CHAPTER 5

SECURE AND RELIABLE COMMUNICATION SCHEME FOR MANET USING ECMS CLUSTER HEAD-BASED CERTIFICATE REVOCATION

5.1 MANETs Certificate Revocation

For the formation of arbitrary topology, wireless links are used in mobile routers for connection in MANET. Various applications used by MANET are wireless communication in vehicular ad-hoc networks, mobile networking, health monitoring system and emergency alert system. A mobile node joins with other nodes and moves randomly wherever needed in mobile ad-hoc networks. MANET does not follow a fixed communication infrastructure for mobiles. An unauthorized or malicious user has more possibility of an attack on mobile ad-hoc networks due to lack of infrastructure. As this problem becomes more complicated than possibly, that creates a way for attacks in MANET.

For this reason, many detection methods are proposed by the previous work and identify the attacks. Moreover, we recommend Time Adaptive Enhanced Acknowledgement (TAEACK) approach for finding malicious nodes and eliminate from the route. The acknowledgment is received or sent by TAEACK approach after or before data transmission takes place among the pair of nodes within a distance and time interval. Blocking of nodes, Security Key verification, and attack detection not only solve security issues in mobile ad-hoc networks but also attacker is removed from the nodes. Unauthorized access repeatedly performed by the attacker against the network. The mandatory solution is to remove the attacker from the network in MANET. A certification system applies this removal process.

A valid certificate is provided by the necessary role of certificate system for communication between the nodes in mobile ad-hoc networks. Hence, it is not possible to communicate mobile nodes in MANET with each other without an appropriate certificate. In other words, by using the certification system, mobile nodes are identifying an attacker that network does not have that identified node. The strategy of revocation certificate is used for evaluation of certificate piece.

In general, during the certificate system, some issues raised are less precision, slow revocation and high network overhead. The dependability's of nodes determination is used for certificate revocation. For isolation or avoiding the malicious nodes, rational nodes are used in mobile ad-hoc networks. The neighboring nodes provide the trusted recommenders identification and exchange of recommendations for performing security system based certification in MANET. Hence, the malicious nodes identified by certification system, other existing nodes help by their judgments that belong to the network.

Also, attackers give false accusation for revoking the certificate of genuine nodes. Hence, true recommendations and false accusation from the neighbor nodes are classified by certificate revocation system. Moreover, the node must be blocked or removed when they identify as a malicious node from the network. In general, MANETs characteristics are given as dynamic topology, distributed routing mechanism, fewer infrastructure, and directness. The exchanged data could not alter or changed by the attacker during the attack process. Certificate revocation scheme in mobile ad-hoc network are shown in figure 5.1.

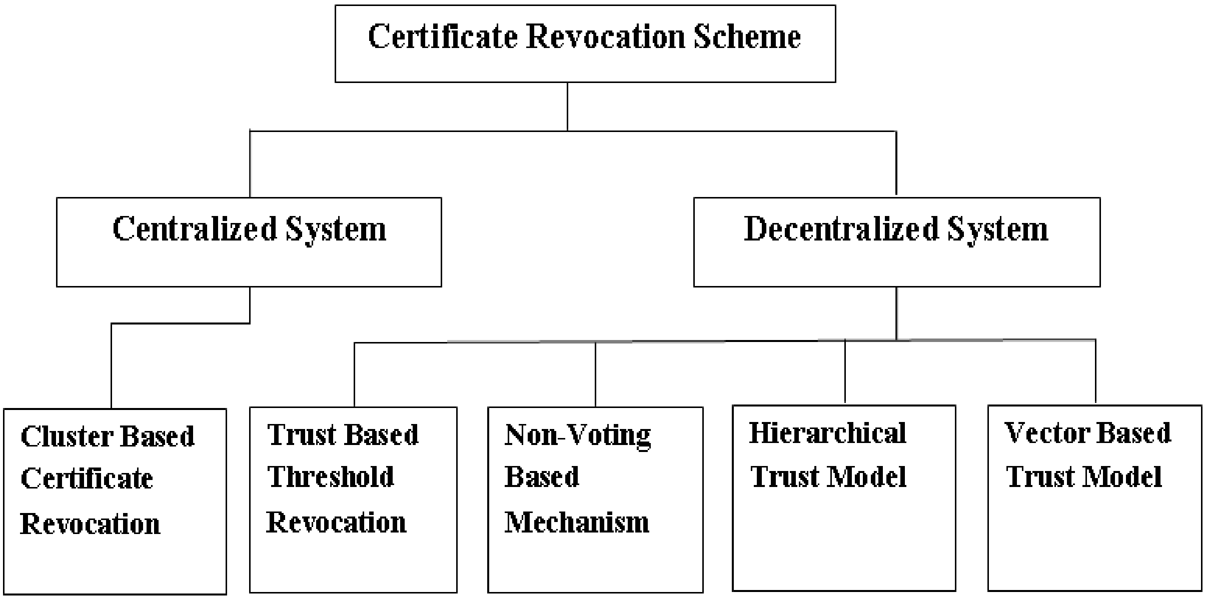
Certificate Revocation Scheme
Centralized System
Decentralized System
Cluster Based Certificate Revocation
Trust Based Threshold Revocation
Non-Voting Based Mechanism
Hierarchical Trust Model
Vector Based Trust Model

