, the DKPS scheme is more efficient and minor storage than crucial pair-wise management.

- **PIKE**

For establishing shared keys, the sensor nodes are used in his scheme. For a set of nodes, Peer intermediaries for key establishment (PIKE) scheme use unique secret keys with pre-distribution of the concept of random key. Mobile nodes O(n) splits unique secret key into horizontal and vertical dimensions in a 2D case which extended to 3D. At least one or more intermediaries of common secret key shared from every pair of nodes in MANET. Fair scalability and good security services are essential features of this model.

- **INF**

This model defined as Key Infection, for making key establishment process this scheme equally participates by every node. Due to trust component of a node, a collaborative effort not needed for INF method. Symmetric key broadcasted by this system. Key Infection consists low encryption, low cost, and operation but security services are weak in this system. Mobile nodes have late entry problem, which has excellent scalability.

1.4.2 Asymmetric Key Management

- **SRP**

This Secure Routing Protocol method acts as a dealer which as administrator authority and three nodes in it. Mobile nodes have given original certificates by the dealers. The nodes classified into; Firstly, Client nodes act as a normal user and which wanted by MANET. Secondly, Server node concept is to request a certificate from one node to other and by storing the certificates and responsible for generating partial certificates. Third, it makes valid certificate from the combination of partial certificates known as Combiner Node.

- **URSA**

The encrypted local communication feature helps this method to be more reliable and efficient availability. This technique has RSA certificate signing keys broadcast by all nodes by using threshold scheme efficiently. Ubiquitous and Robust Access Control periodically updates the certificate of mobile node present in MANET. The nodes in mobile ad-hoc network distribute the CA functionality.

- **Mobile Certificate Authority (MOCA)**

The computational power of each node has high which secured physically, and MOCA nodes have heterogeneity basis in asymmetric key management scheme. From MANET, the nodes of mobile certificate authority nodes selected randomly when equally equipped. The subset of MOCA nodes will decentralize by this scheme and distributes the services of CA. The crucial task of mobile CA in a network is to find a safe path.

- **SOKM**

The acronym of this scheme is Self-Organized Key Management. This method has one updated and non-updated repositories of the certificate, which used locally. Each node maintains repositories of the non-updated certificate by calculating best graph. The public key certificate generated by mobile nodes to other node and act as own authority. The key authentication process is done by using public key chain certificate. The bootstrapping process not needed flexibility configuration in self-organized key management. The certificate path uses web-of-trust relationship, not suitable and not connected strongly to ad-hoc networks.

- **Secure and Efficient Key Management (SEKM)**

This method provides a safe procedure, secret shareholders coordination, detailed and efficient by having single decentralization scheme. Server group uses mesh structure; this team used connection by having partial system private key with all servers consistent. The periodic beacons of SEKM share updates, group by providing, and maintain certificate services and relationship and high cost. Figure 1.15 shows the SEKM method.

