Wireless Personal Communications (2021) 118:647–662
https://doi.org/10.1007/s11277-020-08037-z

Energy Efficient Clustering for Certificate Revocation Scheme in Mobile Ad-Hoc Network

K. Rajkumar[1] · **M. K. Jeyakumar**[2]

Accepted: 23 December 2020 / Published online: 5 January 2021

Abstract
Mobile ad hoc networks (MANETs) have a wide range of uses because of their dynamic topologies and simplicity of processing. Inferable from the autonomous and dynamic behavior of mobile nodes, the topology of a MANET frequently changes and is inclined to different attacks. So, we present certificate revocation which is an efficient scheme is for security enhancement in MANET. This certificate revocation scheme is used to revoke the certificate of malicious nodes in the network. However, the accuracy and speed of the certificate revocation are further to be improved. By considering these issues along with the energy efficiency of the network, an energy-efficient clustering scheme is presented for certificate revocation in MANET. For cluster head (CH) selection, an opposition based cat swarm optimization algorithm (OCSOA) is proposed. This selected CH participates in quick certificate revocation and also supports to recover the falsely accused nodes in the network. Simulation results show that the performance of the proposed cluster-based certificate revocation outperforms existing voting and non-voting based certificate revocation in terms of delivery ratio, throughput, energy consumption, and network lifetime.

Keywords Mobile ad hoc networks (MANETs) · Certificate revocation · Cluster head (CH) selection · Opposition based cat swarm optimization algorithm (OCSOA)

1 Introduction

MANET is a self-sorted out wireless network which comprises of mobile gadgets, for example, laptops, Personal Digital Assistants (PDAs), and cell phones, which can unreservedly move in the system. Notwithstanding mobility, mobile gadgets support and transmit packets for one another to broaden the restricted remote transmission range of every node by multi-hop relaying, which is utilized for different applications, e.g., crisis communications, military activity, and disaster relief [1–3].

✉ K. Rajkumar
rajkumarpillai959@gmail.com

[1] Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India

[2] Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India

Security is one pivotal necessity for these network services. Actualizing security [4–6] is along these lines of prime significance in such systems. Provisioning ensured communications among mobile nodes in a threatening domain, in which a malicious node can dispatch attacks to upset the security of the network, is an essential concern. Inferable from the nonattendance of infrastructure, mobile nodes in a MANET need to execute all parts of network usefulness themselves; they go about as both end clients and switches, which hand-off packets for other nodes. In contrast to the current network, another element of MANETs is the open network condition where nodes can leave and join the network unreservedly. Subsequently, the remote and dynamic natures of MANETs uncover them progressively vulnerable against different kinds of security attacks than the wired networks.

Certificate management is a broadly utilized scheme for security enhancement in MANETs. This certificate management scheme serves as a method for passing on trust in a public key infrastructure to secure network and application services. It comprises three major phases that are prevention, detection, and revocation [7–11]. Many research works have been introduced in these areas such as detection of an attack, certificate distribution, and certificate revocation. Many research endeavors have been committed to moderate malicious attacks on the network. Any attack ought to be detected as quickly as time permits. Certificate revocation is a significant mechanism of enrolling and evacuating the certificates of nodes that have been identified to dispatch attacks on the area. As it were, if a node is undermined or acted mischievously, it ought to be expelled from the network and cut off from every one of its activities right away.

1.1 Problem Statement and Contribution

Certificate Revocation with existing methodologies has a constraint that occasionally malicious nodes will attempt to expel normal nodes from the network by falsely accusing them as malicious. Additionally existing Voting-based and non-voting-based frameworks are having sure constraints regarding accuracy, speed, cost, and reliability. The cluster-based methodology can address this problem of false accusation. With the development of the cluster, it is anything but difficult to trade the data between the associating nodes. Cluster Head (CH) assumes a significant role in identifying the falsely accused nodes inside its cluster and revoking their certificates to settle the problem of false accusation. It can accomplish less overhead and quick revocation.

The contribution of this paper is organized as follows:

- For cluster head selection, *opposition based cat swarm optimization algorithm (OCSOA)* is presented. Depend on the objective functions of energy, connectivity, and mobility of the nodes, the algorithms select the cluster head.
- This selected Cluster Head (CH) plays an important role in detecting the falsely accused nodes within its cluster and revoking their certificates to solve the issue of false accusations.
- This proposed approach is implemented in the platform of NS2.
- The performance of this proposed approach is evaluated in terms of delivery ratio, network lifetime, delay, and successful certification ratio.

The rest of the sections of this paper is organized as follows. Section 2 surveys some recent literature which research on security in MANET. Section 3 proposes cluster-based certificate revocation in MANET. Results of this proposed approach are discussed in Sect. 4. Finally, the conclusion of this paper is described in Sect. 5.

2 Related Works

In this section, some recent literature focused research on the certificate revocation process for enhancement of security in MANET. Researchers had presented their techniques in this literature for enhancing the security of MANET. Among them, Hamouid and Adi [12] had presented reliable and secure certification management method in large scale MANETs. The authors aimed to mitigate the effect of malicious nodes from the network. To achieve this aim, they had proposed a certificate management method based on a compromise tolerant threshold. Also, they had achieved their goal with the support of the Anonymous Certification Authority which was abbreviated as ACA. By presenting this proposed approach, they had improved service availability.