Figure 5.1 Certificate Revocation Scheme

Moreover, the integrity or confidentiality is violated when attackers track the data in the network. In general, network operation not interrupted during a passive attack; the security system in the mobile ad-hoc network is based on certificate revocation that faces a complicated task for the detection of a passive attack. Various types of methods developed to overcome the issues faced by the passive attack in MANET. The data exchanged between the nodes are encrypted by using an encryption mechanism that is the significant solution. In an active attack, the unauthorized user or malicious user affects the normal networks function. During an active attack, the data exchanged between destinations from the source in MANET could be altered or modified by the unauthorized user or malicious user. Moreover, internally or externally the active attack happens in the network. Compromised nodes perform mobile nodes launch outside attacks that belong to mobile networks and inside attacks. Notably, mobile networks have significant issues identifying interior attacks as mobile environment consist of cooperated nodes.

5.2 Related Works

In recent years, for solving security issues faced by MANET use, various security methods are identified. For mobile communication in MANET is not following any fixed structure, there is more possibility of an attack in mobile ad-hoc networks by malicious or unauthorized users. Security mechanism not only used for isolating of nodes and identifying the attack but also removes the malicious attacker from the network. Unauthorized access is performed repeatedly against the network from the malicious user or attacker that possibly could join the network. So, the required solution would be the removal of a malicious user from the network. Two types of security methods used in MANET and classified as, Authentication based security and Trust-based security. In this paper authentication, based security is mainly focused that applicable for cluster-based certificate revocation.

Table 5.1 shows recent algorithms of a certificate revocation in MANET. Fundamental control, constrained resource restrictions, and dynamic process are lacked as it followed by significant issue known to be route optimization in MANET. A considerable solution is processed by the similar objects that based on clustering nodes in which similar groups were divided from the network. In this scenario, a cluster head is selected as a node from that network. Local coordination process is provided by cluster heads essential role and doing intra and inters cluster communication and maintenance of cluster.

In general, the route information is transferred from all the nodes that present in the cluster during the route optimization procedure to the existing other nodes in the network. Moreover, for data communication, it creates high end-to-end delay, more latency and consumes energy among the nodes.

For a specific cluster, a leader selected as cluster head to overcome the issue and the information is transferred behalf of other nodes in the cluster. The end-to-end delay and cost of communication are much reduced via cluster heads communication. Also, when data communication in the mobile ad-hoc network occurs, the energy consumption even reduced by processing cluster head. A security method is presented based on certificate revocation by Lie et al. for MANET. For identifying unauthorized access or malicious user, a primary vindicate capability used in this method.

Cluster heads identification in MANET is proposed in this paper using energy efficient cluster head selection method. This method used mainly two processes namely cut back and MAP for classifying the mobile nodes. For MANET security, Jissmol Jose presented a method named clustering based certificate revocation. From this method, individual certificates are handled by the mobile node before entering into the network. For classifying malicious nodes and authorized nodes, this method transfers certificates to the cluster head. Jarang et al. based on energy consumption for clustering the nodes propose an algorithm.