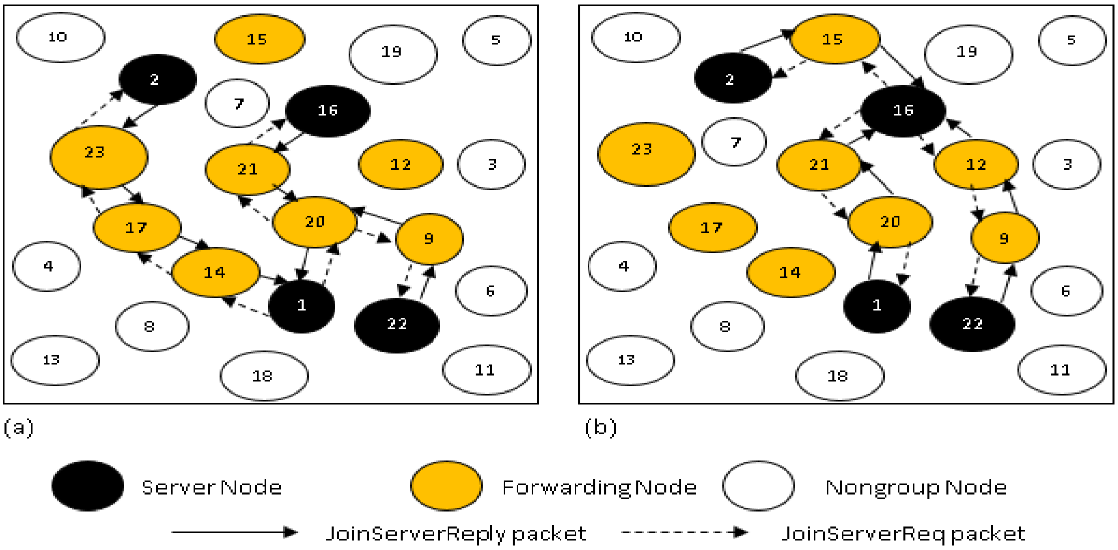


Figure 1.15 Working of SEKM

- **Partially Distributed Threshold CA scheme (Z&H)**

In 1999, Zhou and Hass discovered this scheme for partial distribution. The concept of CA distribution commonly used, when mobile ad-hoc network construction by threshold fashioning. This asymmetric key management scheme has excellent intrusion tolerance, trust management of CA and offline authentication as security service. The MANET accepts the key produced by this model and threshold CA that partially distributed.

- **Self-Organized Key Scheme (SOKS)**

Distinct CA used by each node in a self-organizing network. This scheme has offline authentication and intrusion detection in limited service but low in resource efficiency and scalability. Storage cost is higher in SOKS that also encrypt operation, which has high intermediates.

- **Key Distribution Technique (ID-C)**

Identity-based scheme generates threshold private key for initializing or creating a set of nodes in MANET and accepted by the network, which self-organized. The same security services like SOKS provided with full efficiency. Great resources efficiency of Id Revocation list offers scalability. The encryption, intermediates, operation, and storage cost have a medium in this scheme.

- **Identity-Based Key Asymmetric Management Scheme**

It consists of four phases; trusted key generation center needed for verifying user identity of the node and producing a private key. Figure1.16 shows four characters of this scheme, which defined as initialization Phase (I), Registration Phase (R), Verification Phase (V) and Key Exchange Phase (K).

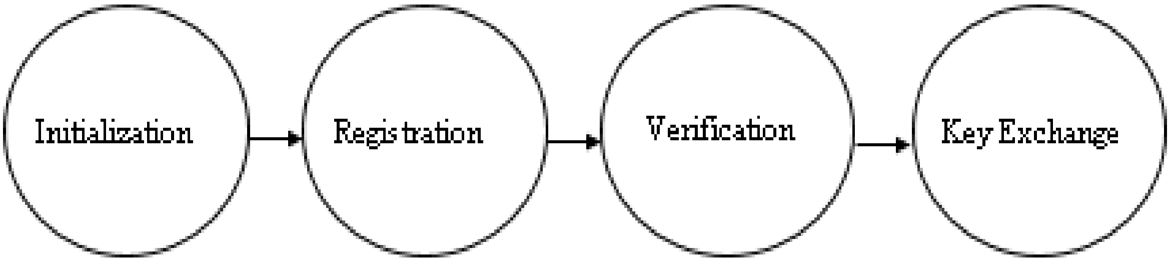


Figure 1.16 Identity-Based Key Management

MANET network prevent the man in a middle attack, replay attack, and brute force attack by providing authenticity at end-to-end. In this network, the public key not needed to produce by the mobile nodes also for broadcasting.

- **Three Level Key Management Scheme**

Wan AnXiong proposed this scheme with highly efficient and secure for MANET networks. The three-level described, ID-Based Cryptography used in the first level with threshold sharing. Bilinear Pairing Computation is second; third, Elliptic Curve Cryptography (ECC) provides security level high and small key to mobile nodes. Secret sharing algorithm threshold (t, n) attacks security services even if adversaries prevent them. RSA equal strength of 160 bits and 1024 bits key provide security in enhanced level. Overhead with reduced communication and computational cost is less for confidentiality and authentication provided by pairing technology.

1.4.3 Group Key Management Scheme

- **SEGK**

Yuhong, Jie Wu, and Bing Wu proposed this Simple and Efficient Group Key Management scheme. For increasing the efficiency in MANET, two multicast tree constructed and maintained by the coordinator. By using underlying tree links, the group coordinator applies computation to all members and distributes keying materials. Then, it ensures all group members maintain protocol and form a reliable multicast tree. This condition defined by computation cost, which directs proportional to no. of mobile nodes by following some situations;

Total no. of Neighbors < Predefined Threshold value, the grey color is chosen for the node. If probability = 0.5, then three colors Red or blue is chosen.