Zarezadeh and Mala [13] had proposed estimation of accuser node's honesty in the key revocation process of MANETs. This literature aimed to enhance the performance of honest accuser node detection. To achieve this aim, the authors had presented a scheme that considered the event of attacks depends on a non-homogeneous Poisson process. The accuser node was evacuated from the warning list if the time interim between the receptions of two back to back accusation packets was not exactly a specific value. Because of this proposed approach, they attained better detection time and warning time.

Janani and Manikandan [14] had presented Hexagonal clustering based on trust for effective certificate management method in MANET. The authors aimed to reduce the certificate management complexity due to the redundant certificates. To achieve this objective, they had proposed hexagonal clustering based on trust for an effective certificate management method which was abbreviated as THCM. They had presented a hexagonal geographic clustering model and also Voronoi method was utilized for trust calculation. Simulation results of the article showed that the proposed THCM scheme achieved better revocation time, revocation rate, and communication cost.

Venkata Swaroop and Murugaboopathi [15] had proposed a reliable and secure communication method for MANET with certificate revocation based on the ECMS cluster head. The authors aimed to remove the malicious node and keep away the network from unauthorized access. For achieving these goals, at first, the authors had identified a cluster head in every cluster using the ECMS algorithm. In this algorithm, E denotes Energy, C denotes Connectivity, M denotes Mobility and S denotes Signal to noise ratio. Then the certificate revocation process was initiated via the selected cluster head. The authors had evaluated the performance of their proposed approach in terms of delivery ratio, throughput, and delay.

Raja et al. [16] had proposed an efficient certificate revocation of malicious nodes for MANET. The authors aimed to revoke the malicious node's certificate from MANET justifying the communication with less risk. To achieve this aim, they had presented an efficient model. Using this mode each node was related to reliance, which was an estimation of its integrity. The model, not just merits node's good behavior, yet additionally finds node's misbehavior. Simulation results of the literature showed that the proposed technique was more effective in the certificate revocation process.

Kim [17] had presented a weighted voting game scheme based efficient certificate revocation method for MANET. The author aimed to enhance the security of MANET.

To achieve this aim, the author had presented a distributed certificate revocation protocol. Also, the author had designed an innovative voting-depend security method based on the game-theoretic model. This game-based security scheme provided the capacity to for all intents and purposes react to the present framework conditions and was appropriate for genuine MANET activities. Simulation results of the article showed that the proposed scheme achieved a better normalized time to revocation and revocation accuracy ratio.

3 Energy Efficient Clustering for Certificate Revocation Scheme in MANET

3.1 Overview

For secure network communication against the attackers in MANET, a certificate revocation scheme is presented. However, to recover the node from the false accusation, a cluster-based certification revocation scheme is proposed. Besides, for enhancing the energy efficiency of the network, a cluster is formed with the opposition based cat swarm optimization algorithm (OCSOA). Using this algorithm cluster head (CH) is selected and the CH joins the members which are in its communication range. This selected CH helps to recover the node which is accused falsely by the certificate authority (CA) during the process of certificate revocation. Figure 1 shows the block diagram of the proposed approach.

3.2 Cluster Head (CH) Selection Using OCSOA Algorithm

To enhance the energy efficiency of the network, the clustering scheme plays an important role. So, in this approach, mobile nodes are clustered with the opposition based cat swarm optimization (OCSOA) algorithm. Using this algorithm, CHs are selected initially before the formation of the cluster. In the CSOA algorithm, cats and the model of behaviors of cats are used to solve the optimization problems, i.e. Cats are used to portray the solution sets. In CSOA, a decision has to be made on how many cats are to be used, and then the cats are applied to CSOA to solve the problems. Every cat has its position composed of N dimensions, velocities for each dimension, a fitness value, which represents the accommodation of the cat to the fitness function, and a flag to identify whether the cat is in seeking mode or tracing mode. The final solution would be the best position in one of the cats because CSOA keeps the best solution till it reaches the end of iterations. For enhancing the population diversity of the CSOA algorithm, the Oppositional Based Learning (OBL) method is used in the CSOA algorithm. According to OBL, for each solution, an opposite solution is generated. Thus the chance of obtaining an optimal solution is increased. The following phases describe the performance of the OCSOA algorithm for selecting the optimal CHs.

Initialization In this algorithm, the position of the cat represents the candidate solution. The optimal CHs are considered as candidate solutions. The candidate solutions are initialized in the D dimensional vector space and the population of the solutions is represented as follows:

