CHAPTER 2
LITERATURE REVIEW

CONTENTS

2.1 Introduction .................................................................................................................................................. 32
   2.1.1 Key Management ............................................................................................................................... 33
   2.1.2 Certificate Distribution and Exchange ............................................................................................. 34
   2.1.3 Certificate Revocation ....................................................................................................................... 35
2.2 Existing Key Management Methods ......................................................................................................... 36
   2.2.1 Contributory Methods ....................................................................................................................... 37
   2.2.2 Distributive Methods ......................................................................................................................... 40
2.3 Existing Certificate Distribution and Exchange Methods .............................................................................. 44
   2.3.1 Trust Based Methods ....................................................................................................................... 44
   2.3.2 Non-trust based Methods .................................................................................................................. 48
2.4 Existing Certificate Revocation Methods .................................................................................................... 52
   2.4.1 Voting based Methods ....................................................................................................................... 52
   2.4.2 Trust based Methods ......................................................................................................................... 57
2.5 Classification of existing Key Management & Certificate
   Exchange/Revocation Methods ..................................................................................................................... 60
2.6 Design Considerations of the Thesis ........................................................................................................... 65
2.7 Summary .................................................................................................................................................... 66

2.1 Introduction

Mobile Adhoc Network (MANET) is a self-sorting out network in which the nodes are allowed to move subjectively and arrange themselves [1]. These networks are utilized as a part of uses ranges from large-scale and exceptionally dynamic networks, to little and static networks [2]. Mobile adhoc networks are effortlessly influenced because
of different attacks like active attacks, passive attacks and so on. When the attacker cause jamming, transmit fake routing information or disturb nodes from giving services, it is said to be active attacks. In passive attack, the attacker desires to pick up control access over the network. To minimize the attacks, one should remove the attackers immediately after detecting the first attack. This can be done by using a certification system.

2.1.1 Key Management

The presence of cryptographic keys acts as a proof of trustworthiness. Therefore, a proper key-management service is very much needed to ensure that the nodes are legitimate members of the network and are equipped with the necessary keys whenever needed. Key-management services are generally needed for application layer security and protection of the network layer. Key management schemes for the application layer can assume an already running network service. Schemes for the network layer routing information cannot. Keys are a prerequisite to bootstrap a protected network service. The classification is illustrated in figure 2.1.

The key management schemes are divided into two methods, contributory method and distributive method. In contributory methods, all the nodes participate together to achieve security. Here, there is no trusted third party for key generation and maintenance. In distributive method, a trusted third party will be there, who is the in charge of key generation and transport. We can ensure security by using certificate based and ID based approach. Different trust management mechanisms can be incorporated together with the certificate exchange for improving the security of the key management scheme.
2.1.2 Certificate Distribution and Exchange

During transmission, each node in the adhoc network produces a public/private key pair. As the node creates this key pair by its own, the node must authenticate with a few individuals in the network before joining and accessing the network resources. This authentication is performed by certificate exchange.

The certificates are produced by any outside resources, for example, server or Certificate Authority (CA). Certificate Authority (CA) is a trusted outsider in charge of issuing and revoking certificates [43]. CA signs a valid certificate digitally for every node. In the certificate exchange system, the nodes authenticate themselves with the individuals before they join and begin accessing the network resources [60]. In self organized environment, the certificate distribution and exchange plays a major role for ensuring availability and security.
2.1.3 Certificate Revocation

Among confidentiality, integrity, authenticity, availability and non-reputability [5], authenticity is the primary issue in MANET. Certificate Revocation is the commonly used authentication mechanisms. When the malicious behavior is detected, the certification of the attacker must be revoked [42]. Certificate revocation invalidates the certificates of the attacker for maintaining the network secured [43]. Here, the nodes are classified into normal nodes, which are exceedingly trusted, warned nodes with faulty trust, and attacker nodes, which can't be trusted. The CA keeps hint of Black List (BL) and a Warning List (WL). At the point when CA gets an Attack Detection Packets (ADP) from an accuser, the accused node is considered as an attacker and enrolled in BL [53].

The certificate revocation strategy has a few difficulties that are discussed as follows. At the point when a node is assigned with more than one key share, redundancy issue might happen in the network. Certificate lifetimes are typically measured in years. Here, a little revocation rate might lead to considerable records and can't scale well [56]. Attacks are brought on because of the nonattendance of secure limits in mobile adhoc network. Because of this, MANET experiences every all weather attack.

A cluster based certificate revocation scheme has limitation in certificate accusation and recovery mechanism where the number of nodes fit for charging malicious nodes diminishes after some time so that malicious nodes can never again be revoked in an auspicious way. Subsequently, these mechanisms are overviewed to design a system for improving the viability and proficiency of the scheme by utilizing a threshold based way to deal with restore a node's accusation capacity and to guarantee adequate typical nodes to accuse malicious nodes in MANETs [43].
This chapter makes a survey of various certificate exchange and revocation mechanisms. In the following sections, we have classified the key management methods into two types, namely, contributory and distributive methods, the certificate revocation mechanisms into two categories, namely voting-based mechanism and trust-based mechanism, and certificate distribution and exchange into trust-based and non-trust based methods. In section 2.5, the advantages and disadvantages are examined to compare the existing mechanisms in key management, certificate exchange and revocation. Finally, section 2.6 gives the summary of this survey work. Several existing works under these categories are discussed below.

