ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2017.0215

CERTIFICATE REVOCATION SCHEME BASED ON WEIGHTED VOTING GAME AND RATIONAL SECURE MULTIPARTY COMPUTING

N. Aravinthan[1] and K. Geetha[2]
Department of Computer Science, Bharathiar University, India

Abstract

The Mobile Adhoc Network consists of deployed mobile nodes which lead to the frequent changes in network topology. Due to topology changes, required infrastructure is unavailable for communication. Moreover, malicious nodes present in MANET make use of this modification and can easily launch highly vulnerable attacks on the routing path of the network. Hence, Security issue such as removing misbehaving nodes is the primary issue in MANET. Effective certificate revocation scheme was introduced to identify and eliminate the node with malicious activities in the network based on the weighted voting game (ECR-WVG) approach. In this approach, weights and quota were two factors, determined for an effective revocation of malicious nodes certificates. However, security during multiparty transmission was not taken into account in ECR-WVG. In Effective Certificate Revocation Scheme based on Weighted Voting Game and Rational Secure Multi-Party Computing (ECR-WVG-RSMPC) method, rational secret sharing scheme is introduced along with ECR-WVG approach for securing multiparty transmission. Performance evaluation can be done between ECR-WVG and ECR-WVG-RSMPC in terms of false revocation, malicious node revocation, normalized time for revocation and revocation accuracy ratio.

Keywords:

Mobile Adhoc Network, Network Topology, Certificate Revocation Scheme, Weighted Voting Game, Multiparty Transmission

1. INTRODUCTION

MANET is an infrastructure less network consists of self configuring mobile devices which can move independently in any direction and leads to frequent modification in the transmission links with respect to other devices. One of the limitations in MANET is malicious nodes present in the network. Such nodes can easily corrupt the data in the routing path and finally resulted in malfunctioning of the network operations. Some of the malicious attacks launched in the network corrupted the information that is transmitted among nodes while other attacks might attempt to change the path that they are transmitted to prevent valid node to receive the correct packets. So, security is considered as an important concern in network topology, routing, and data traffic. Many research works have focused on the security of MANETs.

Certificate management mechanism [1] is developed in which trust values are used for providing protected services in the network and applications of network. Components like Prevention, Detection, and revocation are the security solutions utilized for certificate management. The task of adding and removing the certificates of attacks launching nodes is called certification revocation scheme. This revocation scheme has performed under voting based and non-voting based mechanism.

In voting mechanism, certificate of attacker nodes was revoked based on the votes given by its non attacker neighboring nodes and the latter mechanism consider a given node as malicious attacker with a help of any other node having valid certificate. Thus the certificate of malicious nodes was detected and malicious nodes were removed from the network. But security during multiparty transmission was not considered by this certificate revocation scheme. Hence, in our proposed scheme, rational secret sharing scheme [2] is utilized for improving security for multiparty communication.

The main focus of this paper is to increase the security level of ommunication using RSS in addition with accurate detection and removal of malicious nodes from the network using WVG.

2. LITERATURE SURVEY

Arboit et al. [3] presented a decentralized scheme for revoking the certificates of misbehaving nodes based on weighted accusations. The proposed system utilized certificates with respect to the hierarchical trust model and also hand over all key management tasks to all nodes. This scheme found the malicious nodes at a faster rate and revoked their certificates. No guarantee for revocation of malicious nodes.

Ayyasamy and Subramani [4] utilized the certificate authority with trust counters for providing integrity of the network along with resisting attacks. It is a three phase scheme that consists of RCF of packet monitoring, Certification revival and Certification revocation. RCF of packet monitoring detected the misbehaviour in both the routing as well as the packet forwarding in the network, Certification revival and Certification revocation provide privacy for each node by using Shamir's secret sharing model with redundancy. This scheme results with less delay and overhead. Flexibility is low while controlling and configuring certificates.

Liu et al. [5] proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme for accurate detection of malicious nodes. In this scheme, cluster head solves the false accusation problem by restoring the falsely revoked nodes. CCRVC revoke the attacker nodes by considering only one accusation from a neighboring node. This scheme minimizes the revocation time. The scheme supports only uniformly distributed mobile nodes.

Raj and Kathare [6] introduced the clustering concept in certificate revocation to reinforce an idea for MANET for being able to revoke attacker certificate and to recover falsely accused certificate. The proposed scheme can quickly revoke the malicious device certificate, stop the device access to the network and improves the network security. The loss of energy depends on the number of rounds. But it was unable to recover after corruption.

Xu et al. [7] proposed a lightweight scheme for revoking the certificate of nodes in hybrid mobile Adhoc network to achieve

better efficiency and reliability. The proposed scheme utilized the advantages of voting based mechanism for allowing few nodes to involve in the revocation process for ensuring reliability. Acceleration strategy was proposed to reduce the number of voters required to revoke a certificate. This scheme also provides vindication capability to handle with wrong certificate revocation. If the number of recovery packets exceeds a predefined number, the wrongly revoked node will be removed from Certificate Revocation Lists (CRLs).

Raya et al. [8] proposed three protocols for effective certificate revocation in vehicular networks. First protocol was designed to perform certificate revocation in poor coverage condition. The second protocol was designed based on the storage and trusted processing which focussed on revoked nodes. Third protocol was designed to detect the malicious nodes and avoids malicious attacks. Limited performance was resulted due to the absence of the attacker detection system.