Frequent update for group key processed to ensure forward and backward security. Two essential detection methods used for Simple and Efficient Group Key Management scheme, these are Tree links and Periodic Flooding of Control Messages.

1.4.4 Hybrid or Composite Management Scheme

- **CBCKM**

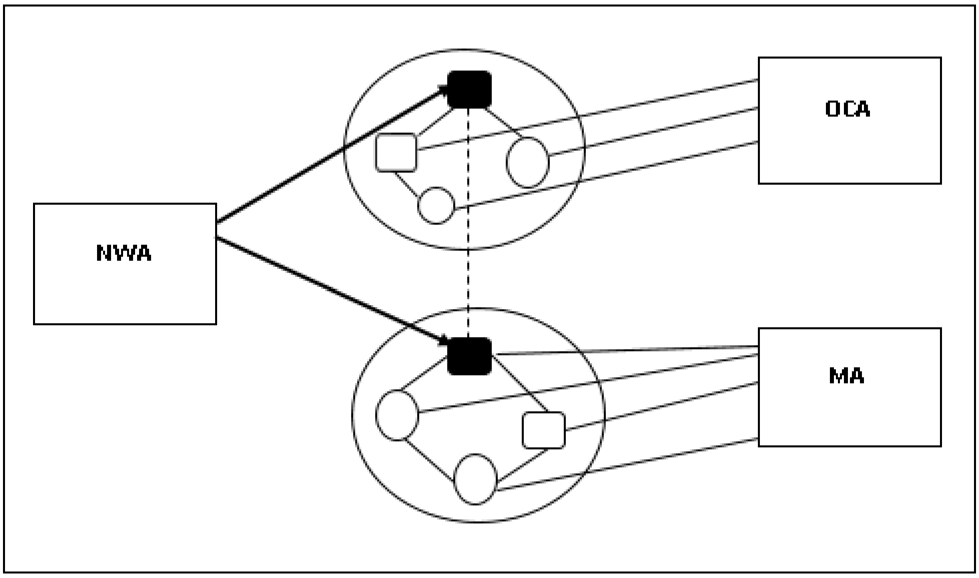


Figure 1.17 Overview of CBCKM in MANET

The acronym for this scheme is Cluster-Based Composite Key Management (CBCKM). In 2010, Vincent Antony and Pushpa Lakshmi proposed this method for mobile ad-hoc networks. Hierarchical clustering, mobile agent, partial distribution and off-line CA are features of this technique. PKI storage problem reduced by cluster head which maintained by the public key of members. PKG services and node revocation present in MANET which provided by mobile agents. Figure 1.17 shows the overview of CBCKM.

The public key of cluster head computed based on old public key and current trust value. The easy way to process essential renewal and key number is by using timestamp method. This model saves storage space and network bandwidth.

- **Zone-Based Key Management Scheme**

This scheme in MANET can use the zone routing protocol method. In 2012, Abdullah Aref and Thair Khdour proposed this model, where each mobile node defined by zone. Depends upon hops distance, each mobile node allocated a pre-defined number. Inside zone radius, the mobile node uses symmetric key management. For inter-zone security, the key management used by the clustering of mobile nodes that without depending on it. Certificates made without losing capability when making an efficient public key.

1.5 Cluster Techniques in MANET

It is an efficient way of routing technique for data transfer between the nodes in the network. By using its hierarchical network environment, it can provide stability and overall scalability is improved in the network. In clustering based mobile ad-hoc networks, the small groups divided from the entire network that named as clusters.