2.2 Existing Key Management Methods

To accomplish the high security in MANET, diverse Key Management schemes are utilized. Utilizing and managing keys for security is a significant task in MANET due to its energy compelled operations, limited physical security, variable limit links and dynamic topology. Secure communication is a critical test in ad hoc networks. The untrustworthy wireless medium in MANET is a risk for Secure Data Transmission. The communication in mobile ad hoc networks contains two stages, the route discovery and the data transmission. In an adverse situation, both Phases are defenseless against an assortment of attacks, one way to counter security attacks would be to cryptographically ensure and authenticate all control and data traffic. Key management is an essential piece of any protected communication structure. Most secure communication protocols depend on a protected, hearty, and productive key management system. The key is a bit of data information for cryptography algorithms. Ensuring security in key generation and exchange plays a major role in MANET.
Key management methods can be classified into two types, namely

(i) Contributory Methods

(ii) Distributive Methods

2.2.1 Contributory Methods

Contributory schemes are described by the absence of a trusted third party in charge of generation and distribution of the cryptographic keys. Instead, all conveying parties coordinate to establish (i.e., "agree" upon) a secret symmetric key. The number of members ranges from two parties (establishing a pair wise key) to numerous parties (establishing a group key). Despite the fact that not as a matter of course designed on account of ad hoc networks, naturally the contributory methodology of coordinated effort and self-association might appear to fit the way of ad hoc networks. A portion of the contributory schemes concentrated on here depend on a centralized entity, others don't.

![Fig 2.2 Contributory approach in key management](image)

Figure 2.2 shows the general network architecture of a contributory key management approach. It does not use a trusted third party in it. In contributory schemes, the key is a result of a collaborative effort of more nodes.
The question of key exchange was one of the first problems addressed by a cryptographic protocol. This was prior to the invention of public key cryptography. The Diffie-Hellman key agreement protocol [61] was the first practical method for establishing a shared secret over an unsecured communication channel. The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key. It applies to just two parties. Assurance of routing messages with pairwise keys requires different signatures for every conceivable beneficiary that scales incompletely. This scheme does not tackle MIM (Man in Middle Attack) vulnerability and not reach out to more than two parties.

As an extension to Diffie-Hellman, the group key agreement scheme is proposed by Burmester and Desmedt (B-D) [62]. Dependable multicasting is hard in wired networks, and considerably additionally challenging in ad hoc networks. Changes in-group enrollment requires a restart of the key-agreement technique. In an ad hoc network with moving nodes, there is no probability for establishment of a group key by B-D and maintenance of later changes in-group participation. Group changes can bring about delay and interruption. B-D likewise demands an already running routing protocol or stand out hop neighbors. This implies, the key-agreement schemes rely on upon an already established routing foundation. In any case, the framework can't be established before the keys have been set up.

For reducing the complexity of existing algorithms Hypercube and Octopus (H&O) [63], has proposed a method which minimizes the number of rounds by arranging the nodes in a hypercube. H&O contains two protocols, to be specific, Hypercube and Octopus. Hypercube expect the number of members is a force of 2. Octopus extends the
Hypercube to permit a self-assertive number of nodes. H&O is helpless against MIM attacks as authentication is absent. Byzantine or defective nodes might block fruitful key agreement. Changes in group enrollment require rekeying. It is left for the nodes to choose when re-keying is required. H&O depends on a basic communication system to offer a reliable node-requesting perspective to all group individuals. H&O is unsuitable for network layer security in ad hoc networks.

As an extension to the H&O, a password Authenticated mechanism is proposed [64] which is the stand out of the contributory systems designed for ad hoc networks. It is often referred to as the H&O method stretched out with secret key authentication. This method expect that all the legal members get a secret word offline. During the pair wise D-H key agreements of the H&O protocols, the nodes must demonstrate the learning of the secret key. The secret word is utilized to encrypt the public quality and a starting test in a test reaction protocol. This scheme duplicates the number of messages and expands the computational many-sided quality when contrasted with H&O. It solves the vulnerability of H&O to MIM attacks at the cost of scalability. The scheme acquires the lacks of H&O in regards to the trustworthiness of an already established communication base and node-requesting scheme. In this manner, it is not fitting for network layer security in mobile ad hoc networks.

CLIQUES [65] is another protocol suite that extends the generic D-H protocol to bolster the dynamic group operations. A group controller synchronizing the key agreement system is required. This scheme is computationally proficient. The designers did not consider the security properties like authentication while concentrating on group
changes. CLIQUES depends upon the solid multicast and the accessibility of a steady perspective of node ordering.

### 2.2.2 Distributive Methods

Distributive schemes include one or more trusted entities and involve both public key systems and symmetric systems. Really ad hoc networks require the trusted entity to be established during network initialization.

![Distributive Approach in key management](image)

**Fig 2.3** Distributive Approach in key management

Figure 2.3 shows the existence of the trusted third party in the distributive scheme. Distributive schemes may be centralized, however can likewise be distributed. In the latter, every node produces a key and tries to distribute it to others.

By Yi, Naldurg, and Kravets et al [66] have proposed Mobile Certificate Authority (MOCA) which is a decentralized key management scheme. In this scheme, a certificate service is distributed to MOCA nodes. MOCA nodes are picked in view of heterogeneity if the nodes are physically more secure and computationally all the more effective. It presents a practical key management framework for ad hoc wireless networks.
using PKI. It clarifies the necessity and the problem of providing a PKI framework for ad hoc network. It also identifies the requirements for such a framework and provides some insights into the configuration of such security services in ad hoc networks.

In Secure and Efficient Key Management (SEKM) [67], it is easier for a node to request service from a well maintained group rather than from multiple "independent" service providers, which may be spread in large area. The servers of MOCA structure a multicast group to effectively update the secret shares and certificates. A node broadcasts a certificate request to the CA server group. The server that first gets the request, produces an partial signature, and advances the request to additional servers. The additional servers are utilized for redundancy as a part of case some are lost or debased. SEKM does not discuss about how a server can let it know is the first to get the refresh request and start the forwarding. SEKM has the same components as MOCA. The required number of servers still must be reached, and the partial signatures returned. Be that as it may, this system neglects to work under different server groups in large networks including partitioned network.