Panke [9] reviewed the revocation scheme in which two nearby nodes received their certificates from each other and share the information about other nodes certificates. Nodes sharing same certificate information belonging to the same network. In such networks, the accused node certificate was revoked when the number of accusations against accused node was greater than the certain threshold. But the operational cost is still high.

Clulow and Moore [10] presented time session for revitalizing the information of certificate of each node. Accusation count was reset at the end of each session. Thus, when the scheme was able to prevent the damage caused by false accusations, the performance can be degraded maximum by the increase of malicious nodes.

Srividya et al. [11] reviewed various certificate revocation mechanisms used in MANET. In this review, clustering technique was used for certificate revocation. The Threshold based mechanism was also provided for recovering the accusation function of nodes in the warning list. The nodes detected as the attackers were completely removed from the network. Modification in revoked certificates resulted in computational complexity.

Luo et al. [12] developed the scheme in which the nodes certificate which was accused by almost one node will be revoked by every node. The proposed scheme shows good performance with respect to promptness and low operating overhead. However, this scheme creates a controversial point where an accuser node will be removed from the network along with the accused node. The proposed approach was fundamentally inconsistent; hence this scheme was not commonly used.

3. EFFECTIVE CERTIFICATE REVOCATION SCHEME BASED ON WEIGHTED VOTING GAME AND RATIONAL SECURE MULTI-PARTY COMPUTING (ECR-WVG-RSMPC)

ECR-WVG is a game theory based mechanism used in MANET to identify the certificate of malicious nodes with the help of Certificate Authority (CA). In cluster based adaptive revocation mechanism, nodes are grouped into clusters according to their transmission range and corresponding cluster head (CH) is selected for forwarding the information. Each node has its own detection mechanism to find the misbehavior activities of its nearby nodes with one hop.

3.1 CRYPTOGRAPHY

The method of transforming plain intelligible text into an unintelligible (cipher) text and again retransforming that ciphered data to its original form is known as cryptography. This method provides integrity, confidentiality and accuracy. There are two types of cryptographic methods namely symmetric key cryptography method (secret key cryptography) and asymmetric key cryptography method (public key cryptography). In the former method, parties involved in communication uses same key while in the latter method two different keys distributed by Certificate Authority (CA) are used by the parties. In our proposed method, we are using private key cryptography because of its authenticated and highly secured nature.

3.3.1 Encryption:

In our proposed system, meaningful or meaningless encryption is utilized as cryptographic tool for protecting the information. In this cryptography method, plain text is transformed into cipher text using public key and the ciphered information cannot be decoded. Public key used for this type of encryption is referred as meaningless secret key (x_{mf}). Keys other than this public key are referred as meaningful secret key (x_{ml}) and these secret keys are essential for providing semantic security. Thus, Secret key should be issued to all parties (nodes) at the beginning of Weighted Voting Game (WVG) theory approach for separating x_{mf} and x_{ml}. Action of each player participated in voting process is decided by interactive Turing machine (ITM) and it gets the input which contains current state information and incoming messages from other parties and produces the output message of particular player with updated state. Then the new message with secret key is forwarded to other parties.

3.3.2 Game Theory:

The Weighted Voting Game (WVG) model is then adapted in order to identify and remove certificates of malicious nodes in each cluster. The purpose of implementing WVG model is to manage the attacks of malicious nodes on data. Six parameters such as players (P), a strategy set (pro-vote (P_v) and con vote (C_v)) for each player, consequences of the strategies (C), quotas (Q), players' voting weights (W), and the characteristic functions ($cf(.)$) are utilized for designing WVG model. Weight of the node can be estimated based on node's reliability and its behaviour history. Node's reliability ($R_i(t)$) is given by the amount of P_v and C_v that are acquired from the previous activity information of node and it is denoted by,

$$R_i(t) = \frac{a_t^i}{a_t^i + b_t^i} \tag{1}$$

where, a_t^i meant for the amount of P_v acquired after each successful accomplishment of revocation. b_t^i meant for total amount of votes without a_t^i.

Past behavior of each node (Pbh_i) is calculated by,

$$Pbh_i = \frac{1}{1+\left[aF^1(i) + bF^2(i)\right]} \tag{2}$$

such that, $F^1(i) = \eta_i/s$ and $F^2(i) = \psi_i/s$, where,

S represents the sum of accusation numbers of all nodes present in the cluster.

η_i represents the accused number of particular node obtained from other nodes.

ψ_i represents the number of times the node is accused but not revoked.

