System Models with Threshold Cryptography for Withdrawal of Nodes Certificate in Mobile Ad Hoc Networks

Priti Swapnil Rathi, Kanika Bhalla and CH. Mallikarjuna Rao

Abstract Achieving security in mobile ad hoc network (MANET) is somewhat difficult compare to wired network because in ad hoc network malicious nodes can freely move from one location to another location and thus able to launch attacks against different nodes. In our previous work, we have explained a simple method to identify the malicious node that is collect information from, n nodes present in MANETs; but in that approach it is difficult to achieve efficient and secure key management as well as it is difficult to differentiate between valid and false accusation made by well-behaving and malicious nodes. As an extension to our previous work, this paper will help to achieve more security by using efficient key management technique. In this technique, we are dividing the functionality of the certificate authority. Threshold sharing techniques are used for distributing CA functionality. In this mechanism, every node present in the network will hold a piece of certificate authority signing key and multiple nodes in a one-hop monitoring range will jointly provide complete service. This paper also clarifies how to distinguish between legal and false accusations messages, as well as different system models will help our planned scheme for revoking the certificate of malicious node efficiently, and for avoiding false accusation attack which can occur due to inside malicious node.

Keywords MANET network · Threshold cryptography · Digital certificate

P. S. Rathi (✉) · K. Bhalla · CH. Mallikarjuna Rao
Department of Computer Science and Engineering,
GRIET College of Engineering, Hyderabad, India
e-mail: pritirathi2@gmail.com

K. Bhalla
e-mail: kanika4world@gmail.com

CH. Mallikarjuna Rao
e-mail: chmksharma@yahoo.com

A. J. Kulkarni et al. (eds.), *Proceedings of the 2nd International Conference on Data Engineering and Communication Technology*, Advances in Intelligent Systems and Computing 828, https://doi.org/10.1007/978-981-13-1610-4_49

1 Introduction

A mobile ad hoc network (MANET) is a group of collection of more than one low-volume calculating devices such as laptops, PDA. These devices are connected to each other through wireless links and do not depend on the predefined infrastructure to keep the network connected. Mobile will act as a node in MANETs. Every node present in the MANETs can work as a sender, receiver or router who is responsible for sending and receiving of data.

There are two main types of network architectures are present, and those are wired network and wireless network. MANETs are type of wireless network. Every network, such as wired network, wireless network, local area network, will have their own features which make them unique from other types of networks. Likewise, MANETs also have their own characteristics which make it different from wired network [1, 2] and these unique characteristics of ad hoc network itself will create opportunities and challenges for achieving security in network. Following are the some of the problems which can arise due to MANETs unique features.

1.1 Absence of Centralized Entity or Server

Following are the some of the task to fulfill these tasks successfully and efficiently centralized entity or server is required that are as follows:

- To establish better trust management

Difficult to establish better trust management because in traditional network; generally, this trust management task gets done by the centralized entity. Every node which is available in MANETs needs to cooperate with the operation which gets performed inside network.

- Issuing and revocation of certificates to nodes

Difficult to perform certificate issuing and certificate revocation task because; certificates are get issued by centralized entity. Storage of certificates and retrieval of certificates in MANETs and it is difficult to perform storage and retrieval of certificates because in traditional network, the information about valid and revoked certificate get stored at some central repositories such that it will get accessed by all the nodes that are present in the network but in MANETs there is no centralized server which is present and so in the proposed system, the information about valid and revoked certificates needs to be preserved toward every node present in MANETs [0][4].

1.2 Infrastructure Support Absence

The absence of infrastructure support makes it impossible from making use of any traditional security methods such as DC for achieving security in MANETs [0]. Mostly, the DC method gets used for achieving security in wired types of network but when it comes to wireless communication network at that time these wired network security methods will not be useful for MANETs for achieving security because it will create different problems.

1.3 Dynamically Change in Network Topology

The nodes in MANETs are permitted to link and to dispensation from the network at any time. This unrestricted mobility feature of the wireless network makes always some changes in topology, with each and every single movement of nodes. This change in the network formation will affect into some route change, loss of packet from sender to receiver.

1.4 Nonexistence of Secure Boundaries

In wired network, when any outside employer wants to enter into the network for performing malicious activity, then first that node needs to go through different security mediums such as firewall, gateway before they can perform any malicious actions to the target nodes; by using these all security mediums that particular node which is adversary get found easily, and next time, it will not allow that adversary node to enter inside the network and thus target node get protected from malicious activity.