Ubiquitous Security Support (UBIQ) [68] is a fully distributed threshold CA scheme. Like MOCA, and SEKM, UBIQ also relies on a threshold signature system with a secret sharing of the private CA key. In addition, all nodes get a share of the private CA key. Every entity holds a secret share and different entities in a nearby neighborhood together give complete services. Confined certification schemes are utilized to empower pervasive services. This scheme operates well at the network with breakages. The solution is completely decentralized to operate in a large-scale network. The limitation in the rescue operations scenario is the possible requirement of human involvement.
Composite Key Management (COMP) [50] joins partially distributed threshold CA of MOCA together with the self organized key management scheme. Certificate-chaining method and expanded accessibility of CA is the specialty of the proposed scheme. Results shows the effectiveness of composite key management under stressful scenarios where the existing approaches fail to work. COMP assumes a level of trust transitivity. This technique uses the highest confidence certificate chain that does not fully exploit the information contained in a certification graph. COMP can provide flexible, modular, and adaptive key management services for mobile ad hoc networks.

Efficient and robust key management scheme [69] is a hierarchical scheme based on threshold cryptography to address both security and efficiency issues of key management and certification service in MANET. Key management scheme provides various parts of MANET the flexibility of selecting appropriate security configurations, according to the risks faced. It also offers the adaptivity to cope with rapidly changing environments. This technique maintains a large number of nodes and issue certificates with different levels of assurance. This scheme can isolate the compromised regions and provide stronger protection to the Global Secret Key (GSK) compared to flat-structured schemes.

Scalable means of cryptographic key management (SMOCK) [57] is an independent public key-management scheme, which obtains irrelevant communication overhead for authentication, and offers greatest service accessibility. Here a combinatorial design of public-private key pairs is made which furnishes every node with additional security of more than one key pair to encrypt and decrypt messages. A combination method is used and a pair of public keys is used to encrypt the data, the pair
ID is going to be assigned during the initialization process. Before the communication, the ID to be forwarded to the destination and depends upon this, the encryption process will be carried out. At the receiver end the decryption will be done by using the private keys of the corresponding public keys. The information about which public key should use for encryption is received from the pair ID communicated by the two parties. Here each node is going to store all the public keys and a set of private keys (depends upon the combination). This reduces the number of keys stored in each node and enhances the traditional public/private pair key generation. This configuration helps in acquiring higher security as far as nodes and storage space. The scheme likewise accomplishes controllable resilience against node compromise by characterizing required benchmark resilience. Be that as it may, this technique has two noteworthy disadvantages. It utilizes the centralized offline servers for revoking/invigorating keys and to make new keys for the new nodes. The second downside is that, the increment in nodes eventually expands the public-private key pairs (yet relatively in low extent than traditional methodology).

ID-based multiple secrets key management (IMKM) [70] protocol is a comprehensive solution for inter and intra-cluster key management, including key revocation, key update, and group key agreement. IMKM requires that cluster heads (CHs) participate in the construction of the key, in order to establish a \( (t, n) \) threshold sharing of the master secret key. The advantages of using a distributed method lie in its efficiency and flexibility in updating CHs’ share keys. This method does not require the exchange or signing of any additional messages when the network is within security tolerance. To address security concerns, it updates the CHs’ share keys when CHs are evicted and the number of revoked CHs reaches a predefined threshold.
2.3 Existing Certificate Distribution and Exchange Methods

The certificate exchange system offers the nodes to authenticate themselves with the individuals in the network before they some assistance with getting joined and begin another communication. Nodes with a valid certificate can participate in a communication. Initially the certificates will be distributed to all normal nodes. The newly joining nodes will get the certificate after an initial verification.

Certificate distribution and exchange method is broadly classified into two types. They are

(i) Trust based methods

(ii) Non-trust based methods

2.3.1 Trust Based Methods

It requires a trust based mechanism to exchange the certificates among nodes. It is to authenticate the nodes before allocating the certificate to it. Mostly it carries a centralized architecture, in order to monitor the participant nodes in the network. Distributed approach can also be applied based on the routing scenario. A trusted authority is required to monitor the certificate distribution as well as allocation. That authority will collect the trust value of a node before allocating the certificate to it. The nodes with a good amount of trust value are considered as normal nodes.

This trust may be calculated dynamically during the path selection of the protocol. Different paths may be obtained by using the existing algorithms and the trust of each path is going to be calculated. A threshold trust value is fixed to identify the normal nodes. If any node does not acquire a minimum threshold trust value, then that node is considered as malicious node and steps are initiated for isolating that particular node.
Figure 2.4 illustrates the trust based certificate exchange mechanism. The trust value will be calculated before issuing certificates. If the trust value is minimal, then the communication will be marked as distrusted communication.

The design focuses on a truly ad hoc networking environment where geographical size of the network, numbers of network members and mobility of the members is all unknown before deployment. The process of development of the protocol and the application to system design are developed to assure information security and potential evidential retention for forensic purposes. Threshold encryption key management is utilized and simulation results show that security within the network can be increased by
requiring more servers to collaborate to produce a certificate for a new member, or by requiring a higher trust threshold along the certificate request chain. The cost such as time, processor use and battery use in mobile devices of information management is also considered here. When the number of servers increases, longer certificate chain is required. An increase in the chain length may increase the likelihood of the chain encountering a malicious node. Therefore, a failure occurs in the network [71].

A key exchange protocol [72] integrated with a routing protocol is lightweight, efficient and alleviates the routing-security interdependency cycle. This routing protocol establishes a path between source and destination by reactive routing protocols. Initially, a route request message is broadcasted to discover the route to the destination. The key exchange protocol uses this approach to retrieve the public keys of the nodes. Source node floods a certificate request to find a certificate of a public key. The receiving node replies either by the target node or by an intermediate node. It tries to distribute spurious certificates and causes routing disruption. Multi-path certificate exchange and trust-based certification are used for providing robustness and reliability. It is resistant to isolated attack launched by malicious nodes that may introduce spurious certificates. When sufficient level of trust exists among some nodes before the network deployment, it performs well against cooperative attacks. When MPKTV value is 0.5, any reply is accepted. Further due to the increase in number of attackers, the probability of accepting corrupted public key increases.