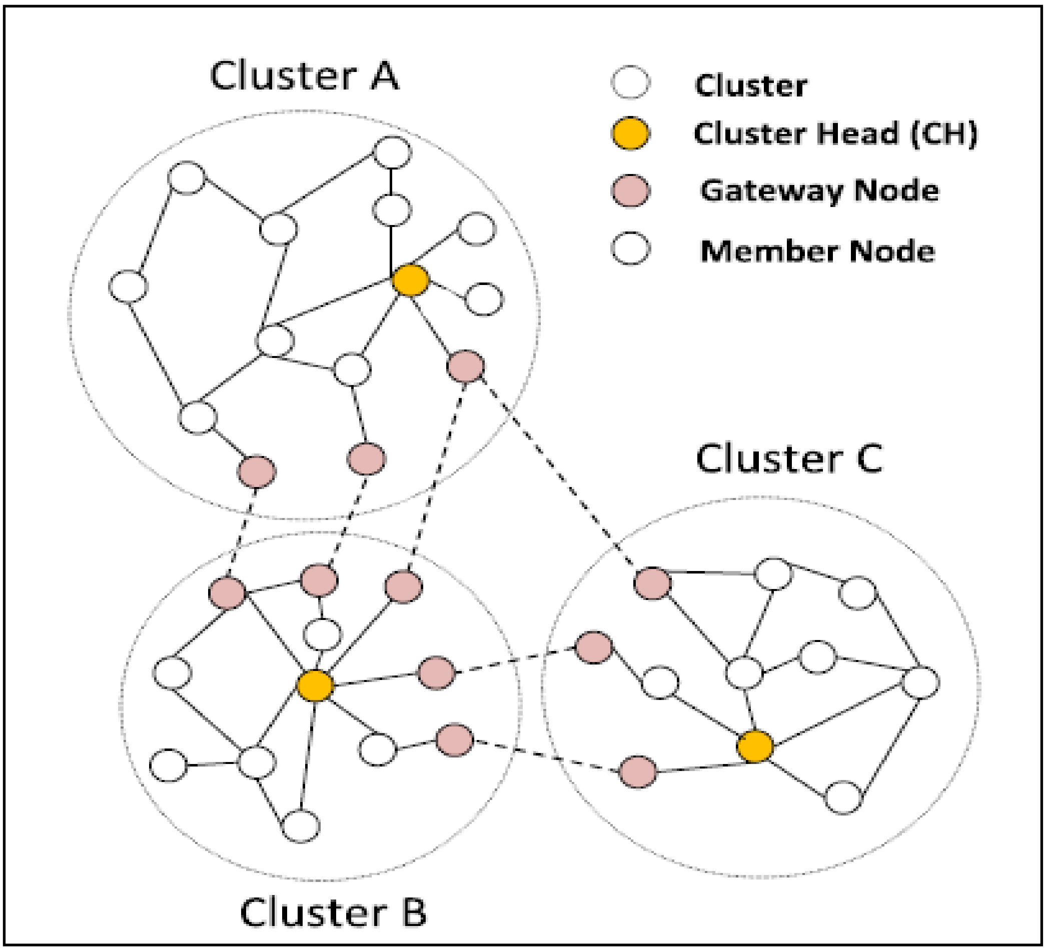


Figure 1.18 Clustering in Mobile Ad-hoc Networks

This cluster consists of gateway nodes, cluster head (CH) and member nodes as shown in figure 1.18. This mechanism of cluster design includes two stages, i.e., cluster management stage and cluster formation stage. Cluster formation takes CH selection place. The clusters overall performance is controlled by CH and among the member nodes elected from the group. For managing the cluster, CH is responsible and can access all the member nodes efficiently. For all clustering algorithms, the primary task is a selection of CH, and at the time of electing CH, the candidate could be any cluster member. And it performs cluster organization task. Cluster management stage controls the re-election procedure of CH, and communications are expertly managed between nodes.

Intra-cluster communication defined as communication between the nodes of the same cluster. Through gateway nodes, the transmission of one cluster node with other cluster nodes is called inter-cluster communication. Among the groups, the discussions managed by gateway nodes between each cluster. The main challenges of clustering algorithms in MANETs are network topology management, optimal CH selection and network performance improvement in the presence of mobility along energy consumption is minimized at every node. In every category of clustering scheme, the CH selection criteria are unique. Based on the weight value of node the decision regarding CH selection among all nodes takes place. The combined amount of node energy and node degree, relative speed of a node are used for calculating the weight value of each node. The calculation of the minimum weighted value of a node used for electing a CH utilizing a formula mentioned in. The main drawbacks of this method are transmission delay and some overheads that performance degraded for the network.