The best cluster heads are identified in this paper using threshold method. Also, WSN mobile nodes used tree construction method as a classifier. Increasing lifetime is the essential goal of the proposed method for nodes present in WSN.

Similarly, a security mechanism based on certificate revocation in WSN has proposed by Park et al. for identifying false accusation.

Table 5.1 Recent Certificate Revocation Algorithms

Algorithm	Parameters	Methodology Used	Merits	Demerits
Vindication Capability in MANET	Revocation Time, Accuracy	Cluster-Based Certificate Revocation	Guaranteed secure communication with effective and efficient revocation scheme	More security attacks are possible
Secure Clustering Protocol for MANET	Successful rate, Failure rate	Secure Clustering	Network which issues false certificates encounter malicious nodes	High unreachable rate
Secure Communication Architecture for MANET	Belief value, Connectivity, stability	Secure communication-based clustering	High security to the network	Subjected to various attacks
Key Management with Authentication	Average delay, Packet delivery ratio, Maintenance cost	Encryption and Key management	Performance metrics improved	High end-to-end delay
Clustering Based Certificate Revocation in MANET	Number of nodes, node position, energy, protocol	Cluster-based Certificate Revocation	Less end-to-end delay and accurately malicious nodes revoked	The number of normal nodes reduced gradually
Cluster-Based MANETs with Threshold Signature	Performance, Security, Correctness	Threshold-based cluster signature	Privacy-preserving	Unresolved security issues

5.3 Proposed Methodology

In this paper, the proposed method for identifying malicious nodes in mobile ad-hoc networks is cluster-based certificate revocation algorithm. This proposed algorithm in MANET solves security issues. The demonstrated blocks followed by this proposed framework are cluster head selection, node classification, cluster construction, certificate revocation, certificate authority and evaluation of false accusations.

5.4 Cluster Construction

ECMS clustering algorithm is proposed in this paper for identifying cluster head in each cluster and its construction. The proposed method stands for Energy (E), Connectivity (C), Mobility (M) and Signal to Noise Ratio (S).

5.4.1 Remaining Energy

More commonly, when compared with other nodes in the networks, the residual energy must be maintained by all cluster heads (CH). Based on the difference between consumed energy and initial energy the calculation of available energy is processed. Let Ti represents the initial energy of the mobile node. The remaining energy for a node at time p is T(p) and defined by,

$$T(p) = \left(n_{pt} * x\right) + (n_{rt} * y) \qquad equation - (9)$$

Where,

$n_{pt} =$ Total no. of transmitted data packets

$n_{rt} =$ Total no. of received data packets

x, y = Constants and its range is (0,1)

In general,

Remaining Energy (E) = Initial Energy (IE) – Consumed Energy (CE)

Total Remaining Energy T_{rem} at time p is defined by,

$$T_{rem} = T_1 - T(p) \qquad equation - (10)$$

5.4.2 Connectivity

Based on the number of nodes connectivity is identified which are available for the targeted node. Two types of connectivity are classified, and these are Inter-cluster and Intra-cluster communication. The detailed information is sent by the nodes present in the network to cluster head, it is known as Intra-cluster communication. Hence, when cluster head is receiving information from sensor nodes, then all the information has been aggregated and then sent to the base station. In inter-cluster communication, the aggregated data sent by each cluster head to their neighboring cluster heads. The communication of cluster head done appropriately and aggregated data sent to the base station.