In an efficient public key management scheme [73] for fully self-organized mobile ad hoc networks, the operations of creating, storing, distributing, and revoking nodes' public keys are carried out locally by the nodes themselves. This method improves
the process of building the local certificate repositories of nodes. An authentication solution based on the web of trust concept is combined with an element of routing based on the multipoint relay concept to introduce the optimized link state routing protocol. It offers good tradeoff among security, overhead and flexibility, considerable reduction in resource consumption whereas performing the certificate verification process. However, this mechanism increases the delay of issued certificates.

Ad hoc Trust Framework (ATF) [74] support ADOPT’s robustness and efficiency. ADOPT is deployed as a trust-aware application that provides feedback to ATF. ATF calculates the trustworthiness of the functions of the peer nodes. ATF also helps ADOPT for improving its performance by quickly locating valid certificate status information. The TrustSpan algorithm reduces the overhead produced by ATF. It can also identify and use the trusted routes to propagate the sensitive information like accusations of the third party. ATF adds limited overhead when compared to its efficiency in noticing and isolating the malicious and selfish nodes. As it can quickly locate a genuine response by using ATF’s information, the reliability of ADOPT is increased. Lastly, the optimized caching policies based on mobility, connectivity, capacity, and trustworthiness is discussed. However, the overhead due to the requested recommendations is largely increased, when the number of invalid responses is maximized.

To obtain resilience and efficient path discovery among Peer-to-Peer trusted PKI’s [75] for issuing entities, a virtual hierarchical architecture is used. As the execution time is less, it is suitable for MANETs. A virtual hierarchy in a Peer-to-Peer PKI is established based on the trustworthiness of the participating neighbors. The upward approach is used to build the hierarchical structure, that is, from the leaves to the root. In
addition, it does not require to issue new certificates among PKI entities, facilitates the certification path discovery process and the maximum path length can be adapted to the characteristics of the users with limited processing and storage capacity. However, the effectiveness of this technique is only analyzed theoretically. There is no practical implementation to prove the results.

2.3.2 Non-trust based Methods

The trust value of the node is used to make the communication authentic and secure. So we are helpless to perform the certificate exchange process without the assistance of a trust mechanism. But, it is possible to eliminate the overhead of trust computation by replacing it with some alternate techniques. Such techniques must guarantee a secure communication in all means. ID based exchange as well as certificate chaining approaches are the good alternatives to the trust based certificate exchange. Here the process itself offers the security without a trust management mechanism.

Figure 2.5 illustrates the non trust based certificate exchange mechanism. Here the public keys can collect either from an existing certifier (intermediate node) or from the destination itself.

A certificate based authentication mechanism [76] is used to contradict the effect of black hole attack. Nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online-centralized authority. After the route establishment process of On Demand Multicast Routing Protocol (ODMRP), this scheme has certification phase and authentication phase. All certificates issued are stored in the repositories of the issuer and the certificate subject. The certificates are exchanged between the neighboring nodes periodically. By utilizing this,
nodes collect certificates in their repositories at a low communication cost in light of the fact that the exchanges are performed locally in one hop. This mechanism can be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks. When the number of attackers is increased, the packet delivery ratio is greatly reduced due to loss of packets in the black hole nodes.

![Certificate Exchange – Non-Trust Based approach](image)

Fig 2.5 Certificate Exchange – Non-Trust Based approach

A completely self-organized public-key management system [59] permits users to create their public private key pairs, issue certificates and perform authentication paying little heed to the network partitions and with no centralized services. The two
users in a mobile ad hoc network can perform key authentication construct just in light of their nearby information, regardless of the fact that security is performed in a self-organized way. With the vicinity of neighborhood repository development algorithm and a little communication overhead, it accomplishes superior on an extensive variety of certificate graphs. Nodes can exploit mobility to encourage authentication and to distinguish conflicting and false certificates. This methodology does not require any trusted authority, not even in the system initialization stage. Nonetheless, the detection and the determination of conflicting certificates are excluded in this mechanism. A few parameters like delay, throughput are not discussed in this mechanism.

A novel key distribution scheme [77] for MANETs exploits the routing base to viably chain peer nodes together. Keying material propagates along these virtual chains through a message handing-off mechanism. It results in a key distribution scheme with low implementation complexity, preferably suited for stationary ad hoc networks and MANETs with low to high mobility. It utilizes mobility as a guide to fuel the rate of bootstrapping the routing security, yet rather than existing schemes does not get to be subject to mobility. The key spread happens totally on-demand; security affiliations are just established as required by the routing protocol. The communication and computational overhead of this methodology has immaterial effect on network execution. In any case, when the mobility builds, route failure might happen.

Here, the node mobility is considered and the major improvements related to the number of elected cluster heads are given for creating the PKI council. Here, the certification authority functions are distributed for a reduced set of mobile nodes to serve for keys management. For selecting the council members, the two solutions are made. 1)
A set of nodes that makes the council of PKI is designed. The members are randomly chosen. They remain the same until the network exists. Hence, it is considered as fixed-members architecture. 2) The network is organized as clusters and each cluster has a cluster-head. The council of PKI is made up of the cluster heads present in the network form. Hence, it is denoted as cluster-based architecture. These two architectures are compared and concluded that the clustered architecture provides a better result and is well suited to the dynamic environment. However, it is not focused on aspects of the choice of the threshold parameter values and the council member’s number [48].