The nodes energy level value is used for taking a selection of CH. The node has the highest possibility of becoming CH if it has high value. Unfortunately, this method needs some other cluster management phase to complete it that cause load in the network, increase delay and results of affecting the efficiency of the overall network. Based on the neighborhood nodes number, every node assigned a unique identifier (ID). The lowest ID is attached to the node that has the most significant amount of neighbor nodes. Two entries are consisting when each node creates neighbor node table. First is the type of the neighbor node and ID of the neighbor node. Within one hop distance, each node broadcasts Hello messages. The information given by hello signals is ID, the total number of neighbor nodes and smallest ID. The nodes ID are compared with smallest ID when receiving the hello message. CH is declared itself by a node with smallest ID. The scalability improved by this scheme and ensures better cluster transmission range, but the control messages between nodes are exchanged more when selecting CH. Then nodes energy level, degree and neighborhood benchmark are considered for electing CH and for managing topological changes in the network. These schemes improve Quality of

Service (QoS), scalability and stability of the system and it is suitable for small-scale mobile ad-hoc networks. More energy consumed when using large scale MANETs due to high computational power is needed for computing many parameters at member nodes and CH. Both intra and inter-cluster communication cause end-to-end delay and congestion. There exist some hybrid methods, which is a combination of two or more algorithms for achieving networks stability but sometimes cause more consumption of energy on the member of a cluster as well as on CH with the presence of mobility.

1.6 Certificate Revocation Scheme

This scheme helps to find the attacks in mobile ad-hoc networks. For securing communication in networks, this method plays a vital role as certification procedure undertaken and issued by Certificate Authority (CA). Although it is a digital signature, the attribute bounded with the public key of certification. Forging and tampering in MANET prevented and varied by this scheme. To remove certificates and to enlist on those nodes could be processed by certificate revocation procedure, which attacks causes for neighboring nodes. Due to false acquisition may be produced; for revoking a certificate from a node is difficult for CA.

While making the mechanism of certificate revocation, it should consider for false acquisition. In certification system, the cluster based technique used for managing certificates instead of routing. By using this method, detecting malicious nodes from all nodes is difficult. Instead, we can use in each cluster. Therefore, access to network stops by removing the malicious nodes and revokes the certificate from that node. Thus, it enhances network security. Figure 1.19 shown various types of certification revocation scheme,

From Figure 1.19 shows Certificate Revocation Scheme in MANET. It mainly classified into two categories namely centralized and decentralized system. Cluster-Based revocation scheme comes under the centralized system, and Voting and Non-Voting-Based Mechanism comes under a decentralized system.