W is calculated based on R and Pbh_i. If any new node joins in the network, its W should be greater than 0. W should maximize at the beginning as fast as possible. Weighted value of node i at time t is given by,

$$W_i^t = \frac{\ln\left(\left[R_i(t) + Pbh_i\right] \times \left(c_i - M_i / m_i - M_i\right) + \gamma\right)}{\ln\left(\left[R_i(t) + Pbh_i\right]\right) + \gamma} \quad (3)$$

Such that,

$$\begin{cases} m_i = \sup\left(R_i(t) + Pbh_i\right) \\ M_i = \inf\left(R_i(t) + Pbh_i\right) \\ c_i = R_i(t) + Pbh \end{cases} \quad (4)$$

where,

γ represents the impact factor

sup(·) represents the supremum functions

inf(·) represents the infimum functions

Fixed value of Q does not support the dynamically changing network environment. Hence iterative learning technique is used for adjusting the Q value. In our proposed work, Quota value Q at time t is assumed to be,

$$Q^t \in \Gamma_Q = \{0.1\mu, 0.2\mu, 0.3\mu, 0.4\mu, 0.5\mu\} \quad (5)$$

where, Q^t represents the quota value that was selected at time t.

$$\mu = \sum_{i \in n} W_i \quad (6)$$

where, n represents the set of nodes in particular cluster.

CH selects Q^t at each t and determine its incentive $i(Q^t)$ as follows,

$$i\left(Q^t\right) = \frac{u\left(Q^t\right) - S}{\sup_{T \in \Gamma_Q} \left|u(T) - S\right|} \quad (7)$$

such that, $T \in \Gamma_Q$ and $i(Q^t) \in [-1, 1]$.

where, $u(Q^t)$ represents the normalised throughput of correspon ding cluster with Q^t. S represents the normalised aspiration performance level of CH. Selection probabilities $p\left(P_S^{t+1}\left(Q^t\right)\right)$ of each strategies of CH at time t+1 are updated by,

$$PP_s^{t+1}\left(Q^t\right) = \begin{cases} \min\left[\begin{array}{l} p\left(P_S^t\left(Q^t\right)\right) + \xi \times i\left(P_S^t\left(Q^t\right)\right) \times \\ \left(1 - p\left(P_S^t\left(Q^t\right)\right)\right), 1 \end{array}\right] & \text{if } i\left(Q^t\right) \geq 0 \\ \min\left[\begin{array}{l} p\left(P_S^t\left(Q^t\right)\right) + \xi \times i\left(P_S^t\left(Q^t\right)\right) \times \\ \left(p\left(P_S^t\left(Q^t\right)\right)\right), 0 \end{array}\right] & \text{if } i\left(Q^t\right) < 0 \end{cases} \quad (8)$$

$$p\left(P_S^{t+1}(\pi)\right) \frac{p\left(P_S^t(\pi)\right)}{\sum_{\varphi \in \Gamma_Q} p\left(P_S^t(\varphi)\right)} \text{ such that } \pi \neq Q^t \in \Gamma_Q \quad (9)$$

where, ξ ranges from 0 to 1.

Based on this iterative strategical result, Q value in each cluster dynamically changes for obtaining best result of Q and CH increases the performance of the system to the local optimal.

For detecting the malicious nodes by WVG, CH transmits the accusing message to other nodes in the cluster. Then voting procedure is followed by each node to confirm whether the accused node is malicious or not. The votes are collected by CH and they are forwarded to the CA (certificate authority) to verify the certificate validation of the accused node. The verification is based on the receiving quotient $r_{qi}(t)$, which is computed by,

$$r_{qi}(t) = \sum_{j=1, j \neq i}^{m} \left(\delta_{ji}(t) \times W_j^t\right) \text{ such that } i, j \in n \quad (10)$$

Certificate status of nodes is determined based on Q and $r_{qi}(t)$. When $Q \leq r_{qi}(t)$, then it represents the successful revocation of certificate of node. Based on CA decision, revocation message is broadcasted to other nodes in the cluster by CH and leads to reliability changes. This certificate revocation mechanism addressed the problem of false revocation. If a node revocation occurs, then the false accused node requests for recovering its certificate. After receiving the request, petition message is sent by CH to all nodes to check whether previous revocation is correct or not. If $r_{qi}(t) < Q$, then the accused node is successfully restored again. After detecting the malicious nodes, encrypted message is shared over the network.

In order to secure the shared message, Rational Secure Multi Party Computing (RSMPC) protocol is developed in which nodes are assumed as rational parties. In general, RSMPC is performed under Rational Secret Sharing (RSS) scheme. RSS shares the secret by m out of n secret sharing scheme where m represents the threshold of shares. If a party consists of m shares, then it gains the secret by utilizing those m shares. Thus, four conditions associated with secret sharing scheme are given as follows:

If all parties P are ready to exchange their shares to other parties, then P can easily gain the secret.

If one party P_i exchanges its share and not receiving any shares from other parties, then P_i cannot gain the secret.

If none of the parties exchange their shares, then no secret will be gain, which leads to selfish assumption.

If a party P_i exchanges its shares to others and not receiving sufficient shares from others, then other parties except P_i can able to gain the secret, which leads to exclusivity assumption.

In our proposed system, RSS considers three parties P_1, P_2, P_3 and undergoes 3 out of 3 Shamir secret sharing scheme. Initially, random strings are generated and they are partitioned into n shares. It should be noted that, input message is different from randomly generated strings.

By using meaningful or meaningless encryption protocol, random strings except an original message are encrypted. Then, for securing input message, steps mentioned below should be performed.