In MANETs, the adversary node does not require to go through different security mediums to access the network because once the adversary node will come within the radio range if any other node present in network, then that adversary node will be able to connect with the nodes which are present within its radio range and thus join the network immediately [3]. Once adversary node gets entered into the radio range of other node, then that respective node will be able for performing false accusation attack and try to prove genuine node as an enemy node.

These are the different challenges that can occur in ad hoc network while achieving security due to its unique characteristics. The MANETs help to set up a temporary network which will allow the user to perform instant communication due to this, and the focus on MANETs has increased lot of attention in the recent years, and due to this increased focus on MANETs, the security-related issues are considered as important and brought to front position.

Different methods such as symmetric key cryptography, digital certificates are existing for achieving security in wired network. These all methods are not able to provide security for MANETs because of the absence of central authority (CA), absence of physical connection presents between nodes, mobility. Certificate revocation theaters play a vital role for achieving sufficient amount of security in MANETs. Revocation of certificate issue in wired network is easy because once certificate of malicious node gets revoked, and then certificate authority stores this revocation information into certificate revocation list (CRLs). The CRLs are either stored on some accessible repositories or else broadcast to all the existing nodes in MANETs. Handling of certificate revocation problem in MANETs is difficult task compared to the wired network because the wired security methods are not able to provide security in MANETs. The planned system makes use of threshold-based cryptography method to revoke certificate of malicious node quickly and correctly and try to achieve security as well as protect legitimate nodes from malicious nodes in MANETs.

This paper is getting break into different section where Sect. 2 analyses and compares the proposed system with the already available techniques, next Sect. 3 gives the idea of system models, and finally, Sect. 4 describes proposed threshold-based cryptographic method with their design.

2 Related Work

This section will describe numerous approaches which are already present for MANETs and their limitations.

2.1 URSA

URSA [4] technique makes use of certified ticket-based approach. This approach, provides the tickets for the node after that the node who is consuming legal ticket those nodes are allowed to enter into MANETs whereas remaining nodes, who are not having legal tickets those nodes are not allowed to by URSA [4] for entering into network. All the tickets of nodes in URSA [4] get managed locally inside the network itself for removing adversary and malicious node form's network. The ticket of malevolent node gets cancel, when it exceeds the number of votes of its fellow citizen beyond the predefined threshold value.

2.2 Voting-Based Scheme

This scheme [5] is a transformed format of the URSA. The main modification amongst URSA and voting scheme is, it allows the nodes presents in MANETs to

vote through different weight. Weight of nodes vote gets calculated from node consistency as well as nodes previous performance. To revoke the certificate of malevolent node, it estimates weights of all the polls which are received in contradiction of a particular node and after calculating sum of these reaches to a predefined threshold value, then it will remove the certificate of that particular node.

2.3 Decentralized Suicide-Based Approach

Voting-based scheme [5] is a modified version URSA. The foremost variance among URSA and decentralized suicide-based approach is that this approach permits the nodes that present in MANETs to poll with different weight value. Nodes reliability and nodes historical performance get taken into consideration for calculating weight of the nodes.

2.4 Working of Existing Methods with Proposed Methods in Comparative Analysis Form

Table 1 indicates different features and also explains the brief working of the existing methods. First column indicates the name of the existing method with its reference number in bracket. Second column indicates whether that particular excising method will make use of CA for issuing and revoking of certificate and fourth column gives information about who is going to issue certificate to nodes and revoke certificate of malicious node. Fifth column indicates the mechanism used by the existing methods to revoke the certificate of node, and last column gives information about the period required for revocation of nodes certificate by these existing methods.

Table 2 gives comparative analysis of the existing method with our new proposed methods. It gives information about advantages and limitations of the existing method whose name is indicated in first column of this Table 2 and last column of Table 2 indicated the advantages provided by planned approach. The relative study of third and fourth column indicates that the new proposed method tries to solve

Table 1 Working of CA and effect of attack on existing methods

Existing methods	CA	False accusation attack
URSA [4]	Not used	Robust for single node
Voting-based scheme [5]	Not used	–
Suicide for the common good [10] or decentralized suicide based approach	Not used	Not able to differentiate between valid and false accusation messages

Table 2 Working of existing methods for certificate revocation task

Existing methods	Mechanism to revoke certificate	Time required to revoke certificate
URSA [4]	Takes opinion from multiple neighboring nodes which are present within one-hop monitoring [12]	Less compared to [5]
Voting based scheme [5]	Allows all nodes to vote with variable weight and if sum of weight of all nodes votes against particular node exceeds a predefined threshold [13]	More compare to [4]
Suicide for the common good [10] or decentralized suicide based approach	Even if only one has made accusation against another node, then certificate of accused as well as accuser get revoked [12]	Very less compared to [4, 5]