$$Y = \{C_1, C_2, \ldots, C_D\} \tag{1}$$

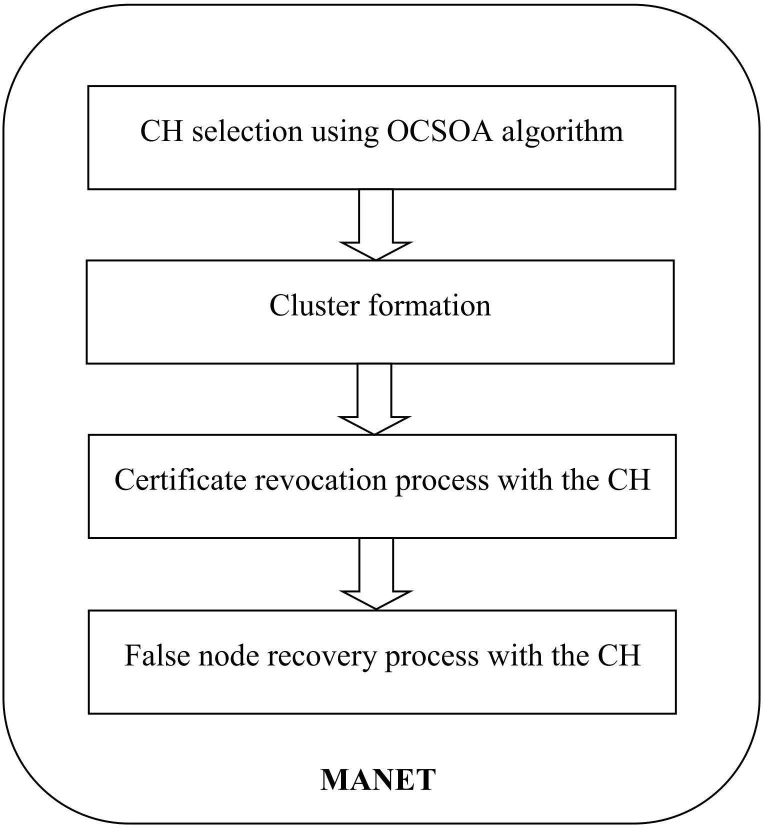


Fig. 1 Block diagram of the proposed approach

where C_D represents the position of cat or candidate solution in the Dth dimensional vector space.

OBL In the OBL method, an opposite solution is generated for each candidate solution or cat. The oppositional solution of ith candidate is defined as follows,

$$C_i' = a_i + b_i - C_i \tag{2}$$

where C_i' represents the oppositional candidate solution, a_i represents the lower limit of the solution C_i and b_i represents the upper limit of the solution C_i.

Fitness After the initialization of the solutions and opposite solutions, fitness is calculated for each solution. In this algorithm, fitness represents the accommodation of the cat. The fitness of the solution or CH is considered as maximum residual energy (RE) in this approach. Fitness of ith solution can be defined as follows,

$$Fit_i = Min\{RE_i\} \tag{3}$$

where RE_i can be calculated as follows,

$$RE_i = IE_i - CE_i \tag{4}$$

where IE_i and CE_i represent the initial energy and consumed energy of the ith CH.

According to Eq. (3), the solution with minimum fitness function is considered as the best solution or CH. Until finding the optimal solution, the solution will be updated with the following phase.

Update the Solutions In this algorithm, solutions are updated by following two main modes that are (1) seeking mode and (2) tracing mode. These two modes are described as follows.

(i) Seeking Mode This sub-model is utilized to show the cat's situation, which is resting, looking around, and looking for the next position to move to. In looking for mode, we characterize four basic variables: seeking a range of the chose dimension (SRD), seeking memory pool (SMP), self-position consideration (SPC), and counts of dimension to change (CDC).

SMP is utilized to characterize the seeking memory size for each cat, which shows the points looked for by the cat. The cat would pick a point from the memory pool concurring to the guidelines depicted later. SRD proclaims the mutative proportion for the chose dimensions. In seeking mode, if a dimension is chosen to mutate, the contrast between the old value and the new one won't out of the range, which is characterized by SRD. CDC unveils what number of dimensions will be changed. These variables are on the whole playing significant roles in the seeking mode. SPC is known as a Boolean variable, which chooses whether the point, where the cat is as of now standing, will be one of the possibility to move to. Regardless of the estimation of SPC is true or false; the estimation of SMP won't be affected. The performance of seeking mode functions can be depicted in 5 phases as pursues:

Phase 1 Generate k copies of the current position of cat_j, where k represents the SMP. If the SPC value is true, let k = (SMP-1), at that point hold the current position as one of the candidates.
Phase 2 For each copy, as indicated by CDC, arbitrarily plus or minus SRD percents of the current values and supplant the old ones.
Phase 3 For all candidates, estimate fitness (*Fit*) values.
Phase 4 If all Fit is not actually approached, compute the choice probability of each candidate point using Eq. (6), generally set all the choice probability of every candidate point to be 1.
Phase 5 Randomly choose the point to forward to from the candidate points, and supplant the position of cat_j.

$$pr_i = \frac{|Fit_i - Fit_c|}{Fit_{\max} - Fit_{\min}}, \quad where \quad 0 < i < k \tag{5}$$

For optimal CH, the minimum fitness function is calculated for finding the optimal solution. So, in Eq. (5), Fit_c is considered as $Fit_{\max}$.

(ii) *Tracing Mode* Tracing mode is the sub-model for demonstrating the instance of the cat in following a few targets. When a cat goes into tracing mode, it moves as indicated by its very own velocities for each dimension. The activity of tracing mode can be depicted in 3 phases as pursues:

Phase 1 Using Eq. (6), velocities are updated for every dimension ($v_{j,d}$).

$$v_{j,d}^{new} = v_{j,d} + ran_1 * c_1 * \left(y_{best,d} - y_{j,d}\right) \quad d = 1, 2, \ldots, M \tag{6}$$

where $y_{best,d}$ represents the position of the cat with the best fitness value, $y_{j,d}$ represents the position of cat_j, c_1 denotes the constant value and ran_1 denotes the random value within the range [0, 1].