3.3.3 Steps involved in RSS:

i. Each party P_i selects one bit b_i either 1 or 0 with probability β or 1-β.

ii. Meanwhile Same Party P_i selects another random bit $b_{(i,+)}$ as 0 or 1 with probability ½.

iii. Consider $b_{(i,-)} = b_i \oplus b_{(i,+)}$.

iv. Party P_i transmits $b_{(i,+)}$ to P_{i+1} party and $b_{(i,-)}$ to P_{i-1} party.

v. Each party P_i transmits $b_{(i+1,-)} \oplus b_i$ to P_{i-1} and P_{i+1} transmits $b_{(i-1,-)} \oplus b_{i+1}$ to P_i.

vi. Probability p is calculated by each party P_i using, $p = b_1 \oplus b_2 \oplus b_3$.

vii. If $p=b_i=1$, then party P_i transmits its shares to other parties.

viii. If $p=0$ and P_i does not receive any share or $p=1$ and P_i receives only one share, then the share is belonged to that ith party which means that P_i does not receive any shares from other parties.

ix. If P_i does not receive any share from others then the secret dealer should restart the protocol.

Thus, Protocol can abort either receiving all shares or detecting any malicious activities.

3.3.4 Decryption:

After successful transmission of message among multiple parties, decryption is adopted. If a party that receives a transmitted message has meaningful secret key, then random strings and input message are only revealed to that particular party. Random strings are reconstructed by decrypting the ciphered information using meaningful secret key. On the other hand, if a receiver party has meaningless secret key, then random strings and input message are not revealed even to that particular party. Thus, effective communication is maintained with the help of both WVG and RSMPC.

Table.1. Comparison Table of ECR-WVG and Hybrid ECR_WVG_RMPC with cryptography

Terms	**ECR-WVG**	**ECR_WVG_RMPC with cryptography**
Methods	Clustering of nodes and Weighted Voting Game theory for detecting malicious nodes	Clustering of nodes, Cryptography, Weighted Voting Game theory for detecting malicious nodes and Rational Secret Sharing for securing communication among Multi parties
Percentage of malicious node revocation (%)	92	98
Percentage of false revocation (%)	40	33
Normalized time to revocation (ms)	300	150
Revocation accuracy ratio	92	99
Merit	Detect and revoke the malicious nodes effectively	Not only remove the malicious nodes from the network but also provides high security on multiparty communication
Demerit	Does not provide security to multiparty communication	-

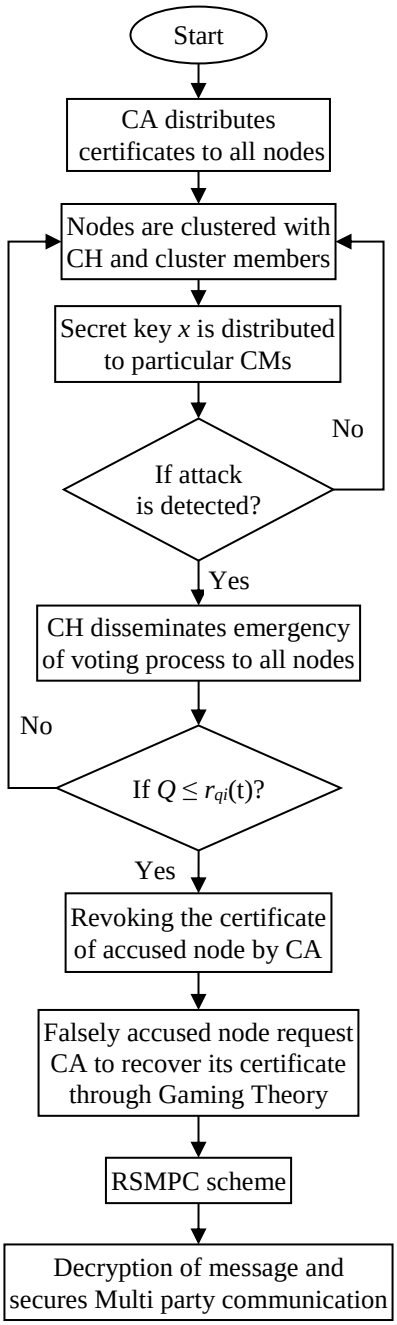

Fig.1. Flow diagram of proposed system

3.2 ALGORITHM OF PROPOSED SYSTEM

1. Forming network with normal nodes and malicious nodes
2. Certificates are distributed to all nodes by CA
3. Cluster formation which includes CH and CMs
4. Select CH for each cluster
5. Assign authorities of CA to each CH

6. Secret key x is distributed to the nodes in a cluster for encrypting the input message by cryptographic protocol before performing the game theory.
7. If malicious attack is detected, a message regarding voting process is then forwarded from CA to all nodes in a respective cluster
8. Weight (W) of suspected node (3) is then calculated by reliability of node $R(t)$ and its past behaviour history pbh using Eq.(1) and Eq.(2)
9. Estimate the value of quota (Q) to revoke the certificate using Eq.(5)
10. Estimate Incentives at time t and selection probabilities of Q at time t+1, $i(t)$ and $p\left(P_S^{t+1}\left(Q^t\right)\right)$, using Eq.(7) Eq.(8) and Eq.(9)
11. Estimate receiving quotient $r_{qi}(t)$ using Eq.(10)
12. If ($Q \leq r_{qi}(t)$), then certificate of suspected node is successfully revoked and it is added to CRL
13. If a node is falsely accused, then CA sends the petition message to all nodes to verify the revocation of previous node
14. Now if, condition $r_{qi}(t) < Q$ is satisfied, then the suspected node is confirmed to be non malicious node and it is again restored in the network
15. After revoking the certificates of malicious nodes, RSMPC is adopted for securing multi-party communication
16. Each node in transmission route is considered as rational party
17. Communication between rational parties are done with the secret sharing scheme
18. Secret dealer gives one share for each party
19. Follow the steps from 1 to 10 of RSS scheme
20. Obtain the final list of malicious nodes and successfully maintains the secured communication among multi parties.