5.4.3 Expected Relative Mobility (ERM)

Based on speed and movement direction, the mobility of the node is described. The relative mobility of the host F_j at instant t is defined by,

$$RM_{(a,b)}^{t} = \sqrt[2]{(f_a^t)^2 + (f_b^t)^2 - [2 f_a^t f_b^t \cos(\Theta_a^t - \Theta_b^t)]} \quad equation - (11)$$

Where,

f_b^t = denoted as the speed of the Host F_j (node)

Θ_b^t= denoted as the movement direction of the Host F_j (node)

In general, different epochs varied by relative mobility. Hence, appropriate mobility parameter could not identify by this from the node. Expected Relative Mobility (ERM) calculated for identifying this mobility of the node over different epochs. The calculation of ERM is between two hosts T_i and T_j by

$$ERM_{(i,j)}^{t} = \frac{1}{k} \sum_{t=1}^{k} RM_{(i,j)}^{t} \qquad equation - (12)$$

Where,

T = Represents the time

k = Represents the number of epochs

5.4.4 Signal to Noise Ratio (SNR)

Level of contextual noise represents by SNR to the level of the preferred signal. For calculating SNR of the node is given based on the formula,

$$\mathrm{SNR} = 10\log_{10}(\frac{Z^2}{MSE}) \qquad equation-(13)$$

Where,

Z = represents the maximum fluctuation among the nodes

MSE = Mean Square Error

The combination of Energy (E), Connectivity (C), Mobility (M) and Signal to Noise Ratio (S) to computing the weight for the node. The weight ‘Q’ is defined by,

$$Q = q_1 * E + q_2 * C + q_3 * M + q_4 * S \qquad equation-(14)$$

Where,

E = Energy

C = Connectivity

M = Mobility

S = Signal to Noise Ratio

The weight q1, q2, q3, and q4 vary the range between 0 and 1. These weights are used for finding cluster heads.

5.5 Cluster Head Selection

Nodes present in the cluster are compared with each node with calculated weights. Weights select the optimal node as a cluster head. The selection steps for cluster head is summarized as follows:

Algorithm 1: Certificate Revocation

Step 1: The neighborhood table is updated by finding neighbors for each node

Step 2: The weight ‘Q’ computed by each node based on Energy (E), Connectivity (C), Mobility (M) and Signal to Noise Ratio (S) as mentioned.

```
Step 3:  The value of weight ‘Q’ broadcasts by each node to its neighbors.
Step 4:  If (weight ‘Q’ of node ‘X’ > weights of all neighbors)
         {
             Node ‘X’ declare as a cluster head
         }
Step 5:  The cluster head information broadcast by node ‘Q’ to all nodes that exist in
         the network.
Step 6:  End for
```

5.6 Certification Authority

Black List (BL) and Warning List (WL) are two lists present in certificate-based revocation. Based on the information of accused nodes the updating of WL lists is continuous. But, for BL lists the accusation information is updated. Storing of detailed information regarding the attacker is the essential role of BL while WL maintains complete details continuously about the accusing nodes. For updating the CA, control packets are monitored when transmitting between the nodes. The entire network specified by particulars of WL and BL when updating task of CA is completed. The certificates of sensor nodes are revoked which are present in the BL is the leading role of this specified messages.

5.7 Node Classification Based on Reliability

Three types of sensor nodes classification present in the network: normal node, revoked node and warned node.

5.7.1 Normal Node

The normal nodes do not perform any attacks instead it only joins the network during its lifetime. Also, when compared with other nodes in the network, the normal node is considered high reliability. Moreover, accused nodes can be identified by the normal nodes and declare itself as a cluster head.

5.7.2 Warned Node

Warned nodes are considered when nodes are stored in warning list. Also, low reliability occurs when compared with other nodes in the network. Since the mixture of a few genuine nodes and malicious nodes are present in warning list, so these nodes are suspicious. However, the encouragement for communication of warned nodes with other nodes occurs that exist in the network. Moreover, depending upon the malicious behavior level, with a threshold value, the communications are restricted.

5.7.3 Revoked Nodes

The storing of nodes in the blacklist is considered as revoked nodes. However, it is considered to be low-reliability nodes. Also, it consists of the malicious certificate that found to be malicious attackers which disposed of the network.

5.8 Certificate Revocation Procedure

In Certificate Revocation Procedure, one-hop neighbors help to monitor each node present in the network. Malicious information about the sensor nodes is collected by using this one-hop neighbor. The malicious activity started by the sensor nodes, the certificate revocation process is started. Normal nodes check certificate Revocation List (CRL) for the presence of neighboring node included in CRL or not.