Table 3 Comparative analysis of existing methods with new proposed method in this paper

Existing methods	Advantages of existing methods	Limitations of existing methods	Newly proposed methods
URSA [4]	Strong for false accusation attack generated by single node	The subject of spotting false accusation attack generated by more than one nodes that present in MANETs is still not resolved	Able to detect false accusation attack caused by one node as well as by more than one nodes
Voting based scheme [5]	Improves the accuracy of certificate revocation	Increases the time required to revoke certificate of malicious node	Certificate of node get revoked when it will detect the first misbehavior of that node

the limitations of these existing methods. Tables 1 and 2 show the working of the existing methods with different parameters (Table 3).

3 Planned System Models

In this unit, we will discourse about the net model, the trust model, the attack model, and the mathematical model which will be used in the proposed system.

3.1 Network Model

We consider a wireless MANETs as shown in Fig. 1 where the network is made-up from 'N' nodes and $N > 0$.

Once the network gets created with specified number of nodes 'N', then from that network our proposed system draws accusation graph $G = (V, E)$ where G represents 'Directed Graph,' V represents 'Nodes,' and 'E' represents 'Edges' as shown in Fig. 2.

In Fig. 1, nodes in the network communicate with each other if they present inside the radio or else it gets performed in multihop or ad hoc manner where more than one hop is requiring to send data from source to destination. The value of 'N' changes dynamically as new node joins or leaves the network. Each node has a unique ID which is used to identify the node. Due to the absence of structure supports the nodes that present in network and needs to get prepared with some additional net functionality those include packet forwarding, need to be fortified with a local one-hop intensive care apparatus. The one-to-one monitoring technique helps for finding neighboring nodes between its straight neighbors.

3.2 Trust Model

To achieve security in MANETs, every node which is present in the networkneeds to be genuine. This model helps to determine on which node user can keep trust and on which not. In every security design, 'trust' is very basic and important element.

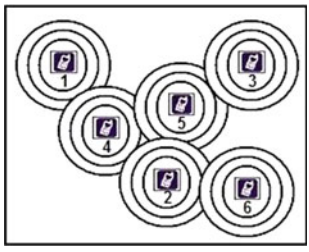

Fig. 1 MANETS with six nodes

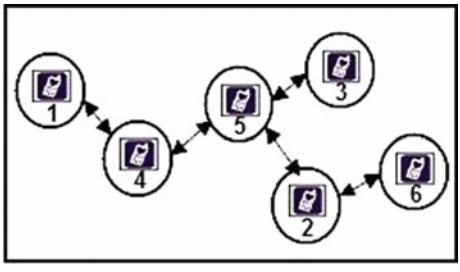

Fig. 2 Accusation graph

Basically, there are two main trust models are available that are trusted third-party model (TTP) [6] and the PGP 'web-of-trust' model [2].

Crepe and Davis [7] proposed a trust mechanism which will help to establish a good trust relationship among the nodes that are present in MANETs as follows: All the nodes in the MANETs maintain 'Profile Table' (PT). This table maintains different information details regarding other nodes that are present in MANETs such as nodes which they have determined as accused and their behavior index β_i. β_i is used to calculate the reputation of each node.

If A_i is large for ith node, then β_i or reputation of ith node decreases the supplementary nodes that do not believe on the accusation completed by the node whose β_i value get decreased. This model defined by [7] helps to establish good trust relationship but the β_i handles only skyjacking nodes. Opponent model is not wide and also not stated, and how the nodes are authentic, what is to be done with the malicious node as well as the process of exchanging PT each time is time-consuming.

A. **Distributed Trust Model**:

We define a scattered trust model. This model gets used to validate the nodes preset in the MANETs. It is also called as a 'trusted third-party model' where 'certificate authority' (CA) will play the role of TTP. We are using the concept of 'secret sharing,' which is based upon Shamir's 'secret sharing model' [8, 9] through threshold cryptography.

Shamir's secret sharing model helps for key management and also provides privacy among a set of nodes N. To protect message generally, we make use of encryption algorithm and encrypt that message to protect it; but what about the key protection which gets used for encrypting message? What will happen with it if it the attacker obtained it? If attacker will succeed to obtain the encryption key using which the message gets encrypted, then that attacker can easily obtain our message and misuse it. So, to avoid damage and to protect message securely we need to use efficient key management technique. Threshold scheme helps to manage encryption key so that message gets protected. In our proposed scheme, we need to protect CA signing key.