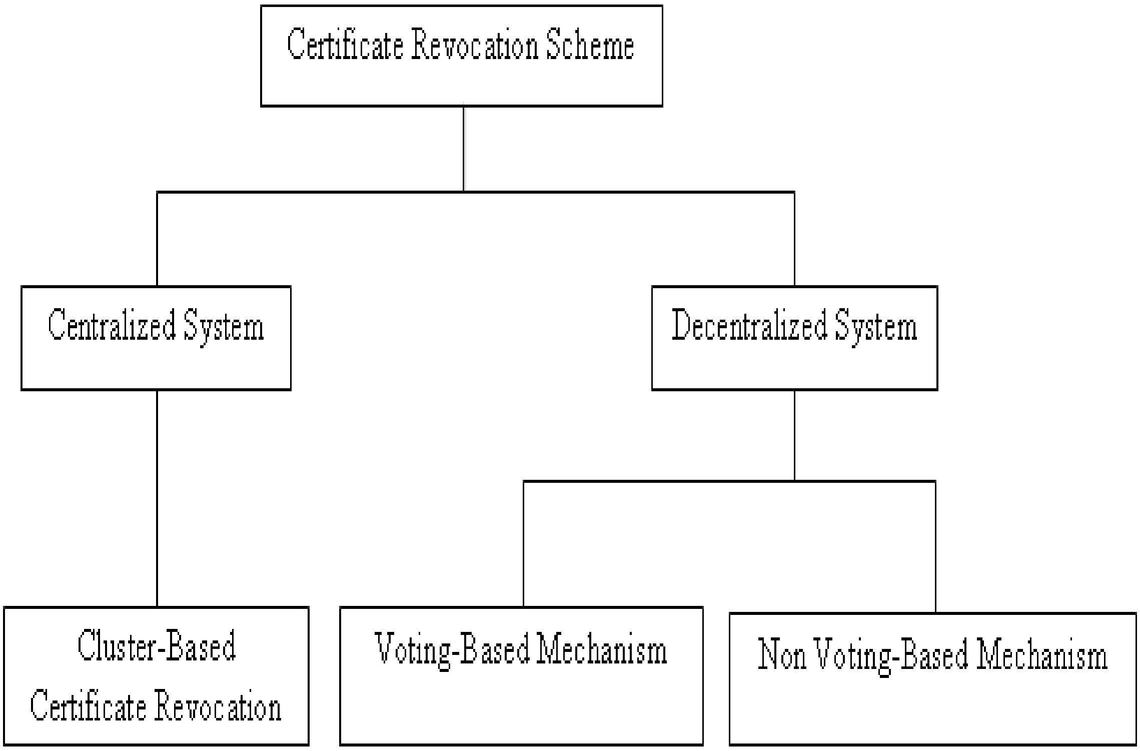

Certificate Revocation Scheme
Centralized System
Decentralized System
Cluster-Based Certificate Revocation
Voting-Based Mechanism
Non Voting-Based Mechanism

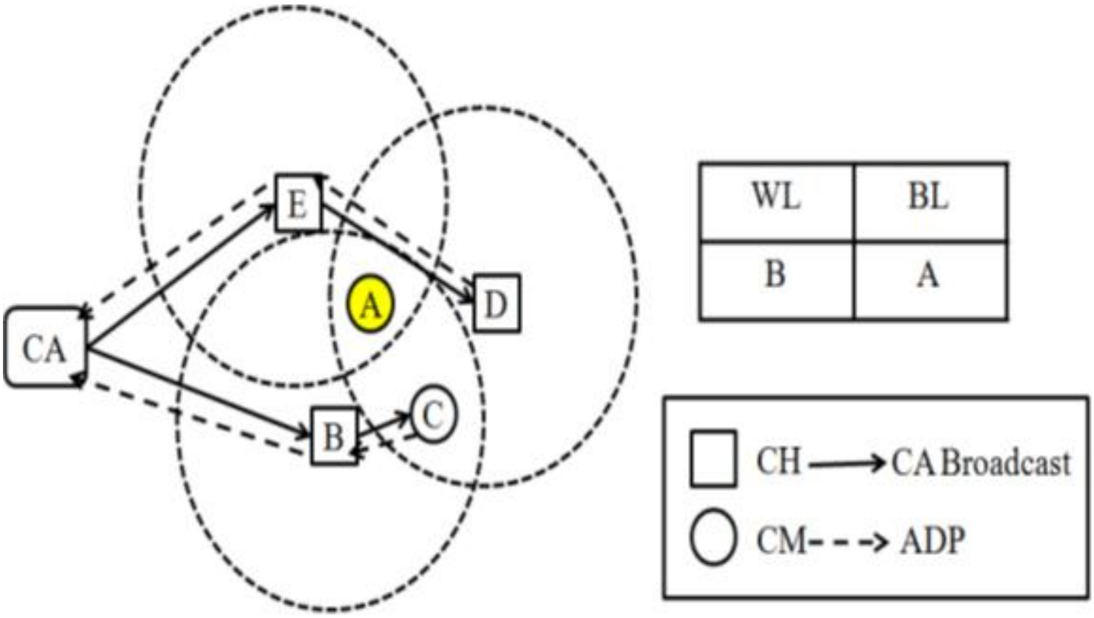
Figure 1.19 MANETs Certificate Revocation Scheme

- **Cluster-Based Certificate Revocation Scheme in MANET**

A large number of nodes contains in the scale of the network, various challenges occur in MANET and identify using clustering methods. Different techniques proposed for clustering-based certificate revocation scheme in MANET. Within the communication range of CH, each cluster consists of a Cluster Head (CH) with Cluster Members (CM). Due to mobility, the changes in topology are by robustness which different groups belong to each CM. For routing, clustering information is not used. It only used for managing certificates. For any routing technology, can used by this scheme.

CH must be legitimate to work with clustering-based certificate revocation. Three categories of nodes are classified. Highly trusted named as normal nodes, questionable trust named as warned nodes and non-trusted named as attacker nodes. Attackers send Attack Detection Packets (ADPs) which accused by normal nodes who allowed for becoming CHs to the CA. Nodes present in Warning List (WL) can communicate and join as CMs without restrictions but cannot accuse attackers and not possible to become CHs. Nodes completely took out from the network if it is considered as an attacker and malicious.

From Figure 1.20 and 1.21 shows the revocation and recovery procedure of certificate present in clustering. Figure1.20 shows, its neighbors B, C, D and E attacked by malicious node defined as A. For accusing Node A, these neighbors send ADPs to the certificate authority after detection of the attack. Firstly, CA puts into WL for citing from neighbor node B and the node A to BL after receiving the attack. Then entire network receives information present in WL and BL.