4. EXPERIMENTAL RESULT

In this section, results obtained from NS2 simulation are briefly explained. In our experiment, we are using 100 nodes and these nodes are randomly placed over the network with respect to X axis and Y axis. For example, first node '0' is plotted at the X axis value of '80' and Y axis value of '80'. The way of placing nodes are shown in the Fig.2.

The Fig.3 shows the diagram representation of the node placement in network. Here, nodes are placed as per the values given in X axis and Y axis. Node's numbers are also specified at the middle of each node.

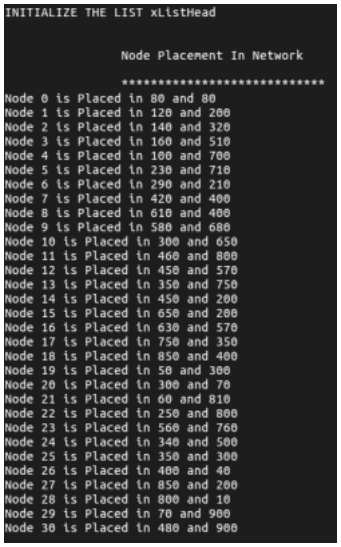

Fig.2. Node placement in network

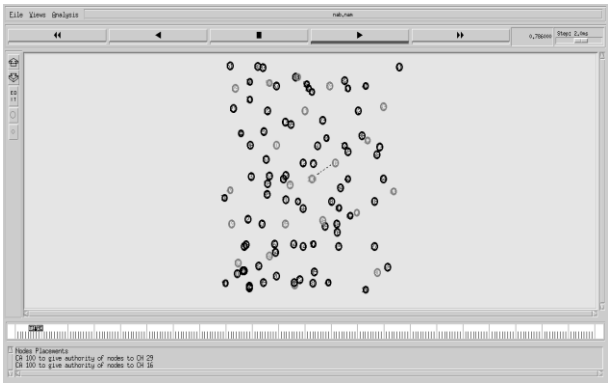

Fig.3. Diagram representation

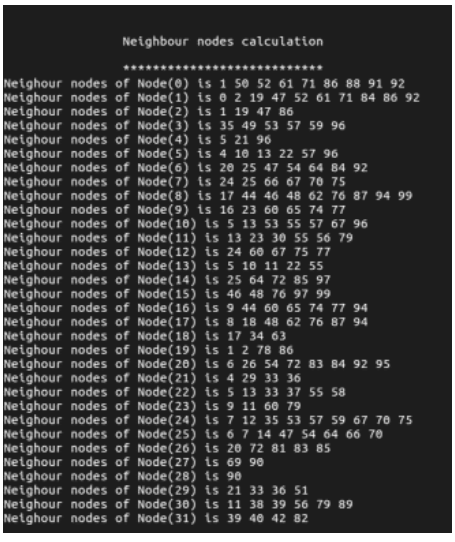

Fig.4. Neighbour node calculation

After node displacements, distributed nodes have to be clustered before entering into the communication process. For clustering of nodes, it is necessary to calculate the neighbouring nodes of each node based on their location or position and the result obtained is shown in Fig.4. For example, nodes 1, 50, 52,

61, 71, 80, 88, 91 and 92 are found to be the neighbouring nodes of node '0'.

```
Cluster formation

CH-29   clusters are 21 33 36 51 4
CH-16   clusters are 9 44 60 65 74 77 94
CH-83   clusters are 20 26 72 81 85 45
CH-10   clusters are 5 13 53 55 57 67 96
CH-25   clusters are 6 7 14 47 54 64 66 70
CH-19   clusters are 1 2 78 86
CH-49   clusters are 3
CH-58   clusters are 22 37 80 93
CH-38   clusters are 30 56 79 89
CH-75   clusters are 12 24 35 59
CH-32   clusters are 42 68 73 98
CH-52   clusters are 0 50 61 71 88 91 92
CH-63   clusters are 18 34
CH-39   clusters are 31 82
CH-11   clusters are 23
CH-90   clusters are 27 28 69
CH-46   clusters are 8 15 48 76 87 97 99
CH-84   clusters are 95
CH-43   clusters are 40
CH-17   clusters are 62

Authority Center send information about nodes to CH


Enter Source node between 0~99
20

Enter Destination node between 0~99
30

Source and Destination communication path is 20 6 25 7 67 10 55 11 30


Enter the text to be sent
hello
```