Phase 2 Verify if the velocities are in the range of the most extreme velocity. On the off chance that the new velocity is over-range, set it to be equivalent as far as possible.

Phase 3 The position of cat_j is updated using Eq. (7)

$$y_{j,d}^{new} = y_{j,d} + v_{j,d}^{new} \tag{7}$$

To consolidate these two modes into the algorithm, a mixture ratio (MR) is defined, that directs the joining of seeking mode with tracing mode. The running behavior of the cat after targets is applied to tracing mode. In this manner, MR certainly ought to be a small value to ensure that the cats spend more often than not in seeking mode, much the same as this present reality.

Termination The solutions will be updated until finding the optimal CH. Otherwise, the algorithm will be terminated. Figure 2 shows the flowchart of the proposed OCSOA algorithm.

After the selection of CH, it forwards the HELLO message to the nearby nodes which are in its communication range for acknowledging itself as CH. Then, the cluster will be formed by the CH after receiving the ACK message from the nearby nodes.

3.3 Certificate Revocation Process

Before nodes can join the network, they need to get substantial certificates from the Certificate Authority (CA), which is liable for distributing furthermore, manifesting certificates all nodes considered, so nodes can communicate with one another seamlessly in a MANET. The CA is likewise accountable for updating two lists are Warned List (WL) and Blacklist (BL). BL is used to hold the node accused as malicious, while the WL is utilized to hold the accusing node. The CA refreshes each list as indicated by received control packets. Nodes that are in the WL are esteemed as warned nodes with low reliability. Warned nodes are viewed as suspicious because the WL contains a combination of normal nodes and some malicious nodes. The accused nodes that are in the BL are viewed as revoked nodes with little unwavering quality. Revoked nodes are considered as malicious attackers denied of their certificates and expelled from the network.

In the certificate revocation process, each node available in the network is observed with the assistance of one-hop neighbors. These neighbors are additionally used to gather the malicious information of the sensor nodes. The certificate revocation process is begun