WL	BL
B	A

Figure 1.20 Certificate Revocation Procedure

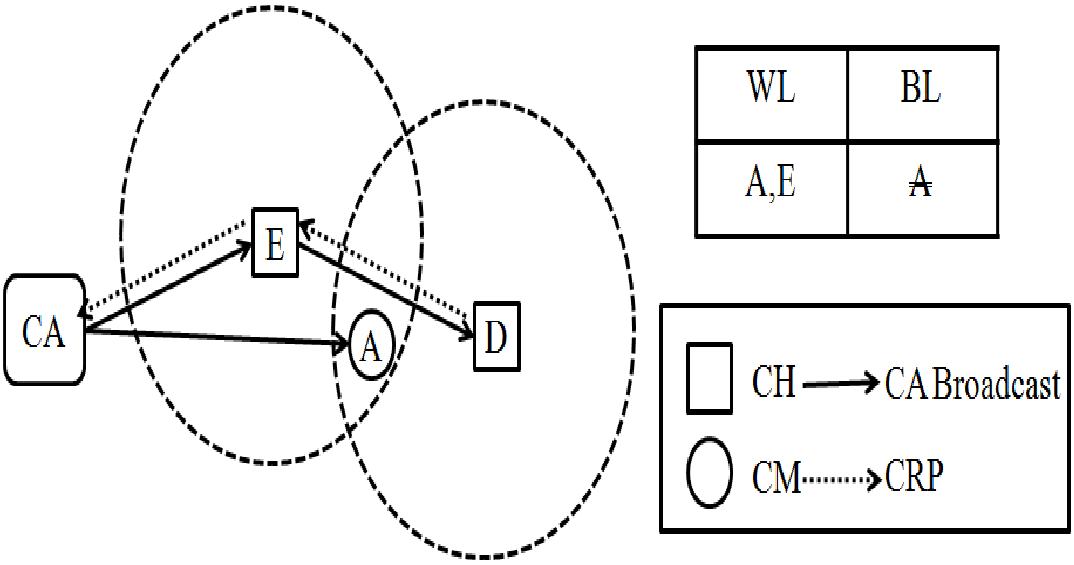


Figure 1.21 Certificate Recovery Procedure

Figure 1.21 shows the procedure of certificate recovery. Node A’s certificate will recover by sending CRP to the CA when nodes E and D have not received any attack from this node and identify as the false acquisition.

- **Voting-Based Mechanism**

Neighboring nodes give votes for detecting malicious node and make certificate revocation using this scheme. By using one-hop monitoring approach, the revoked nodes exchange information to neighboring nodes. The increase in predetermined value is by giving negative votes to the accused node and the certificate revoked. The challenging task of this voting-based scheme is not applicable for finding threshold value. False acquisition problem is not handling by this URSA.

- **Non-Voting-Based Mechanism**

Here, a single node with the valid certificate can give a vote for deciding malicious attacker. A strategy proposed by Clulow named as “suicide for the common good” for this mechanism. One accusation only processed for certificate revocation. An attacker in the network removes by notifying node, which scarifies itself. Due to its suicidal strategy, the communication overhead and the revocation time reduce by this approach. False accusation is not possible, and accuracy degrades by this scheme.

1.7 Need for the Study

This thesis focuses on secure communication over Mobile Adhoc Networks (MANET) and different methods to prevent and detect the attacks.

As MANET does not have infrastructure for communication, the security always faces issues to safeguard the information transmitting from with each other. Therefore, a proper dynamic key management is proposed and designed the technique that could be better understandable for other researchers as well as users. Also, the experiment regarding the unique ID for communication helps in depth analysis for securing information. Secondly, the attacks that faced by MANET can be easily identified and shown the working method of Time Adaptive Enhanced Acknowledgement approach for eliminating the sinkhole attacks. The third scope of study is to isolate the malicious nodes present in networks using ECMS cluster head that is based on Certificate Revocation procedure which helps to understand the nodes activities and dependability of each node and the preferences given to each node.