Fig.5. Cluster formation

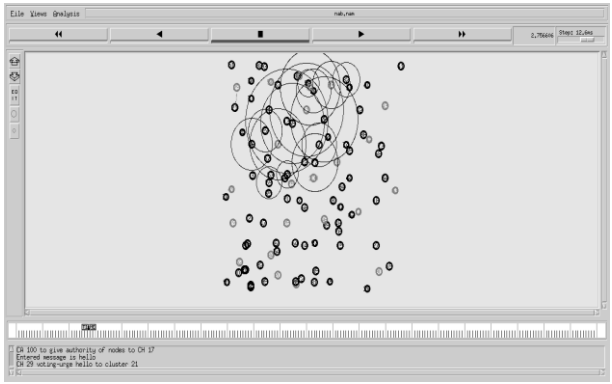

Fig.6. Cluster formation Diagram

```
hello
9 should not communicate with other nodes
26 should not communicate with other nodes
96 should not communicate with other nodes
6 should not communicate with other nodes
78 should not communicate with other nodes
61 should not communicate with other nodes
69 should not communicate with other nodes
15 should not communicate with other nodes
95 should not communicate with other nodes

Malicious nodes are 6 96 9 15 26 78 61 69 95

Reliability value of 6 is 0.14285714285714285
Reliability value of 96 is 0.0
Reliability value of 9 is 0.5
Reliability value of 15 is 0.20000000000000001
Reliability value of 26 is 0.40000000000000002
Reliability value of 78 is 0.0
Reliability value of 61 is 0.20000000000000001
Reliability value of 69 is 0.0
Reliability value of 95 is 0.5


Behaviour history of node 6 is 0.085365853658536578
Behaviour history of node 96 is 0.0065298507462686565
Behaviour history of node 9 is 0.0608695652173913
Behaviour history of node 15 is 0.038674033149171262
Behaviour history of node 26 is 0.022508038585209004
Behaviour history of node 78 is 0.0080091533180778017
Behaviour history of node 61 is 0.0096818810511756555
Behaviour history of node 69 is 0.0091383812010443852
Behaviour history of node 95 is 0.0065420560747663538


Weight of node 6 is 0.42488836448160522
Weight of node 96 is 0.0
```

Fig.7. Malicious nodes based on nodes communication

Now, based on the transmission range, nodes are clustered. Based on nodes position and communication, Cluster formation is done to pass and manage the information easily. In each cluster, cluster head and cluster members are selected as shown in Fig.4 and the diagrammatic representation of cluster formation is given in Fig.5.

After forming the cluster, next step is to detect the malicious nodes present in the network. Detection of malicious nodes is done by estimating weight, reliability and past behaviouring history of each node participating in the communication process. The Fig.7 represents the malicious node based on their weight and behavior history of the node.

The Fig.8 shows the diagrammatic representation of detection of malicious nodes. In this figure, black dots represents cluster members, blue dots represents cluster heads and red dots represents the detected malicious nodes.

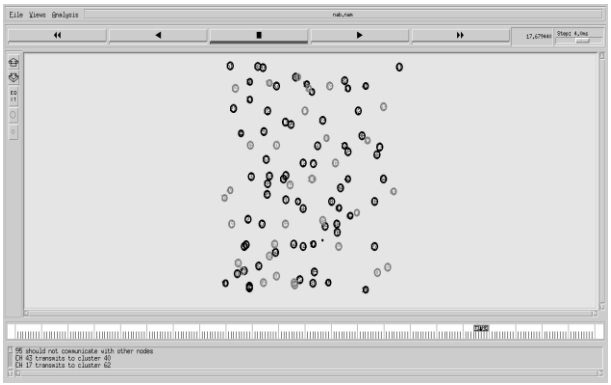

Fig.8. Malicious nodes representation

Malicious nodes present in each cluster are detected and removed from the respective clusters. New clusters are then formed based on procedure followed before and new cluster lists are updated which is shown in Fig.9.

```
Weight of node 96 is 0.0
Weight of node 9 is 1.0
Weight of node 15 is 0.44508008444001734
Weight of node 26 is 0.78143741510660791
Weight of node 78 is 0.00267922857730766653
Weight of node 61 is 0.3889205032739293
Weight of node 69 is 0.00472701999898256 23
Weight of node 95 is 0.91823947176573362

Malicious nodes are 96 78 69
Covert adversaries are 6 15 61
Semi honest nodes are


Non malicious nodes are 9 26 95


Malicious nodes are 6 96 15 78 61 69

Node 6 is Covert adversary

Updated cluster list

CH-29   clusters are 21 33 36 51 4
CH-16   clusters are 9 44 60 65 74 77 94
CH-83   clusters are 20 26 72 81 85 45
CH-10   clusters are 5 13 53 55 57 67
CH-25   clusters are 7 14 47 54 64 66 70
CH-19   clusters are 1 2 86
CH-49   clusters are 3
CH-58   clusters are 22 37 80 93
CH-38   clusters are 30 56 79 89
CH-75   clusters are 12 24 35 59
CH-32   clusters are 42 68 73 98
CH-52   clusters are 0 50 71 88 91 92
CH-63   clusters are 18 34
```