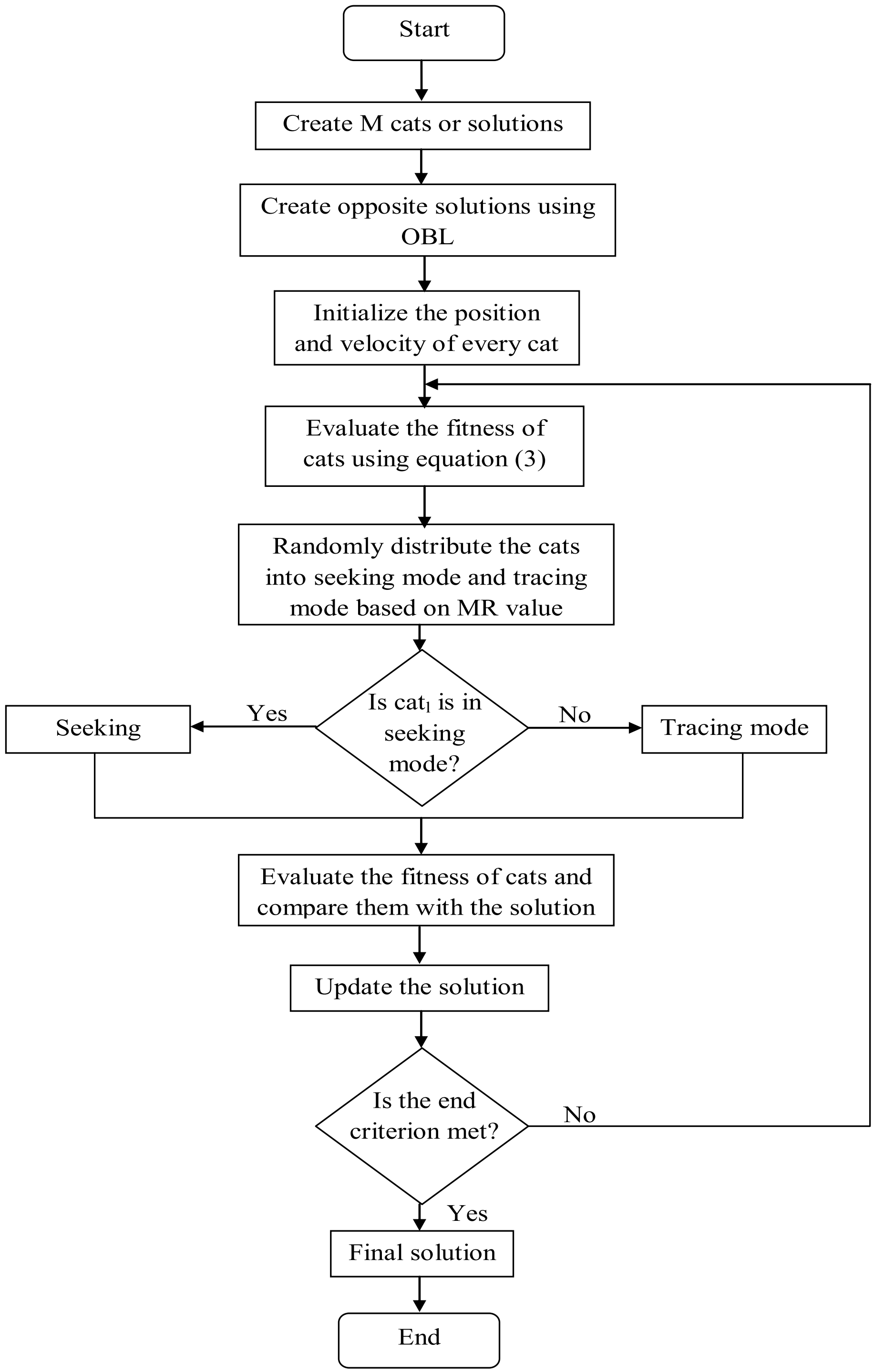


Fig. 2 Flowchart of the proposed OCSOA algorithm

when the sensor nodes initiate their malicious activity. The normal nodes verify the local list BL regardless of whether the neighboring node is listed in the BL or not. If the neighboring node is distinguished as a malicious node dependent on the certificate then the malicious node will be revoked from the network and it doesn't execute any harmful attack in the future. On the off chance that the neighboring node is recognized as a normal node based on its certificate at that point, the normal node will transmit the accusation packet (AP) to CA through the CH. Therefore, the normal node doesn't execute any harmful attack in the future.

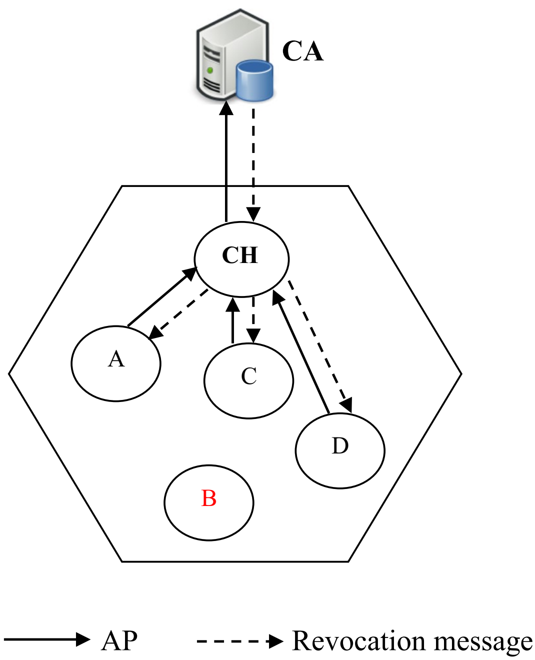
From that point onward, once getting the first reached AP, the CA checks the validation of the certificate of the accusing node: if valid, the accused node is considered as a malicious attacker to be placed into the BL. In the meantime, the accusing node is held in the WL. At last, by communicating the revocation message including the WL and BL to the nodes through the CH by the CA, nodes present in the BL are effectively revoked from the network.

Figure 3 shows an example of the certificate revocation process. Nodes A, C, and D detect that node B is a malicious node. Then they send Accusation Packet (AP) to the CH and the CH forwards the AP to the CA. After receiving the AP, the CA updates the node B in BL and updates the nodes A, C, D, and CH in WL. Finally, the CA forwards the message which includes certificate revocation of node B to all nodes through the CH.

3.4 False Accusation Node Recovery

To overcome the problem of false accusation against a normal node by the CA, CH is utilized to recognize false accusation and recover the falsely accused node within its cluster. Since each CH can identify all attacks from its CMs, requests for the CA to restore the

Fig. 3 An example of the certificate revocation process



falsely accused node's certificate can be practiced by its CHs by sending Recovery Packets (RPs) to the CA. After getting the RP from the CH, the CA can expel the falsely accused node from the BL to recover its normal behavior. Initially, the CA distributes the WL and BL information to every one of the nodes in the network, and the nodes update their WL and BL from the CA regardless of whether there is a false accusation. Since the CH doesn't recognize any attacks from a specific accused node listed in the BL from the CA, the CH gets mindful of the event of false accusation against its CM. At that point, the CH sends an RP to the CA to vindicate and restore this node from the network. At the point when the CA acknowledges the RP and checks the legitimacy of the sender, the falsely accused node will be discharged from the BL and held in the WL. Moreover, the CA forwards this information to every node through the CH. Figure 4 shows an example of a false accusation node recovery process. As shown in the figure, the CA forwards the updated BL and WL to the CH. After receiving it, the CH verifies and detects that the S is falsely considered as an accused node by the CA. Then the CH forwards the RP to the CA. By verifying the RP packet, the CA removes node S from the BL and holds nodes P, Q, R, S, and CH in WL. Finally, these updated BL and WL are disseminated to all nodes for recovering node S.