Generally, the key is kept at a central location as shown in Fig. 3, if attacker 'E' is able to access 'C' provider, then that attacker can easily obtain the CA signing key 'D' and then by making use of obtained CA signing key, the attacker is able to listen the communication which is done between source 'A' and destination 'B' and thus security get break. This will happen because the secrete key 'D' is stored at a central location and so this scheme is highly unreliable. To avoid this and to protect secrete key, threshold scheme is get used. Threshold scheme was introduced by Shamir in [1, 10].

Using this scheme, user is allowed to divide a CA signing key into 'n' different shares such that $k < n$ as shown in Fig. 4. Data 'D' is nothing but CA signing key in our proposed system. Figure 4 shows that CA signing key is get divided into 'n' parts. Figure 5 shows that it is possible to obtain CA signing key by making use of any 'k' or from more D_i ($D_1, D_2, \ldots D_{k-1}, D_k, D_{k+1}, D_{k+2}, \ldots D_n$) pieces, whereas Fig. 5 shows that it is possible to obtain CA signing key by making use of any 'k' or from more D_i ($D_1, D_2, \ldots D_{k-1}, D_k, D_{k+1}, D_{k+2}, \ldots D_n$) pieces, whereas

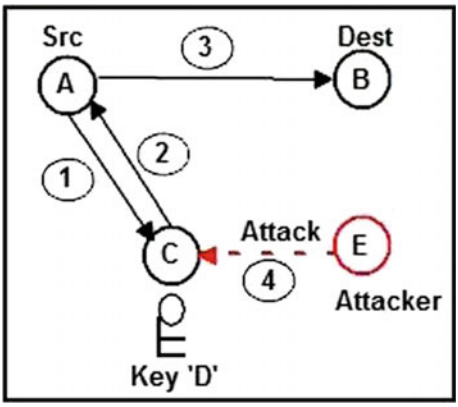

Fig. 3 Without threshold cryptography and secrete sharing (where 'A' → Source 'B' → Destination 'C' → Provider 'E' → Attacker 'M' → Message, 1 'A' makes request to 'C' for obtaining CA signing key 'D', 2 'A' makes request to 'C' for obtaining CA signing key 'D', 3 'A' makes request to 'C' for obtaining CA signing key 'D', 4 'A' makes request to 'C' for obtaining CA signing key 'D')

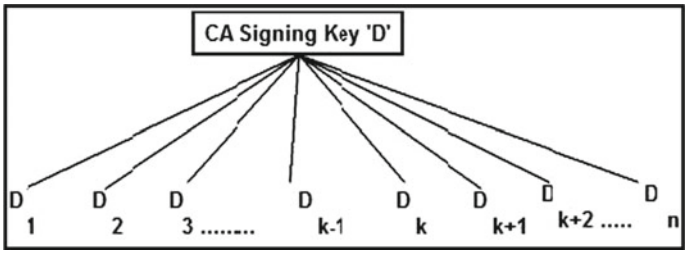

Fig. 4 Without threshold cryptography and secrete sharing

it is not possible to obtain CA signing key by making use of $k - 1$ or fewer D_i (D_1, D_2, $D_3 \ldots$) pieces.

This type of structure is called a (k, n) threshold scheme. For efficient key management and to avoid the drawbacks occurred in Fig. 3, we make use of threshold cryptography. Consider, for example, there is one ad hoc network in which CA private key get used to sign the certificates of each and every node which are present in the network. In this situation, there are two options are available to keep CA private key secure that are.

If we are given a copy of the private key to all the nodes in MANETs so that each node is able to protect their encryption key, then in this situation the system is convenient but there are lots of chances of misuse of key.

If we make use of teamwork mechanism, then to protect CA signing key the cooperation is required among all the node's which are existing in MANETS for signing the certificate of each node. This option will keep our system safe but it is not convenient because every time the cooperation among all the network node is required to sign the certificate of newly entered node. Threshold cryptography (k, n)