Fig.9. Updated cluster list

Secured communication path is identified and then message is transferred from source node to destination node using private key

cryptography method. Using private key as secret key, message from source node is encrypted into ciphered message. Destination node uses different key to decrypt the retrieved message. This process is shown in Fig.10.

```
CH-25   clusters are 7 14 47 54 64 66 70
CH-19   clusters are 1 2 86
CH-49   clusters are 3
CH-58   clusters are 22 37 80 93
CH-38   clusters are 30 56 79 89
CH-75   clusters are 12 24 35 59
CH-32   clusters are 42 68 73 98
CH-52   clusters are 0 50 71 88 91 92
CH-63   clusters are 18 34
CH-39   clusters are 31 82
CH-11   clusters are 23
CH-90   clusters are 27 28
CH-46   clusters are 8 48 76 87 97 99
CH-84   clusters are 95
CH-43   clusters are 40
CH-17   clusters are 62

Cluster key generation


commuication path is 20 54 25 7 67 10 55 11 30


Message is encrypting.........

Since entered message is not a neighbour node encrypting using private key
Encrypted message using the private key is 24b91c338c


Message is decrypting.........

Decrypted message using the private key is hello

channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
```

Fig.10. Cluster key generation

The Fig.11 shows the diagrammatic representation of transferring of message over the network. From this figure, it is proved that, the message is securely passed from source to destination through secured path, found from updated cluster list obtained after the successful removal of malicious nodes.

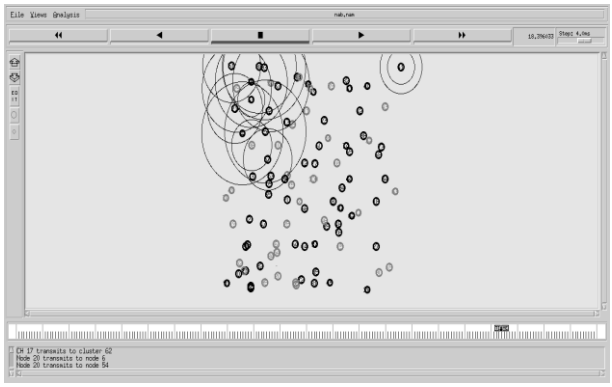

Fig.11. Message passing between nodes

5. PERFORMANCE EVALUATION

Performance of ECR-WVG and ECR-WVG-RSMPC is estimated using NS2 simulation. 300 nodes are deployed over the network. The number of malicious node chose is ranges from 0 to 60. Normal and malicious nodes are randomly deployed. Control parameters a and b are set as 1.1 and 0.9 and γ is set as 1. Aspiration performance level (S) is normalised as 0.7 and ξ is set as 1.

The Fig.12 shows the comparison result of proposed ECR-WVG-RSMPC scheme with the existing ECR-WCG scheme in terms of malicious node revocation with different node densities. Percentage of revocation of malicious nodes is calculated as the ratio of revocation success. ECR-WVG-RSMPC revoked the certificate of malicious node based on adaptive weighted game model. Thus the result proved that, ECR-WVG-RSMPC outperformed than ECR-WCG with respect to malicious node revocation.

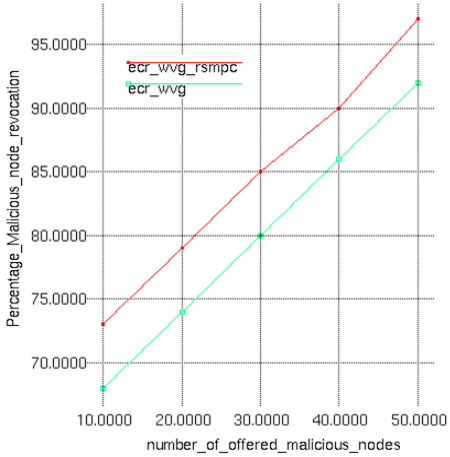

Fig.12. Malicious nodes Revocation

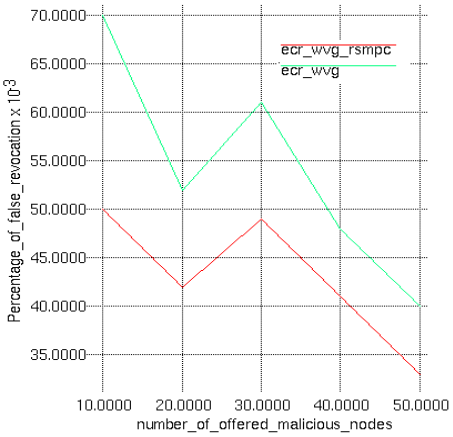

Fig.13. Percentage of false Revocation

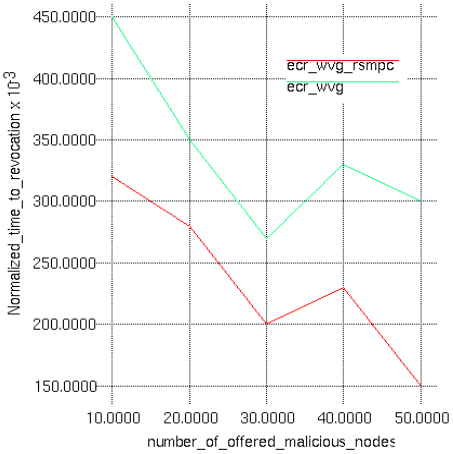

Fig.14. Normalised time to revocation

The Fig.13 shows the comparison result of proposed ECR-WVG-RSMPC scheme with the existing ECR-WCG scheme in terms of false revocation with different node densities. False

revocation is mainly due to the limited detection ability. ECR-WVG-RSMPC can able to restore the nodes that are accused wrongly. Thus the proposed scheme minimizes the percentage of false revocation when compared to the existing system.