Based on the certificate issued the neighboring node identifies as malicious then it revoked from the network and harmful attacks are not performed by this node in future. The neighboring node transferred to Accusation Packet (AP) if it identified to be legitimate node based on its certificate from source to corresponding gateway node in the network.

Accuser’s certificate of the sensor node is checked by gateway node once this node receives the AP. In other words, accusation list stores the AP if the valid certificate of gateway identified during the checking process. Accordingly, it updates the details of the accuser and accused node. Figure 5.2 shows the representation of the workflow.

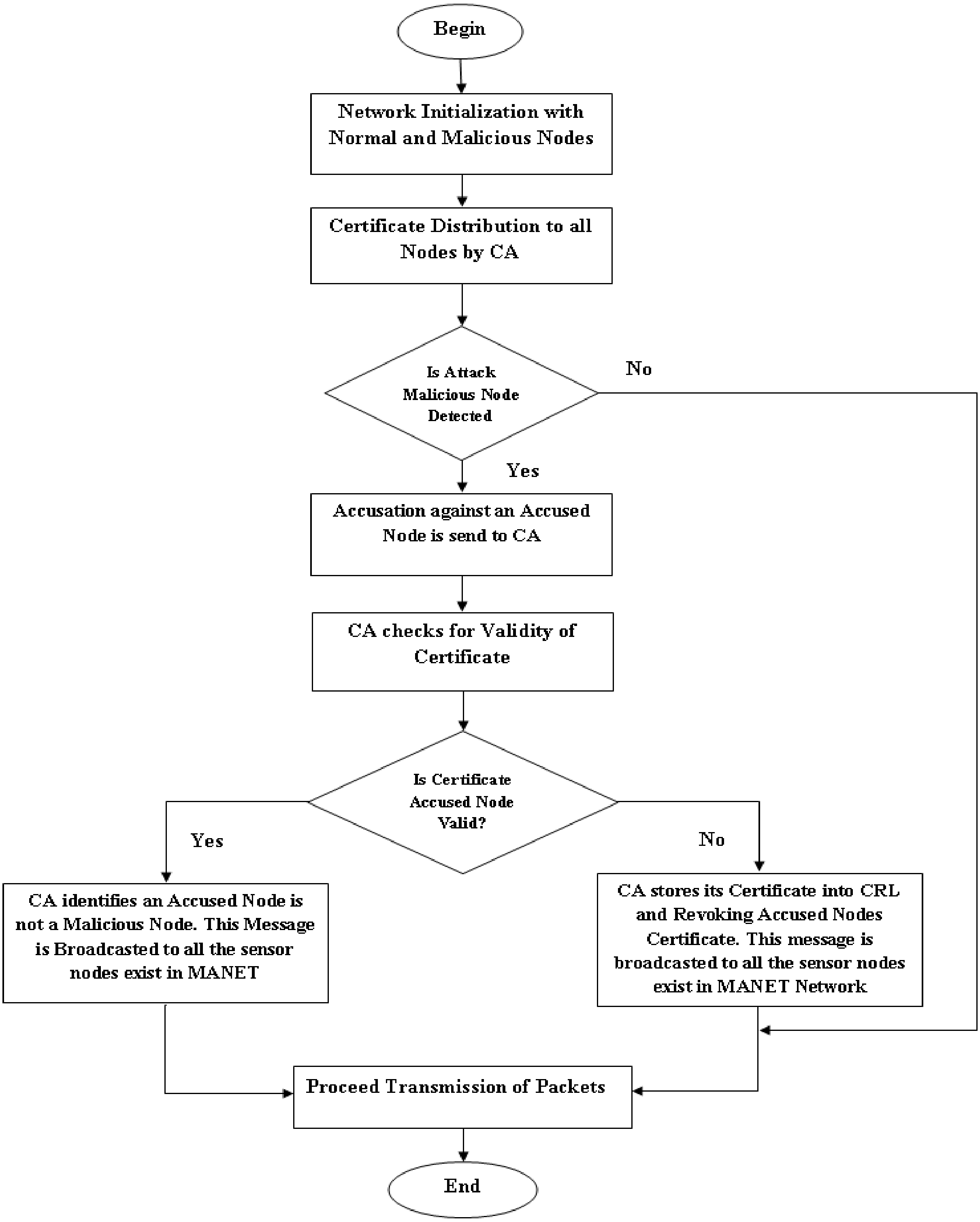
Begin
Network Initialization with Normal and Malicious Nodes
Certificate Distribution to all Nodes by CA
Is Attack Malicious Node Detected
No
Yes
Accusation against an Accused Node is send to CA
CA checks for Validity of Certificate
Is Certificate Accused Node Valid?
Yes
No
CA identifies an Accused Node is not a Malicious Node. This Message is Broadcasted to all the sensor nodes exist in MANET
CA stores its Certificate into CRL and Revoking Accused Nodes Certificate. This message is broadcasted to all the sensor nodes exist in MANET Network
Proceed Transmission of Packets
End