4 Results and Discussion

The proposed cluster-based certificate revocation scheme is implemented in the platform of NS2. The simulation parameter and its assumption are detailed in Table 1. In this simulation, 250 mobile nodes and one CA node are utilized. These nodes are initialized in the simulation area of 1000 m × 1000 m. Also, for this simulation, Constant bit rate (CBR) traffic source and IEEE802.11 MAC protocol are used. The packet with a size of 512 bytes is transmitted at the rate of 500 kbps. For routing the data packet, the AODV routing protocol

Fig. 4 An example of a false accusation node recovery process

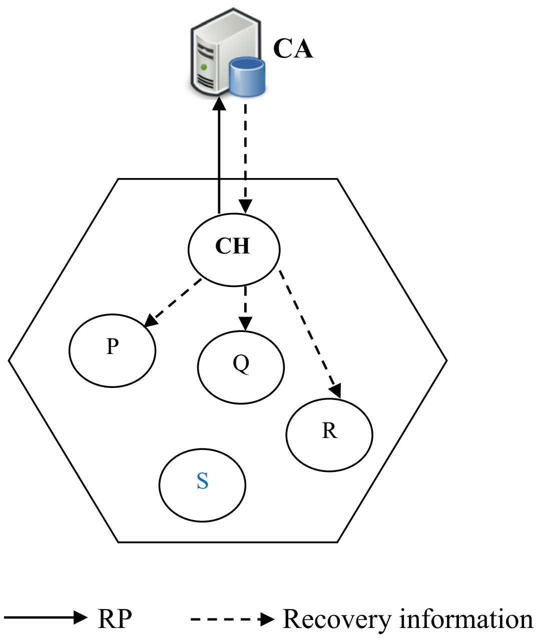


Table 1 Simulation settings

Parameters	Assumptions
No. of nodes	250 mobile nodes and one CA node
Area	1000 m × 1000 m
MAC	802.11
Simulation time	200 s
Traffic source	CBR
Rate	500 Kbps
Propagation	TwoRayGround
Antenna	Omni antenna
Packet size	512 byte
Routing protocol	AODV

is utilized. The performing nodes are clustered using the CH which is selected using the proposed OCSOA algorithm. The CH monitors the malicious nodes inside the cluster. If the malicious node is detected, then the certificate of the node is revoked by the CA via CH. Besides, a node that is falsely accused by the CA is recovered using the selected CH. This whole simulation is done within the simulation time of 200 s.

4.1 Performance Analysis

In this section, the performance of the proposed Energy Efficient Clustering (EEC) certificate revocation is evaluated in terms of throughput, delay, delivery ratio, energy consumption, and network lifetime. Also, the performance of EEC based certificate revocation is compared with that of existing voting based certificate revocation and non-voting based certificate revocation.

4.2 Performance Based on Varying Nodes

The performance of the proposed EEC based certificate revocation is analyzed by a varying number of nodes 50, 100, 150, 200, and 250. Figure 5 shows the comparison of delay of different certificate revocation schemes. As shown in the figure, the delay is increased when the number of nodes increases. However, compared to voting and non-voting based certificate revocation schemes, the proposed EEC based certificate revocation scheme decreases the delay to 19 and 37% respectively. Because of the proposed cluster-based certification revocation scheme, malicious node activities are removed from the cluster so it leads to a decrease in the delay of data delivery.

The trade-off between the number of nodes and the delivery ratio for different certificate revocation schemes is shown in Fig. 6. The delivery ratio is decreased when the number of nodes increases. Nevertheless, the delivery ratio of the proposed EEC based certificate revocation scheme is increased to 32 and 53% than that of the voting and non-voting based certificate revocation schemes respectively. Due to the selection of optimal CHs using OCSOA, the delivery ratio of the network is increased. Figure 7 shows the comparison of energy consumption of the different certificate revocation schemes for a varying number of