The Tseng model and the Capkun model [78] are merged to improve the overall performance and offer less overhead with high security. This model authenticates the nodes via 4G services to facilitate the communication after the nodes becoming the part of certificate chain-based groups. The nodes have logins and passwords through server before joining the MANET that forms the basis of verifiable identities for getting certificates. Nodes generate private and public keys by built-in PKI techniques. For issuing certificate, the servers sign these public keys. Each node needs a certificate for joining the certificate chain based group. A long chain of certificates leads to group formation. The session last until the expiry time of either of the node’s certificate. This process saves the bandwidth and increases efficiency. However, when the time period is very limited, it leads to extra burden of entity verification messages. When the time period is large, security related issues might occur. This produces lack of performance of the protocol in terms of delay and security related parameters. This tradeoff becomes a major drawback of this approach.
2.4 Existing Certificate Revocation Methods

In MANET, the certificates are used to make the communication more secure. Only the nodes with a valid certificate can participate in the communication. Thus the certificate of an attacker node has to be revoked once it listed as a malicious node.

The certificate revocation methods are classified based on the mechanisms used to revoke the certificates. They are

(i) Voting Based Method

(ii) Trust Based Method

2.4.1 Voting based Methods

The voting based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. Voting-based scheme, allows all nodes in the network to vote (accuse) against malicious nodes. Each node monitors the behavior of its neighbors. An authorized node will collect the accusations from the normal nodes. The accusations will be treated as a valid one only if the authorized node is able to get same accusation from different nodes. The malicious nodes can accuse legitimate nodes. Thus, it is important to identify valid accusations. In the case of invalid accusations, the accuser node will be treated as a malicious node. The nodes can vote with variable weight. The weight is ascertained from a node's dependability which is received from its past conduct. The higher its unwavering quality is, the more prominent its weight will be. The certificate of a suspicious node can be revoked when the total of the weights of the votes against the node comes to or surpasses a predefined threshold. Thusly, the exactness of certificate revocation can be moved forward. Then again, since all nodes are required to participate during each vote, the
communication overhead required to exchange voting information is entirely high. That will thusly expand the time expected to revoke the certificate.

**Fig 2.6 Certificate Revocation – Voting Based approach**

Figure 2.6 illustrates the voting based certificate revocation mechanism. Here the votes can treat as the accusations from normal nodes. An accusation will consider as a valid accusation, only if the collecting node is able to get enough number of accusations
about a same node. Certificate of the accused node will be revoked in the case of valid accusation. Otherwise the accuser node will be marked as a malicious node.

In this voting-based scheme, all nodes in the network are permitted to vote. Like URSA, no CA exists in the network, and instead every node screens the conduct of its neighbors. Here, the nodes vote with variable weight. The weight is ascertained from a dependability of the node that is gotten from its past conduct. The higher unwavering quality can bring about more prominent weight. The certificate of a suspicious node can be revoked when the entirety of the weights of the votes against the node comes to or surpasses a predefined threshold. Consequently, the exactness of certificate revocation strategy can be progressed. Then again, since all nodes are required to participate during each vote, the communication overhead required to exchange voting information is entirely high, along these lines expanding the time expected to revoke the certificate [55].

URSA [79] utilizes a voting-based mechanism to expel nodes. The certificates of recently joining nodes are issued by their neighbors. The certificate of an attacker is revoked in light of votes from its neighbors. In URSA, every node per-frames one-hop checking, and exchanges screen information with its neighboring nodes. At the point when the number of negative votes surpasses a foreordained number, the certificate of the accused node will be revoked. Since nodes can't communicate with others without valid certificates, revoking the certificate of a voted node infers disconnection of that node from network exercises. Deciding the threshold, on the other hand, remains a test. If it is much larger than the network degree, nodes that dispatch attacks can't be revoked and can be progressively continued speaking with different nodes. Another basic issue is that URSA does not address false accusations from malicious nodes. While URSA does not
require any exceptional gear, for example, Certificate Authorities (CA), the operational cost is still high.

T.R.Panke [80] has improved their proposed clustering-based certificate revocation scheme which considers quick certificate revocation. At the point when the number of normal nodes gradually diminished, a threshold-based mechanism is utilized to restore the accusation function of nodes in the WL. Despite the fact that a centralized CA oversees certificates for every one of the nodes in the network, cluster development is decentralized and performed autonomously. Every CM has a place with two unique clusters so as to give robustness against changes in topology because of mobility. The protocol does not address security analysis part.

The procedure of revoking malicious Certificates is discussed to revoke a malicious attacker’s certificate, there is a need to consider three stages accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node. The false accusation of a malicious node against a legitimate node to the CA will degrade the accuracy and robustness of our scheme. To address this problem, one of the aims of constructing clusters is to enable the CH to detect false accusation and restore the falsely accused node within its cluster. This certificate revocation process tends to take a long time in detecting malicious node [81].

By ordering nodes into clusters, this scheme permits every Cluster Head (CH) to distinguish false accusation by a Cluster Member (CM) inside of the cluster. Node clustering gives a way to alleviate false accusations. CHs always screen their CMs and look for false accusations. Just normal nodes having high unwavering quality are permitted to wind up a CH. Nodes with the exception of CHs join the two unique clusters
of which CHs exist in the transmission range of them. By developing such clusters, each CH can know about false accusations against any CMs since each CH knows which CM executes attacks or not, on account of the greater part of the attacks by a CM can be identified by any node, obviously including the CH, inside of the transmission range of the CM.

The motivation behind why every node with the exception of CH has a place with two distinct clusters is to diminish the danger of having no CH because of dynamic node development. To keep up clusters, CH and CMs as often as possible affirm their presence by trading messages, i.e., the CH intermittently broadcasts CH Hello packets to the CMs inside of its transmission range, and every CM answers to the CH with the CM Hello packet.