1.8 Problem Statement

Mobile Adhoc Networks are vulnerable to several attacks due to its disadvantage of not having fixed infrastructure. Therefore, the issues regarding the security aspects of MANET is to be considered and improve for new approaches and develop more techniques to prevent the attacks from external sources and detect the incoming malicious activities. Many risks are available when using the MANET technology like transmission error due to different kinds of attacks and information are stolen for the receiver end, Authorization of accessing the data should be developed with safe and secure manner. Finding a secret communication is always meant to be a main problem that MANET kind of techniques usually faces today.

Challenges in MANET

- The essential characteristics of this wireless communication are time varying in nature. Interference, blockage, fading, and path loss are the transmission obstruction, which acts as a vulnerable behavior of wireless channels. These different aspects are resistant towards the reliability of wireless communication.
- Transmission over the limited range – Compared to the wireless networks the data rates reduced by giving a limited radio band. Due to this reason, the possible overhead kept low to obtain most favorable bandwidth usage when necessary.
- Transmission error leads to packet loss – Factors like hidden terminal experiences higher packet loss in MANETs, which results to wireless channel issues, collisions, and interference and the movement of nodes in the network makes a frequent breakage in the path. Due to the existence of unidirectional links and hidden terminals, which possibly increase collisions in mobile networks?
- Changes in route when mobility occurs – Network topology has an active nature, which results in repeated path breaks. Regular network partitions – The network obtains separation when movement of nodes randomly occurs. This kind of situation affects the in-between nodes.

1.9 Objectives of the Study

- To analyze the MANET work and scope for communication.
- To obtain the reliable information of issues faced by MANET.
- For secret communication, the dynamic key management is obtained for authentication.
- To produce unique IDs for node using UDRPG for secret communication.
- To detect sinkhole attacks occurred in MANET.
- To prevent attacks, the TAEACK is proposed.

- To provide a Certificate Revocation for the nodes in MANET.
- To improve reliable and secure communication, a cluster head certificate revocation is used as ECMS.

1.10 Methodology of the Study

This thesis contains three methodologies to overcome the problems that faced by Mobile Ad-hoc Network (MANET). The first one is to communicate secretly and transmitting information in highly secure manner. So for this, UDRPG technique is used which named to be Unique-Dynamic-Random-Password-Generation for generating unique IDs for nodes and a dynamic authentication key management for secret communication. Secondly, the prevention and detection of sinkhole attacks and malicious nodes in MANET is to be identified for secure communication. The Time Adaptive Enhanced ACK mechanism is used for the prevention of attacks from malicious nodes and detect them. Third, for reliable and secure communication in MANET has to take into account and propose ECMS cluster head Certificate Revocation procedure that is based on Energy (E), Connectivity (C), Mobility (M), and Signal to Noise Ratio (S).

1.11 Limitation of the Study

The limitations of this thesis of proposed work are to improve the dynamic key management system for secret communication of a reliable manner and determination of sinkhole attacks in timelier manner is limited. Even though the efficiency in detection rate, throughput, and energy is up to the expectation, still, the improvement in detection of attacks should be considered more in future study using other algorithms.

1.12 Organization of the Thesis

Chapter 1 gives the overall introduction of the types of key management schemes in mobile ad-hoc networks. Also, described the multiple attacks occurred by the nodes in the network and certificate revocation techniques to process the identity of the nodes. The primary process of this introduction part is to analyze Distributed Key Management System (DPSK), UDRPG method, TAEACK, and ECMS.

Chapter 2 discussed and suggested various literature survey proposed by other techniques and these work shown the existing problems and each reviewed by this process of experiment results. These investigations include drawbacks and motivation for future actions.

Chapter 3 analyzed a proposed approach to our work based on dynamic key management for authentication of nodes to communicate secretly in mobile ad-hoc networks, also present a unique ID to the nodes using UDRPG.

Chapter 4 discussed the attacks from the malicious nodes that mainly concentrate on sinkhole attack in MANET, also, a new method used for detecting and preventing these attacks in the network; Time Adaptive Enhanced ACK mechanism (TAEACK) works fine to find the sinkhole attacks and results discussed in detail.

Chapter 5 discussed based on cluster head–based certificate revocation procedure using ECMS algorithm and finding a reliable and secure communication for mobile ad-hoc networks. Also, various parameters based on this cluster based certificate revocations that presented in detail.

Chapter 6 concluded the proposed methods; performance results and explained in detail by using each proposed scheme. The future work also discussed for further improvement and discussed in this chapter.