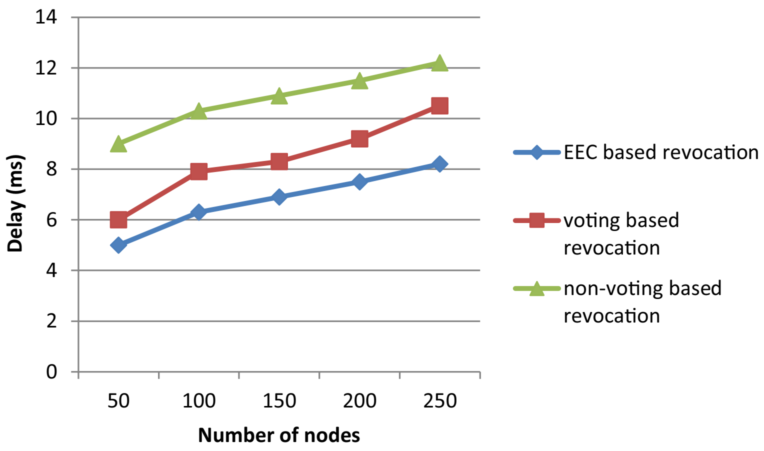


Fig. 5 Number of nodes versus delay

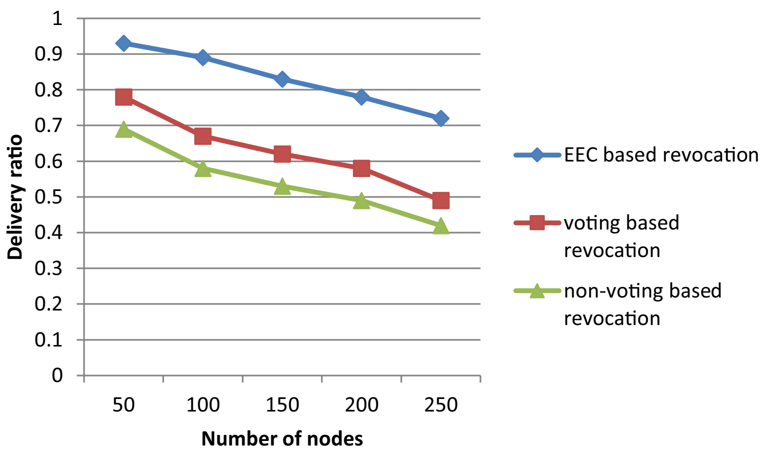


Fig. 6 Number of nodes versus delivery ratio

nodes. As the nodes are clustered using the OCSOA algorithm, energy consumption of the proposed EEC based certification revocation scheme is reduced to 42 and 51% than that of existing voting and non-voting based revocation schemes respectively.

The comparison of the network lifetime of different certificate revocation schemes for varying numbers of nodes is shown in Fig. 8. As shown in the figure, the network lifetime is decreased when the number of nodes increases. However, compared to existing voting and non-voting based revocation schemes, the network lifetime of the EEC based certificate revocation is increased to 25 and 44% respectively. Figure 9 shows the tradeoff between throughput and the number of nodes for different certificate revocation schemes. As shown in the figure, the throughput of the proposed EEC based certification revocation scheme is increased to 20 and 67% than that of the existing voting and non-voting based revocation schemes respectively.

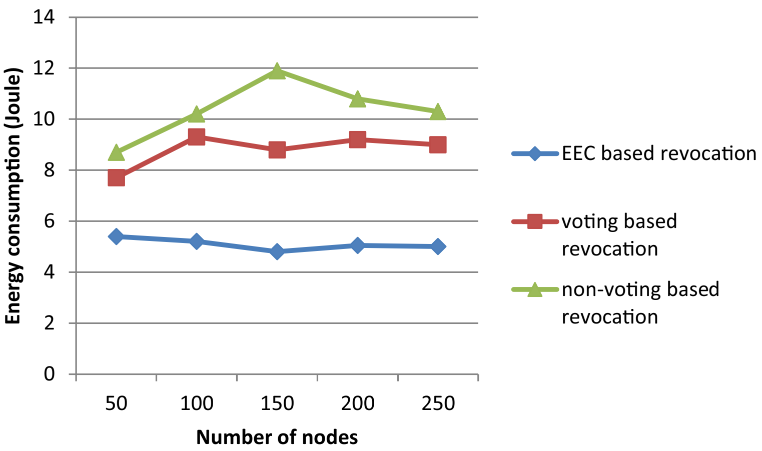


Fig. 7 Number of nodes versus energy consumption

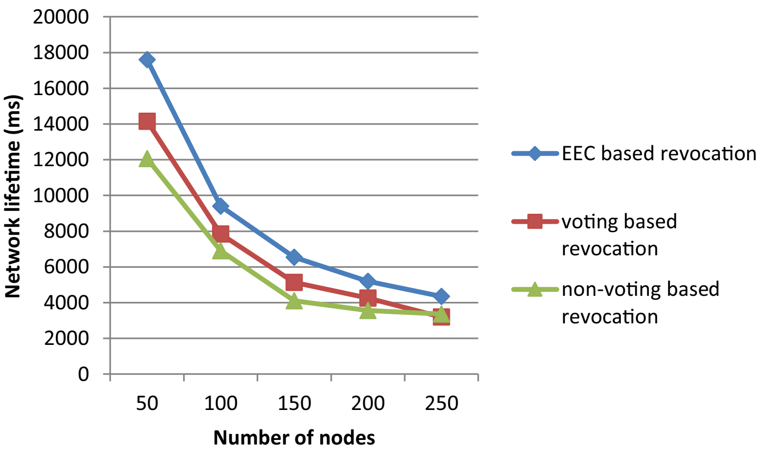


Fig. 8 Number of nodes versus network lifetime

5 Conclusion

As malicious node activities affect the security services of MANET, a certificate revocation scheme is presented in this paper. Although this scheme isolates the malicious node from the network, the accuracy, and speed of certificate revocation are further to be improved. So, an energy-efficient clustering scheme for certificate revocation is proposed. In this approach, CH is selected using an opposition based cat swarm optimization algorithm (OCSOA). The CH monitored malicious nodes inside a cluster. The certificate of the malicious node is revoked by CA via CH. Also, the CH is used to recover the falsely accused nodes inside a cluster. The performance of the proposed cluster-based certificate revocation scheme is compared with that of voting and non-voting based certificate revocation

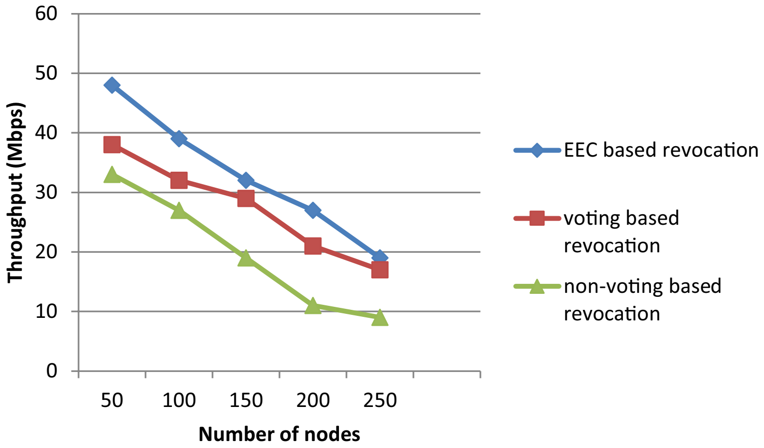


Fig. 9 Number of nodes versus throughput

schemes. Simulation results showed that the proposed scheme outperformed the existing certificate revocation schemes in terms of delivery ratio, energy efficiency, and network lifetime.