A newly joining node becomes CH at a constant rate. A node, which has decided not to become a CH itself, will look for other CH nodes in the area. If there are more than two CHs near the node, it will attempt to join two of these clusters by randomly selecting two of their CHs and sending each of them a CM Hello packet. Otherwise, the joining node declares itself as a CH and broadcasts CH Hello packets. When a CM leaves the cluster, it needs to invoke a similar procedure to find out new CHs. If the CM receives no CH Hello packet from its CH for a certain period of time, the CM considers itself having departed from the cluster, and tries to find and join a new cluster [42]. This certification revocation method outperforms all the other existing revocation mechanisms since it uses a vindication capability mechanism to identify the malicious behavior of a node.
2.4.2 Trust based Methods

Establishing trust among the nodes in an ad hoc network is critical from a security point of view as the nodes go about as self securing devices to ensure themselves with no infrastructural support. Besides, nodes route packets to a destination through intermediate nodes. Thus, nodes need confirmation to depend on different nodes in the network and this is accomplished by establishing trust relationships among the nodes. The certificate of a node will be revoked in view of the trust value. A good trust model ought to be adaptable; it ought to have a broad adversary control mechanism and ought to establish trust among the nodes. On the other hand, establishing trust relationships among the nodes includes communication overheads. A good trust based model must have the capacity to address the issues identified with the communication overhead. Dependable nodes ought to get by in the network, while nodes which don't give a good nature of service or are malicious ought to be distinguished rapidly and expelled from the network.

Figure 2.7 illustrates the trust based certificate revocation mechanism. Here the revocation happens purely based on trust value. The revocation can be done either by a neighbor node or by a trusted third party.

An enhanced distributed certificate authority scheme [5] give data integrity by making the network more secure from both inside and outside attacks. It makes utilization of Shamir's secret sharing scheme along to a redundancy strategy to backing certificate renewal and revocation. In this strategy, the malicious nodes are recognized by the monitoring so as to trust mechanism the conduct hop by hop. This scheme builds the integrity of the network and gives the network nodes to be more mobile. Be that as it may, this method lessens the general throughput significantly.
Fig 2.7 Certificate Revocation – Trust Based approach

A distributed trust model for certificate revocation [82] permits trust to be constructed after some time as the number of interactions between nodes increment. Besides, trust in a node is characterized as far as its potential for maliciousness and nature of the service it gives. Trust in nodes where there is practically no history of interactions is dictated by proposals from different nodes. If the nodes are narrow minded, trust is acquired by an exchange of portfolios. The rate of helpful communication is enhanced by presenting setting particular trust connections among the nodes. The intrusion detection system of every node joined with the trust associations with alternate nodes viably removes malicious nodes in the network. Thus, the malicious nodes are viably uprooted and the expulsion of honest nodes from the network is minimized. A few parameters like accessibility and nature of service are excluded for the determination of trust. Bayesian model causes execution overheads.
This revocation scheme [56] is utilized for the distribution of revocation information in mobile ad hoc networks (MANETs). This scheme can be executed in conjunction with the transcendent routing protocols in ad hoc networks. At that point it gives an itemized security examination somewhat taking into account the utilization of formal techniques. It basically concentrates on revocation of certificates and IDs used to secure routing information in MANETs utilized as a part of crisis and rescue operations. The revocation records should thusly be particular to the network. They are established with the guide of trusted gateways reporting the identity of the nodes to a focal trusted entity. To minimize overhead, the revocation records are distributed alongside the routing messages. It offers limited robustness to fluctuating network availability.

In the decentralized suicide based approach [83], while the certificate revocation can be done with an accusation, the certificate of the accused node and the accuser's certificate are revoked. No less than one node needs to give up itself to expel an attacker from the network. This system significantly lessens both the time required to remove a node and the communication overhead of the certificate revocation methodology. On the other hand, inferable from its suicide-based procedure, the use of this methodology is limited. This scheme does not give a mechanism to separate erroneously accused legitimate nodes from appropriately accused malicious nodes. Thusly, the exactness is degraded.

DICTATE[84] utilizes a number of CA to productively perform the publication and revocation of certificates. CA screens node conduct so as to recognize attacks and share the certificate information with one another. In the event that a CA distinguishes a malicious node, the certificate of the node is revoked by the CA and its information is
shared among other CA, there by isolating the node from the network. Then again, the deployment of an adequate number of CA is not a simple task in MANETs.

Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network (CONFIDANT) is a reputation system going for adapting to trouble making in MANET [85] [86] [87]. The thought is to recognize the got into misbehaved nodes and confine them from communication by not utilizing them for routing and sending and by not permitting the acted mischievously nodes to utilize it to forward packets. CONFIDANT remains for Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Network. It normally fills in as an augmentation to on demand routing protocols.