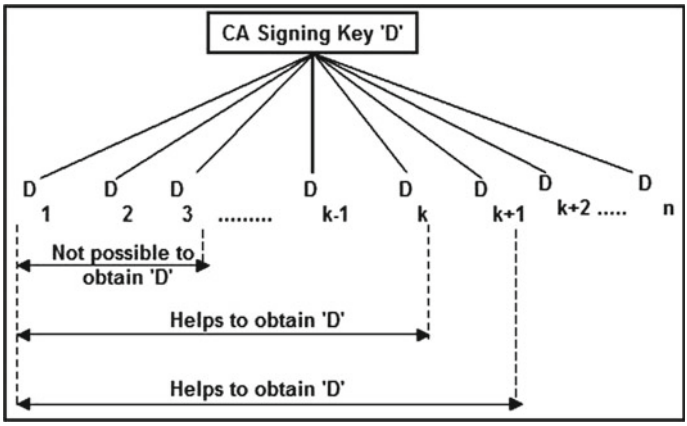

Fig. 5 Obtaining data 'D'

allows us to develop standard solution, for example, if $(k, n) = (3, n)$, then for each node a small piece D_i of CA signing key 'D' is given then to generate a temporary copy of the actual CA signing key 'D'. At least three secretes of signing key 'D' are required, and after using this temporary copy that gets destroyed and in this situation, if any malicious node want to perform any malicious activity such as obtaining CA signing key, then that malicious node requires at least two node's which also want to perform malicious activity and which will help him to obtain CA signing key.

Figure 6 shows that if attacker 'E' is able to perform attack on provider 'C', then also attacker 'E' is not able to obtain CA signing key because it will obtain only one part of signing key 'D', and due to this, attacker 'E' is not able to perform malicious activity.

3.3 Attack Model

This paper focuses on false accusation attack and to some extent with misbehaviors that can occur in network layer. The main feature of network layer is sending the data toward destination, that is, routing and packet forwarding; so our attack model tries to solve false accusation attack, packet forwarding that sends packet to well-behaving destination. In this, we are not considering other attacks that can occur at other layers.

Initially, all the 'N' nodes using which the ad hoc network get created that 'N' nodes are considered as well-behaving nodes so initially the attack can be initiated by a single node. Once the attack gets initiated, then again accusation graph $G = (V, E)$ get updated which will help to find out A_i and β_i depending on the attack that get occurred and then certificate revocation module which is discussed in our previous work [11] and get invoked to determine the value of α_i and ω_i and from all of these

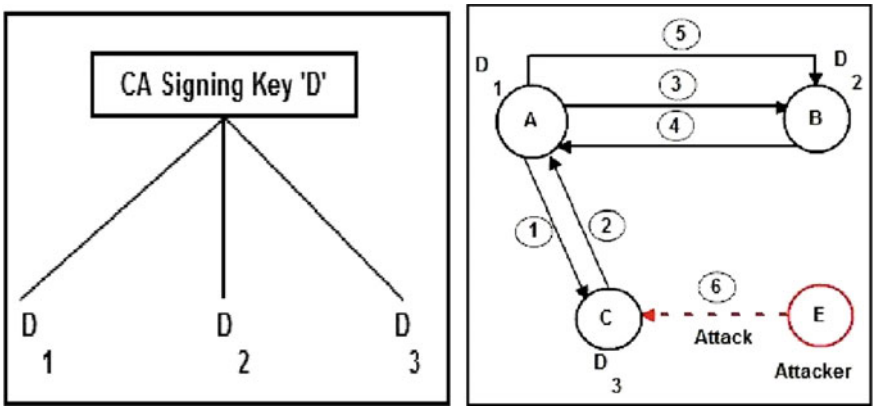

Fig. 6 With threshold cryptography and secrete sharing (Suppose $(k, n) = (3, n)$. Where 'A' → Source 'B' → Destination 'C' → Provider 'E' → Attacker 'M' → Message, 1 'A' request to 'C' for obtaining one piece of CA signing key 'D', D3, 2 'C' gives D3 piece of key 'D' to 'A' after verification and authentication, 3 'A' makes request to 'B' for obtaining other piece of CA key 'D' that is D2, 4 'B' gives D2 piece of key 'D' to 'A' after verification and authentication, 5 'A' will generate temporary key and communicate with 'B', 6 Although 'E' is able to access 'C', 'E' will not be able to perform malicious Activity)

values R_j get calculated. This calculated R_j will help to find out whether it is needed to revoke the certificate of jth node or not. Single or more than one malicious nodes can also target other well-behaving node and then false accusation attack get occurs. When attack gets occurred due to multiple misbehaving nodes, then it is called as joint accusation against well-behaving node.

In this paper, our focus is more toward the insider attacks which can occur due to malicious or selfish nodes. We consider malicious or selfish nodes which are already present in the system. We are considering the attacks caused by single node, as well as by multiple nodes which works within collaboration.