Authors' Contributions All authors read and approved the final manuscript.

Funding Not applicable.

Availability of Data and Materials Not applicable.

Compliance with Ethical Standards

Conflicts of interest The author declare that they have no conflict of interest.

References

1. Saravanan, K., & Vellingiri, J. (2017). Defending MANET against flooding attack for medical application. In *2017 2nd international conference on communication and electronics systems (ICCES)*.
2. Kwak, K., Huerta-Canepa, G., Ko, Y., Lee, D., & Hyun, S. (2009). An overlay-based resource monitoring scheme for social applications in MANET. In *2009 33rd annual IEEE international computer software and applications conference*.
3. Pease, S. (2013). ROAM: Supporting safety critical applications in MANETs with cross-layer middleware. In *2013 IEEE 14th international symposium on "A world of wireless, mobile and multimedia networks". (WoWMoM)* (2013).
4. Ochola, E. O., Eloff, M. M., & van der Poll, J. A. (2013). Democratic detection of malicious behaviour in MANET: A voting process. In *2013 information security for South Africa. IEEE* (pp. 1–7).

5. Sharma, S. B., & Chauhan, N. (2015) Security issues and their solutions in MANET. In *2015 international conference on futuristic trends on computational analysis and knowledge management (ABLAZE)*, *IEEE* (pp. 289–294).
6. Sheikh, R., Chande, M. S., & Mishra, D. K. (2010). Security issues in MANET: A review. In *2010 seventh international conference on wireless and optical communications networks-(WOCN), IEEE* (pp. 1-4).
7. Yosaka, N., Iichiro, N., & Nagase, T. (2011). Authentication and certificate managements of unauthorized intrusion in Ad hoc networks, problems and solutions. In *2011 14th international conference on network-based information systems*, *IEEE* (pp. 646–650).
8. Haibing, M., Yun, L., & Changlun, Z. (2006). A certificate management model for MANET. In *2006 8th international conference on signal processing*, *IEEE* (Vol. 4).
9. Li, R., Li, J., Kameda, H., & Liu, P. (2004). Localized public-key management for mobile ad hoc networks. In *IEEE global telecommunications conference, 2004. GLOBECOM'04*, *IEEE* (Vol. 2, pp. 1284–1289).
10. Krishnan, R., Julie, E., Robinson, Y., Kumar, R., Thong, P., & Son, L. (2020). Enhanced certificate revocation scheme with justification facility in mobile ad-hoc networks. *Computers & Security, 97,* 101962.
11. Bhavyashree, H., Nagarathna, C., Preetham, A., & Priyanka, R. (2019). Modified cluster based certificate blocking of misbehaving node in MANETS. In *2019 1st international conference on advanced technologies in intelligent control, environment, computing & communication engineering (ICATIECE)*.
12. Hamouid, K., & Adi, K. (2019). Secure and reliable certification management scheme for large-scale MANETs based on a distributed anonymous authority. *Peer-to-Peer Networking and Applications, 12*(5), 1137–1155.
13. Zarezadeh, M., & Mala, H. (2018). Determining honesty of accuser nodes in key revocation procedure for MANETs. *Mobile Networks and Applications, 24*(3), 903–912.
14. Janani, V. S., & Manikandan, M. S. K. (2016). Trust-based hexagonal clustering for efficient certificate management scheme in mobile ad hoc networks. *Sādhanā, 41*(10), 1135–1154.
15. Venkata Swaroop, G., & Murugaboopathi, G. (2017). Secure and reliable communication scheme for MANET using ECMS cluster head-based certificate revocation. *Cluster Computing, 22*(5), 11513–11525.
16. Raja, K., Deivasigamani, A., & Ravi, V. (2015). A reliant certificate revocation of malicious nodes in MANETs. *Wireless Personal Communications, 90*(2), 435–455.
17. Kim, S. (2016). Effective certificate revocation scheme based on weighted voting game approach. *IET Information Security, 10*(4), 180–187.

K. Rajkumar Research Scholar, Department of Computer Science and Engineering, Noorul islam Centre for Higher Education, Kumaracoil-629180, Tamil Nadu, India. He is working as an Associate Professor and Head of the Department in Musaliar College of Engineering Chirayinkeezhu. He has 21 years of teaching experience in different Engineering Colleges.

Dr. M. K. Jeyakumar is working as Professor in the Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India. He has 25 years of teaching experience including 17 years of research experience in the field of Mobile Computing and Image Processing. He published more than 110 peer review research articles and one book chapter.