2.5 Classification of existing Key Management & Certificate Exchange/Revocation Methods

<table>
<thead>
<tr>
<th>S. No</th>
<th>Approach</th>
<th>Category</th>
<th>Metrics</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>New Directions in Cryptography [17]</td>
<td>Contributory Method</td>
<td>Packet Overhead</td>
<td>Basic approach for key management</td>
<td>Vulnerable to MIM attack</td>
</tr>
<tr>
<td>2</td>
<td>A Secure and Efficient Conference Key Distribution System [62]</td>
<td>Contributory Method</td>
<td>Packet Overhead</td>
<td>Secure against any type of attack and solve DL problem</td>
<td>Not used in real time applications</td>
</tr>
<tr>
<td>3</td>
<td>Communication Complexity of Group Key Distribution [63]</td>
<td>Contributory Method</td>
<td>Number of exchange, number of rounds and no. of messages</td>
<td>Minimizes the number of rounds</td>
<td>It cannot be adopted for network layer security. Authentication is not discussed.</td>
</tr>
<tr>
<td>4</td>
<td>Key Agreement in Adhoc Networks [64]</td>
<td>Contributory Method</td>
<td>Number of rounds</td>
<td>Eliminates the MIM attacks</td>
<td>Not appropriate for network layer security in MANET</td>
</tr>
<tr>
<td>5</td>
<td>CLIQUES: A New Approach to Group Key Agreement [65]</td>
<td>Contributory Method</td>
<td>Lifespan and security of particular key</td>
<td>Computationally efficient</td>
<td>Do not provide authentication.</td>
</tr>
<tr>
<td></td>
<td>Title</td>
<td>Method</td>
<td>Metrics</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks [66]</td>
<td>Distributive</td>
<td>Packet overhead, certificate delay, number of CREP</td>
<td>Less vulnerable to attacks</td>
<td>Bandwidth wastage</td>
</tr>
<tr>
<td>7</td>
<td>Secure and Efficient Key Management in Mobile Ad Hoc Networks [67]</td>
<td>Distributive</td>
<td>Average Number of Hops, average delay, server rate, convergence time</td>
<td>Effectively update the secret shares and certificates</td>
<td>Fails to work under multiple server groups in large networks</td>
</tr>
<tr>
<td>8</td>
<td>Providing Robust and Ubiquitous Security Support for Mobile Ad- Hoc Networks [68]</td>
<td>Distributive</td>
<td>Success ratio, average delay, and average number of failures</td>
<td>Decentralized to operate in large network</td>
<td>Need human intervention</td>
</tr>
<tr>
<td>9</td>
<td>Composite Key Management for Ad Hoc Networks [50]</td>
<td>Distributive</td>
<td>Success ratio, mobility, crypto Threshold, communication overhead, average confidence value</td>
<td>Flexible, modular, and adaptive key management service</td>
<td>Has limited robustness and scalability</td>
</tr>
<tr>
<td>10</td>
<td>Efficient and Robust Key Management for Large Mobile Ad Hoc Networks [69]</td>
<td>Distributive</td>
<td>success rate, error rate, average retries of certification renewals</td>
<td>Maintain large number of nodes. Adaptive to cope with rapidly changing network</td>
<td>Susceptible to some attacks</td>
</tr>
<tr>
<td>11</td>
<td>SMOCK: A scalable method of cryptographic key management for mission critical wireless ad-hoc networks [57]</td>
<td>Distributive</td>
<td>Memory storage, Delay</td>
<td>Reduction in the number of key pairs.</td>
<td>Increase in nodes ultimately increases the public-private key pairs.</td>
</tr>
<tr>
<td>12</td>
<td>Securing Cluster-Based Ad Hoc Networks with Distributed Authorities [70]</td>
<td>Distributive</td>
<td>Memory storage, Delay</td>
<td>Address the problem of varying link qualities.</td>
<td>Bandwidth overhead</td>
</tr>
<tr>
<td>Certificate Distribution and Exchange</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Black Hole Attack Prevention in Multicast Routing Protocols using Certificate Chaining [76]</td>
<td>Non-trust based Scheme</td>
<td>Packet delivery ratio, Average end-to-end delay</td>
<td>Secure the network from routing attacks by varying the security parameters based on attacks.</td>
<td>The packet delivery ratio is reduced due to loss of packets, When the attackers increases,</td>
<td></td>
</tr>
<tr>
<td>14 Secure Key Deployment and Exchange Protocol for MANET Information Management [71]</td>
<td>Trust based Scheme</td>
<td>Mobility, Speed, certificate issuance ratio</td>
<td>Security inside the network can be increased with more servers</td>
<td>Increased servers can cause longer certificate chain that may increase the likelihood of the chain encountering a malicious node. A failure occurs in the network.</td>
<td></td>
</tr>
<tr>
<td>15 A Multi-Path Certification Protocol [72]</td>
<td>Trust based Scheme</td>
<td>Valid PK acceptance rate, Corrupted PK acceptance rate, Delay</td>
<td>Resistant to isolated attack by malicious nodes that may introduce spurious certificates</td>
<td>When MPKTV value is 0.5, any reply is accepted. Due to more attackers, the probability of accepting corrupted public key increases.</td>
<td></td>
</tr>
<tr>
<td>16 Self-Organized Public-Key Management [88]</td>
<td>Non-trust based Scheme</td>
<td>Average shortest path, mobility</td>
<td>Mobility facilitate authentication and detect the inconsistent and false certificates.</td>
<td>Parameters like delay, throughput are not discussed</td>
<td></td>
</tr>
<tr>
<td>17 Key Distribution based on Message Relaying [77]</td>
<td>Non-trust based Scheme</td>
<td>Packet delivery ratio, packet end-to-end delay</td>
<td>Communication and computational overhead has less impact on performance.</td>
<td>When the mobility increases, route failure may occur</td>
<td></td>
</tr>
<tr>
<td>18 Efficient Public Key Certificate Management [73]</td>
<td>Trust based Scheme</td>
<td>Number of nodes in graph, rate of certificates in repository, clustering</td>
<td>Good tradeoff among security, overhead and flexibility, considerable</td>
<td>The delay of issued certificates are increased</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Integrating a Trust Framework with a Distributed Certificate Validation Scheme [74]</td>
<td>Trust based Scheme</td>
<td>Communication overhead, detection time, number of responses and trusted paths, Cerberus function gain, roundtrip delay</td>
<td>ATF adds limited overhead for detecting and isolating malicious and selfish nodes</td>
<td>Overhead due to the requested recommendations is increased, when there is more invalid responses</td>
</tr>
<tr>
<td>20</td>
<td>Certificate Path Discovery by Constructing Virtual Hierarchy to Administer Trust Relationship using Peer to Peer PKI [75]</td>
<td>Trust based Scheme</td>
<td>-</td>
<td>Formation of trust relationship to establish the hierarchy and not to issue new certificates or to adjust the trust points.</td>
<td>No practical implementation to prove the results.</td>
</tr>
<tr>
<td>21</td>
<td>A Distributed Key Management Scheme using council architecture [48]</td>
<td>Non-trust based Scheme</td>
<td>Delivery delay of a certificate, certificate delivery fraction, response time of PKI</td>
<td>Delay is reduced with increased efficiency</td>
<td>Aspects of the choice of the threshold parameter values and the council member’s number are not focused</td>
</tr>
<tr>
<td>22</td>
<td>Certificate Chain based Authentication using 4th Generation Technologies [78]</td>
<td>Non-trust based Scheme</td>
<td>Cost of external messages, number of nodes</td>
<td>Saves the bandwidth and increases efficiency.</td>
<td>Limited time period causes extra burden of entity verification messages. Larger time period causes security related issues</td>
</tr>
</tbody>
</table>