False accusation attack means the spiteful node drive to show the well behaving, nodes as attacker and owing to this the well-behaving node gets removed from MANETs Fig. 7. Demonstrate that user has designed MANETs with four nodes that are i, j, k, and L where well-behaving nodes are indicated by white color and malicious nodes by red color. Initially, all the nodes are considered as a well-behaving node and attack gets initiated by single node suppose that node is 'j'. Then in this situation, if node j will try to prove any well-behaving nodes from the available well-behaving nodes, i, k, and L as malicious node by generating and sending fake accusation message to other nodes except to the node to which that is trying to prove as malicious node and then we can say that the false accusation attack get occurred. Here we are considering that malevolent node j is trying to show genuine node L, as malevolent node then Fig. 7. For this will look like as shown in Fig. 8.

Figure 8 shows the network when malevolent node j will try to prove well-behaving node L, as malevolent node. Node j is generating fake accusation message

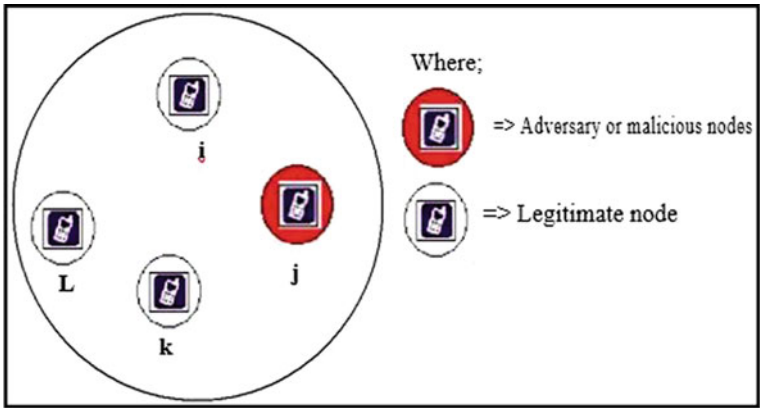

Fig. 7 Original network

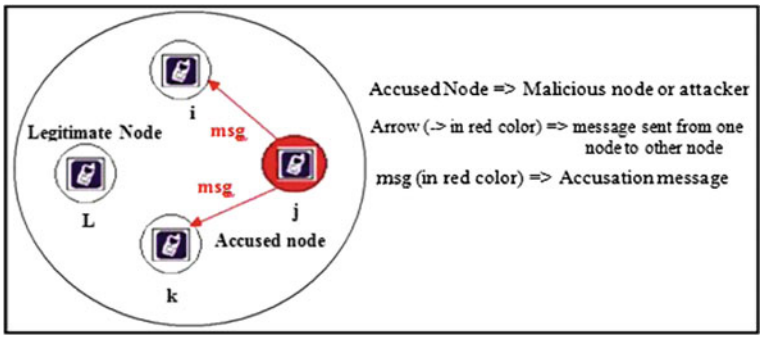

Fig. 8 False accusation attack

and then sends this fake accusation message to node *i* and node *k* to tell them that node *L* is malicious node and by doing this the malicious node *j* in this example is trying to show well-behaving node *L*, as malevolent node in such situation we can say that 'false accusation attack' get occurred in the network, and this will result in the revocation of well-behaving node *L* from the MANETs network while malevolent node leftovers in the network as shown in Fig. 9.

Figure 9 shows the effect of false accusation attack on network shown in Fig. 7. It shows that due to false accusation attack generated by malicious node j for legitimate node *L*, the well-behaving node *L* gets detached from MANETs; however, the malevolent node *j* will present in the network. The original network is shown in Fig. 7. Will result into Fig. 9. Due to false accusation attack.