The Fig.14 shows the comparison result of proposed ECR-WVG-RSMPC scheme with the existing ECR-WCG scheme in terms of normalized time to revocation with different node densities. ECR-WVG-RSMPC effectively monitors the condition of network and address the certificate revocation problem. The result proved that, lower revocation time is achieved by ECR-WVG-RSMPC than ECR-WCG.

The Fig.15 shows the comparison result of proposed ECR-WVG-RSMPC scheme with the existing ECR-WCG scheme in terms of the revocation accuracy ratio with different node densities. This ratio can be increased because of effective handling of false revocation issue. Thus, our ECR-WVG-RSMPC scheme obtains maximum revocation accuracy than the existing system.

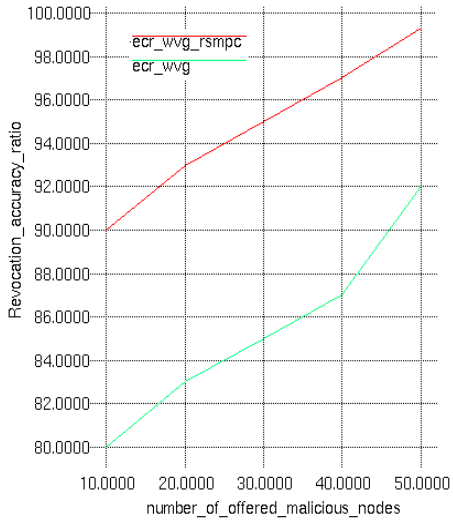

Fig.15. Revocation accuracy ratio

6. CONCLUSION

This paper mainly focussed on security issues occurred in MANET. A certificate revocation scheme is developed based on the weighted voting game (WVG) approach and Rational Secure Multi Party Computing (RSMPC) mechanism and proposed scheme is known as ECR-WVG-RSMPC. The proposed scheme can effectively handle the malicious nodes and security problem in MANET. Experiments and simulation result proved that, our ECR-WVG-RSMPC shows better results in terms of false revocation, revocation of malicious nodes, the accuracy ration of revocation and normalised time to revocation. In our future work, we have an idea to explore more than three parties in RSS to improve the security of multiparty ommuniation further.

REFERENCES

[1] Sungwook Kim, "Effective Certificate Revocation Scheme based on Weighted Voting Game Approach", *IET Information Security*, Vol. 10, No. 4, pp. 180-187, 2016.

[2] Yilei Wang, Tao Li, Hairong Qin, Jin Li, Wei Gao, Zhe Liu and Qiuliang Xu, "A Brief Survey on Secure Multi-Party Computing in the Presence of Rational Parties", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 6, No. 6, pp. 807-824, 2015.

[3] Geneviève Arboit, Claude Crepeau, Carlton R. Davis and Muthucumaru Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks", *Ad Hoc Networks*, Vol. 6, No. 1, pp. 17-31, 2008.

[4] R. Ayyasamy and P. Subramani, "An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-Hoc Networks", *The International Arab Journal of Information Technology*, Vol. 9, No. 3, pp. 291-298, 2012.

[5] W. Liu, H. Nishiyama, N. Ansari, J. Yang and N. Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, No. 2, pp. 239-249, 2013.

[6] N. Steven Raj and Sneha Kathare, "Clustering of Certificate Revocation to Reinforce an Idea for Mobile Ad Hoc Networks", *International Journal of Engineering Research and Technology*, Vol. 3, No. 7, pp. 682-685, 2014.

[7] Huaqiang Xu, Rui Wang and Zhiping Jia, "A Lightweight Certificate Revocation Scheme for Hybrid Mobile ad Hoc Networks", *International Journal of Security and Its Applications*, Vol. 10, No. 1, pp. 287-302, 2016.

[8] Maxim Raya, Daniel Jungels, Panos Papadimitratos, Imad Aad and Jean-Pierre Hubaux, "Certificate Revocation in Vehicular Networks", Available at: https://infoscience.epfl.ch/record/83626/files/CertRevVANET.pdf.

[9] T. Pank, "Review of Certificate Revocation in Mobile Ad Hoc Networks", *International Journal of Advances in Management Technology and Engineering Sciences*, Vol. 2, No. 6, pp. 2249-7455, 2013.

[10] Jolyon Clulow and Tyler Moore, "Suicide for the Common Good: a New Strategy for Credential Revocation in Self-Organizing Systems", *ACM SIGOPS Operating Systems Review*, Vol. 40, No. 3, pp. 18-21, 2006.

[11] M. Srividya, K. RadhikA and D. Jamuna, "Review on Certificate Revocation of Mobile Ad Hoc Networks", *International Journal of Engineering Research and Technology*, Vol. 1, No. 7, pp. 1-4, 2012

[12] H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", *IEEE/ACM Transactions on Networking*, Vol. 12, No. 6, pp. 1049-1063, 2004.