**Certificate Revocation Methods**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>A localized certificate revocation scheme [55]</td>
<td>Voting-based scheme</td>
<td>Communication overhead, communication complexity</td>
<td>Accuracy of certificate revocation technique can be improved</td>
</tr>
<tr>
<td>Page</td>
<td>Title</td>
<td>Scheme Type</td>
<td>Metrics</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>24</td>
<td>URSA: Ubiquitous and Robust Access Control [79]</td>
<td>voting-based scheme</td>
<td>Success ratio, number, average number of retries, average delay, normalized overhead</td>
<td>Effectively enforces access control in the highly dynamic network. Operational cost is still high.</td>
</tr>
<tr>
<td>25</td>
<td>Certificate Revocation to Cope with False Accusations [42]</td>
<td>voting-based scheme</td>
<td>Ratio of revoked attackers, control packet traffic, node density, attack success count,</td>
<td>It promptly removes the attackers with low operating traffic even in the presence of malicious nodes carrying out false accusations. The reliability and accuracy is low when compared to other schemes.</td>
</tr>
<tr>
<td>26</td>
<td>Clustering Based Certificate Revocation Scheme for Malicious node [43]</td>
<td>voting-based scheme</td>
<td>-</td>
<td>Rapidly revoke attacker’s certificates and recover falsely accused certificates. There is no security analysis.</td>
</tr>
<tr>
<td>27</td>
<td>Cluster-Based Certificate Revocation with Vindication Capability [81]</td>
<td>voting-based scheme</td>
<td>Revocation time, number of warned nodes, node speed, node density</td>
<td>Effective and efficient to guarantee secure communications. Detection of malicious node takes longer time.</td>
</tr>
<tr>
<td>28</td>
<td>Suicide for the Common Good: a New Strategy for Credential Revocation in Self-Organizing Systems [83]</td>
<td>-</td>
<td>Overhead, delay</td>
<td>Has fully decentralized, low communication and storage overhead, fast removal of misbehaving nodes. There is no mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes. So, accuracy is degraded.</td>
</tr>
<tr>
<td>29</td>
<td>DICTATE: Distributed Certification Authority With Probabilistic Freshness [84]</td>
<td>-</td>
<td>Freshness degree, speed, freshness load</td>
<td>Robust against various attacks in MANET. Deployment of a sufficient number of CA is a complex task.</td>
</tr>
<tr>
<td>30</td>
<td>An Enhanced Distributed Certificate</td>
<td>Trust based scheme</td>
<td>Control overhead, average end-to-end delay</td>
<td>Integrity of the network increases. Overall throughput is considerably</td>
</tr>
</tbody>
</table>
2.6 Design Considerations of the Thesis

A secure framework suitable for military and tactical applications based on trust is to be developed. The trusted system should address the following applications,

- Key management
- Secure source routing
- Malicious node detection.

While designing such a system, the following mechanisms should be considered in the framework.

- Independent key generation mechanisms
- Key distribution based on certificate/ID exchange
- Reducing the number of public/private key pair used
- Battery power and memory of a mobile node should be preserved
• Path establishment based on trust
• Trust calculation based on the connectivity and past performance of a node
• Future trust prediction of a node
• Malicious node detection
• Isolation of a malicious node

The proposed framework should possess the following performance criteria.

• Overall network resilience should be improved
• Detection rate of a malicious node to be improved
• The above improvements should be done without affecting the basic performance factors like delay, throughput, packet drop and overhead.

2.7 Summary

In this section, several key management schemes, clustering techniques used for effective key management and certificate Revocation schemes have been discussed. Some of them are having some disadvantages. To overcome them, effective techniques must be developed. In this research thesis, some limitations stated below are considered and overcome by proposing effective techniques.

The scalable method of cryptographic key management (SMOCK) [57] proposes a method to deal with such node compromise attacks. It has certain main drawbacks such as over dependent on centralized server and increase in key-pair when node increases.

The existing Weighted Clustering Algorithm (WCA) [89] induces increased overhead. Also, the details of the mobile nodes are gathered always before joining or
starting the clustering process, which produces Congestion and drain the CH. From these issues, it is known that an effective clustering technique for key management must be developed to reduce the overhead and congestion.

The proposed technique [59] to cope with misbehaving node does not prevent users from creating virtual identifiers or from stealing the identity of people that do not participate in the network. Also, exploration of more sophisticated load-balancing/data management schemes for public-key management is not handled. In [51], the author has not discussed the authentication parameters.

In [53], the proposed technique lags certificate revocation methodology. Also, authentication parameters are discussed in detail. In [60], the authors have only assumed that every node in a MANET first generates a public/private key pair. From these existing works, it is known that strong self-certified key generation and certificate exchange mechanisms along with some trusted model must be developed.

The existing certificate chaining mechanisms did not provide assurance to the public keys authentication. Certainly the certificate chaining among two nodes are possibly not established. There is a requirement of extensive time until the web-of-trust is set up among each other. The predicted results in this scheme will not be precise since it is not based on TTP. The nodes acts as individual CA and consequently the certificate chain will depend on the nodes honesty concerned with the formation.

Even though the existing certificate revocation schemes have handled the situation that no on-line access to trusted authorities in MANET. They provide a large amount of operational traffic and a long revocation time, because the opinion of every node in the network is needed for each node to decide whether to revoke the certificate of
the malicious node or not. Also, most of the existing revocation schemes did not provide trust management along with certificate revocation mechanism. Therefore, it is evident that a certificate revocation mechanism integrated with the underlying routing protocol and the trust Management must be developed.

A security framework based on trust is proposed to address the above issues. The framework consists of trusted certificate exchange and revocation, trusted route discovery/path selection, trust prediction of intermediate node and isolation of malicious node in various multipath/clustered routing protocols.