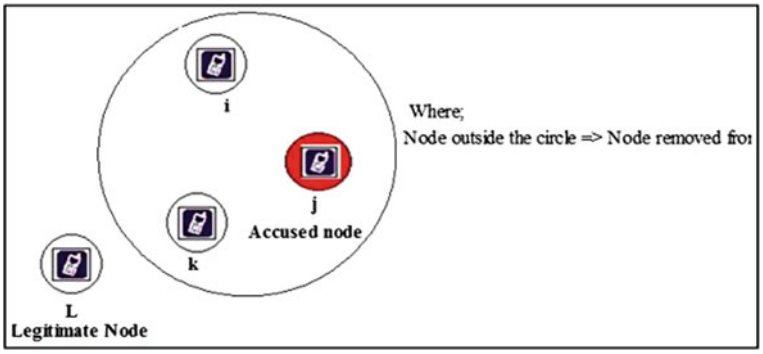

Fig. 9 Effect of false accusation attack

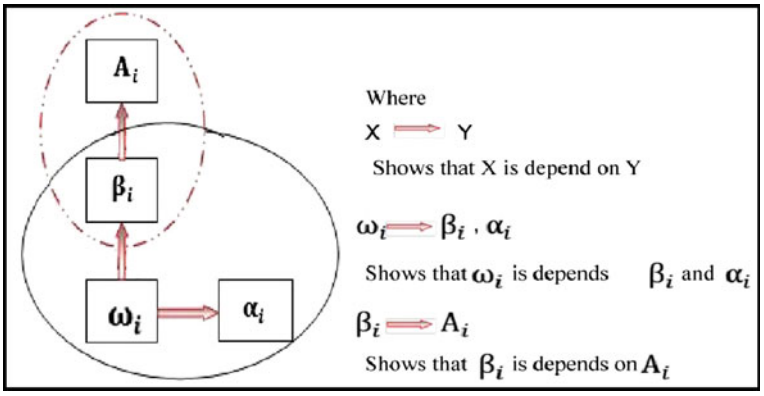

Fig. 10 Effect of false accusation attack

3.4 Planned System Mathematical Model

Figure 10 demonstrates that the mathematical model of planned system.

Parameters A_i, α_i, β_i, ω_i of ST bring variety of information. We refer to recent publication [11] for the detail discussion of the $A_i, \alpha_i, \beta_i, \omega_i$. In planned system, '$N$' represents the number of nodes with which user want to design MANETs. If user has decided to design a MANETs with 'N' numbers of nodes, then extreme number of claim posts which remain allowed A_i agreed as per

$$A_i = \mathrm{Na} - 1 \tag{1}$$

The node does not get charged for first claimed message which is generated, in the planned system. Depending on this situation, amount of claim message aimed at node gets exciting becomes Na − 1. Other important bit is that none of the node present in the MANETs will not produce claim note in contradiction of themselves.

Finally, reduce 1 from Na − 1, for obtaining worth aimed at total amount of claim messages aimed at node charges thus

$$\alpha_i = \text{Na} - 1$$
$$\alpha_i = \text{Na} - 1 - 1$$
$$\alpha_i = \text{Na} - 2 \tag{2}$$

Calculation of equation (1), (2) gives the value for A_i as well as on the value of α_i, as Na − 1, Na − 2 respectively. In Fig. 10, the projectile ($X \Rightarrow Y$) determination specifies that adjustable X is dependent on Y. It also gives information about two different relationships which are present among diverse variables by manufacture use of dotted and plain ovals. Unadorned ovals from Fig. 10 demonstrate the β_i rest scheduled the A_i since β_i get used for calculating the morality of the node. The nodes' honesty is get intended by manufacturing the use total number of claim messages, which are made in contradiction of particular node ith, A_i.

If large number of nodes such as A_i = Na − 1, when Na is the number of node count which are in MANETs has generated accusations message against any node n_i, at that time node n_i is in query that whether it is malevolent node or well-behaving node and due to this less weight get assigned to the claim messages that are generated by node n_i which is in question. So to assign weight to the accusation messages generated by any node n_i proposed system needs to first determine the morality of that node i that β_i which depends on A_i. Therefore, from this obtained β_i

$$\beta_i = 1 - \lambda A_i \tag{3}$$

Scattered oval in Fig. 10 protests that ω_i is rest on β_i and α_i since we know that ω_i is used to assign weight to the claims memo that made by the node i who has detected misconduct of another node j. Then to assign weight to the accusation, we need to determine the honesty of that node i firstly that means β_i which will help to find out the honesty of the node So that depending on that weight is get assigned to claim message made by that node i. So Fig. 10 shows that ω_i depends on β_i which will help to find out behavior of node i. Therefore, from this gained ω_i is:

$$\omega_i = \beta_i - \lambda\alpha_i \tag{4}$$

The value of λ in Eqs. (3) and (4) got as shadow:

$$A_i = \text{Na} - 1 \tag{1}$$
$$\alpha_i = \text{Na} - 2 \tag{2}$$
$$\beta_i = 1 - \lambda A_i \tag{3}$$
$$\omega_i = \beta_i - \lambda\alpha_i \tag{4}$$