Figure 5.2 Workflow of Certificate Revocation

Algorithm 2: Certificate Revocation

```
Step 1:  Detect malicious activities of node N by neighboring nodes $M_i$ ( i = 1, 2,
         3…, M )
Step 2:  Casts an Accusation Packet (AP) against node N
Step 3:  AP broadcasts to gateway G
Step 4:  Store and verify the accusations in the waiting list of gateway G based on
         arrival time (AT)
Step 5:  if (waiting list == NULL)
         {
                 Go to the last step
         }
         else
         {
             Verify the earliest arrived accusation by gateway G supposing
         made by node ‘w’
         }
Step 6:  Update $a_w$ and $A_n$ by gateway G
             #$a_w$ = total number of accusations made by node ‘i’
             # $A_n$ = total number of accusations made against node ‘i’
Step 7:  Calculate accusation weight of node w and n
                         $X_w = 1 - \lambda A_n - \lambda a_n$
         Where,
         $\lambda = \frac{1}{2}(M - 1)$ N represents the number of nodes
Step 8:  if $(X_w > X_m)$
         {
             Go to Step 9
         }
         else
         {
                 Repeat Step 5 to Step 8
         }
Step 9:  Gateway G clears the waiting list (WL), and malicious node ‘m’ and
         added to CRL; revocation details broadcast to the network; $a_i$ update as
         minus one for every successful accusing node ‘m’.
Step 10: Based on received revocation information each node updates its local CRL
         in the network.
```