Place value of A_i obtained in Eq. (1) into Eq. (3)

$$\beta_i = 1 - \lambda A_i \tag{3}$$

$$\beta_i = 1 - \lambda(\mathrm{Na} - 1) \tag{5}$$

Place value of α_i obtained in Eq. (2) into Eq. (4)

$$\omega_i = \beta_i - \lambda\alpha_i \tag{4}$$

$$\omega_i = \beta_i - \lambda(\mathrm{Na} - 2) \tag{6}$$

Place value of β_i obtained in Eq. (5) into Eq. (6)

$$\begin{aligned}\omega_i &= \beta_i - \lambda(\mathrm{Na} - 2)\\ &= 1 - \lambda(\mathrm{Na} - 1) - \lambda(\mathrm{Na} - 2)\\ &= 1 - \lambda[(\mathrm{Na} - 1) + (\mathrm{Na} - 2)]\\ &= 1 - \lambda[(\mathrm{Na} - 1 + \mathrm{Na} - 2)]\\ &= 1 - \lambda[(\mathrm{Na} + \mathrm{Na} - 1 - 2)]\\ &= 1 - \lambda[(2\mathrm{Na} - 3)]\end{aligned} \tag{6}$$

$$1 = \lambda[(2\mathrm{Na} - 3)] \quad \text{Thus} \quad \lambda = \frac{1}{2\mathrm{Na} - 3}$$

4 Conclusion

In this paper, we have extended our previous work on certificate revocation to achieve better security and efficient key management by distributing certificate authority's functionality through threshold secrete sharing. Our work is divided into five phases that consists of creating ad hoc network, establishing trust among the nodes, distributing certificate authority's functionality, generating attack, and removing it. We used Shamir's secret sharing model with severance to reduce the effect of malicious node because it states that by using less than $(k - 1)$ pieces, it is not possible by attacker to recreate the certificate authority key, and thus, it will help to improve the integrity of the ad hoc network. The proposed scheme removes window of opportunity problem, false accusation attack, improves reliability of network, achieve efficient key management. For certificate revocation, our proposed scheme takes the reliability of each node into consideration and depending on the nodes reliability it assigns weight ω_i to each accusation message A_i made by nodes which will help to take decision about whether to revoke the certificate of node or not.

References

1. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
2. Zimmermann P (1995) The official PGP user's guide. MIT Press, Cambridge
3. Liu W, Nishiyama H, Ansari, Nakao (2011) A study on certificate revocation in mobile ad hoc networks. IEEE
4. Luo H, Kong J, Zerfos P, Lu S, Zhang L (2004) URSA: ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Trans Netw 12(6):1049–1063
5. Arboit G, Crepeau C, Davis CR, Maheswaran M (2008) A localized certificate revocation scheme for mobile ad hoc networks. Ad Hoc Netw 6(1):17–31
6. Perlman R (1999) An overview of PKI trust models. IEEE Netw 13(6):38–43
7. Crepe C, Davis C (2003) A certificate revocation scheme for wireless Ad hoc networks. 1st ACM workshop on security of ad hoc and sensor networks, pp 54–61
8. Stamatios V (2009) Security of information and communication networks. Wiley-IEEE Publications, USA
9. Wikipedia (2011) Shamir's secret sharing. Available at: http://en.wikipedia.org/wiki/Shamir"s_Secret_Sharing, last visited 2011
10. Luo J, Hubaux JP, Eugster PT (2005) DICTATE: Distributed CerTification Authority with probabilisTic frEshness for ad hoc networks. IEEE Trans Dependable Secure Comput 2(4):311–323
11. Rathi P, Mahalle P (2013) Proposed threshold based certificate revocation in mobile ad hoc networks. ICACNI 243(2014):377–388
12. http://essaymonster.net/technology/13772-proposed-threshold-based-certificate-revocation.html
13. Sabeena S (2014) Reduced overhead based approach for secure communication in mobile ad hoc networks. IOSIR-JCE 16(5), Ver. III:73–78

Priti Rathi has completed her BE in computer science and engineering in 2010 and M. Tech in 2014 from Pune University. She has achieved distinction throughout academic examination in BE and having 2 years of experience in teaching. Currently, she is working in 'Gokaraju Rangaraju Institute of Engineering and Technology,' in Hyderabad, as 'Assistant Professor.'

Kanika Bhalla has completed her B. Tech in computer science and engineering in 2010 and M. Tech in Software Engineering in 2014, Engineering College, Rajasthan. Currently, she is working in 'Gokaraju Rangaraju Institute of Engineering and Technology,' in Hyderabad, as 'Assistant Professor' and having 5 years of teaching experience.

Dr. Ch. Mallikarjuna Rao received the B. Tech degree in computer science at Maharashtra in 1998 and M. Tech from JNTU Anantapur, Andhra Pradesh, in 2007, and Ph.D. from JNTU Anantapur. Currently, he is working in 'Gokaraju Rangaraju Institute of Engineering and Technology,' in Hyderabad. His areas of interest are data mining, big data, and software engineering.