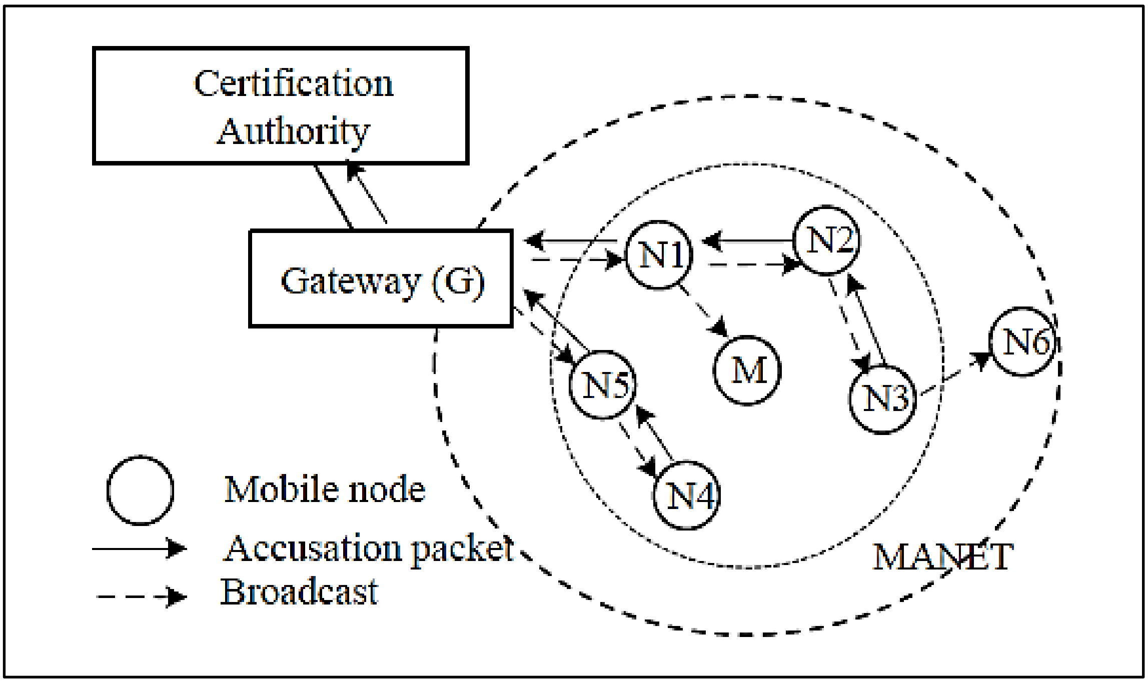

Figure 5.3 Revoking a Node's Certificate

Simple certificate revocation procedure is shown in figure 5.3. When network attacked by the malicious node M, then malicious activities are detected by neighboring nodes N1, N2, N3, N4, and N5.

5.9 Evaluation of False Accusations

In general, malicious nodes against legitimate nodes make false accusations. The legitimate node weight reduced when false accusation accepted by the gateway against the legitimate node. So this would be affected by revoking the certificate of the malicious node. Also, revoking the wrong legitimated node will lead to high risk. Hence, based on the accusation message the node identifies to be malicious node then the information broadcasted by gateway G to each node present in the network. Thus, based on broadcast information, the values of local CRL are updated for each node as shown in figure 5.4. The Vindication Packets (VP) are sent to appropriate gateways when wrongly identify the node as malicious for correcting the mistake. Malicious node changed as a legitimate node by the gateway when the number of VPs exceeded the threshold value.

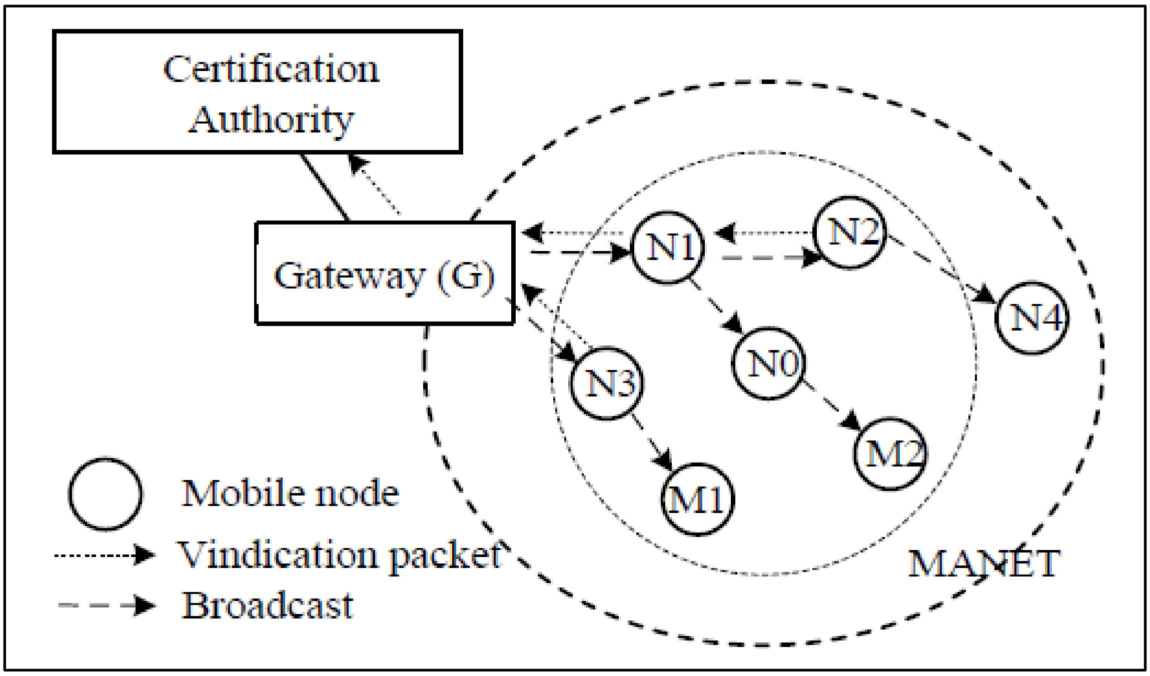

Figure 5.4 Recovering a Wrongly Revoked Node

Algorithm 3: Managing the False Accusations

```
Step 1:  If node (N0) certificate is revoked
Step 2:  This information transmitted by gateway G to every node in the network
Step 3:  If normal nodes detect N0 wrongly
Step 4:  number of VPs count by gateway G
Step 5:  If (Threshold < Total number of VPs)
         {
                Certificate of N0 recovered
                N0 declare as normal node
         }
         else
         {
```

```
        Certificate of N0 not recovered
        N0 declare as malicious node
    }
```

5.10 Performance Evaluation

The evaluation of proposed cluster-based certificate revocation method and the performance based on various parameters that include, Settling Time (ST), Packet Delivery Ratio, Successful Certification Ratio (SSR), Average Certification Delay (ACD), End-to-End delay, Throughput and Normalized Overhead.

5.10.1 Settling Time (ST)

For issuing a valid certificate to the nodes in the network, ST represents the time taken for it. The algorithm of pre-authentication techniques and the number of malicious nodes uses key generation method that dependable by Settling Time.

5.10.2 Packet Delivery Ratio

The ratio of the total number of packet sent and the number of packets successfully delivered is used for computing PDR. It is defined as,

$$PDR = \frac{Packets\ Delivered}{Packets\ Sent} \qquad equation - (15)$$

5.10.3 Successful Certificate Ratio (μ)

The ratio of the number of successful certification services to the total number of request for that services. This calculation is represented as SSR.

$$\mu_{REN} = \frac{NC_{REN}}{NC_{TOT-REN}} \qquad equation - (16)$$

$$\mu_{ISS} = \frac{NC_{ISS}}{NC_{TOT-ISS}} \qquad equation - (17)$$

Where,

NC_{REN} = represent renewed certificate count

NC_{ISS} = represent issued certificates total count

$NC_{TOT-REN}$ = represents certificate issuance request total count

$NC_{TOT-ISS}$ = represents certificate renewal request total count

5.10.4 Average Certification Delay (ACD)

The delay among the certificate service request (CSReq) and certificate service reply (CSRep) used for calculating ACD that averaged over the specific period. It is defined by,

$$ACD = \frac{\sum_{i=1\dots n}(CSRep_i - CSReq_i)}{R_{int}} \qquad equation - (18)$$

5.10.5 Average End-to-End Delay (EED)

The calculation of EED is based time taken for routing a packet from client to server. It is represented as,

$$Average\ EED = \frac{1}{q}\sum_{i=1}^{q} Delay(i) \qquad equation - (19)$$

Where,

q = total number packets received

Delay (i) = time difference

5.10.6 Throughput

Throughput defines the average of delivered data packets to destination per second. It defined as,

$$Throughput = \frac{No.of\ sent\ packets}{Taken\,Time} \qquad equation - (20)$$

5.10.7 Normalized Routing Overhead (NRO)

NRO represents the ratio between number of data packets and number of control packets and as follows,

$$NRO = \frac{No. of\ Control\ packets}{No. of\ Data\ packets} \qquad equation - (21)$$

5.11 Summary

For solving the security issues in mobile ad-hoc networks this proposed method, ECMS cluster head is used based on certificate revocation method. This technique helps to isolate the malicious node and protect the unauthorized access to the network. The classification of ECMS cluster head is presented as, cluster construction, certificate authority, cluster head selection, certificate revocation, evaluation of false accusation and node classification. The proposed algorithms categorize sensor networks into three types these are normal, warned and revoked node. For revoking certificates malicious node, we combine voting and non-voting based algorithm and solve false accusation of the legitimate node. The simulation and performance of the proposed algorithm proved to perform well.