ISSN:0975-9646

Efficient Certificate Revocation with Vindication Capability for Mobile Ad-Hoc Networks

[1]Nausheen Shamsi, [2]Ranjana B Nagagoudar, [3]Amareshwari Patil

[1]P.G.Student, Department of Computer Science & Engineering, VTU RO PG Centre,
Gulbarga, Karnataka, India.
[2]Associate Professor, Department of Computer Science & Engineering, VTU RO PG Centre,
Gulbarga, Karnataka, India.
[2]Associate Professor Department of Computer Science & Engineering, PDACE
, Gulbarga, Karnataka, India.

Abstract– **Mobile ad-hoc networks are self-organizing and self configurable with an open network environment. The nodes in this network can join and leave the network freely. Therefore, the wireless and dynamic natures of MANET make them more vulnerable to various types of security attacks than their wired counterparts. To guarantee the secure network services certificate revocation is an important integral component. In our proposed scheme, when the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. In this paper we propose Certificate Revocation with Vindication Capability scheme which gives quick and accurate certificate revocation. To improve the reliability of scheme warned nodes are recovered to take part in the certificate revocation process. We propose a new method to enhance the effectiveness and efficiency of the scheme by employing a threshold based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.**

Keywords: **Cluster, certificate revocation, Mobile ad hoc networks (MANETs), security, and threshold.**

I. INTRODUCTION

With the recent advances in wireless communication technologies Mobile Ad-hoc Network has attracted much attention due to their mobility features, dynamically changing topology and ease of deployment. MANET is a highly flexible network with no fixed infrastructure formed by a number of self-organized mobile devices such as laptops, cell phones, and Personal Digital Assistants (PDAs). In addition to mobility mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multihop relaying. Application areas range from conference hall networks to ad hoc networks for emergency and rescue operations and military operations.

Another feature of MANET is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANET expose them more vulnerable to various types of security attacks than the wired network. Among all security issues in MANET, Certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure [1],[2] to secure the applications and network services. For certificate management a complete security solution must encompass three components such as prevention, detection and revocation. Many research effort took place in some areas such as certificate distribution [3][4], attack detection[5][6] and certificate revocation[7][8][9][10][11].

In order to secure network communication, certification is considered as a prerequisite. The public key is encrypted into an attribute using the digital signature of the issuer. It is used to assure that a public key belongs to an individual and helps in preventing tampering and forging in Mobile ad hoc networks. If any attack is identified certificate plays a major task of enlisting and removing the certificates of nodes which have been detected to launch attacks in the neighborhood. Certificate revocation's basic security problem is aimed at providing secure communications.

II. RELATED WORK

To enhance the network security a number of certificate revocation techniques have been proposed in the literature. The existing approaches for certificate revocation are basically classified into two categories: voting-based mechanism and non-voting-based mechanism.

A. *Voting-Based Mechanism*

The voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes.

URSA [7] proposed a voting-based mechanism to evict the nodes. The certificates of newly joining nodes are issued by their neighbors as a certified ticket. In this mechanism, each node performs one hop monitoring and exchanges their monitoring information with their neighboring nodes. There is no third party like Certification Authority (CA) in these networks; the certificate of a suspected node can be revoked when the number of access against the node exceeds a certain threshold. Threshold detection remains challenge. If network degree is much smaller than its nodes that can launch attacks cannot be revoked and keep successfully communicating with other node. False accusation which are malicious are not addressed from nodes is a critical issue.

G. Arboit et al [8] proposes the scheme which allows all nodes that are connected in the network to vote together. As like in URSA, no certificate authority exists in the network, but each node plays a role of monitoring the behavior of its neighbors. The primary difference from URSA is that nodes vote with different weights. The variable weight of a node is calculated on the basis of reliability and trustworthiness of that node from its past behavior. The stronger its reliability, the acquired weight is increased. If the weighted sum of votes exceeds a predefined threshold, certificate of an accused node will be revoked. This improves the accuracy of certificate revocation. However, the communication overhead used to exchange voting information would be high and it increases the revocation time because all nodes are required to participate in each voting.

B. Non-Voting-Based Mechanism

In the non-voting based mechanism a node with a valid certificate will decide a node as a malicious attacker to revoke its certificate.

J. clulow et al [9] proposed the decentralized suicide-based approach "suicide for the common good strategy, revoke the certificate by only one accusations. This will simultaneously revoke the certificates of both the accused node and accusing node to remove an attacker from the network; the accusing node has to sacrifice itself. Although this approach dramatically reduces both the time required to evict a node and communication overhead. This suicidal approach does not take into account to differentiate falsely accused nodes from genuine malicious attackers.

Park et al. [10] proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. A trusted certification authority is responsible to hold the accuser and accused node in the warning list (WL) and blacklist (BL) and manages control messages, respectively. Further, it also deals with the issue of false accusation the certificate of the malicious attacker node can be revoked by any single neighboring node. It takes short time to complete certificate revocation process.

III. Existing System

A Cluster-based Certificate Revocation in the combination of voting-based and non-voting-based mechanism. This system contains the centralized Certificate Authority unit along with the cluster, which is responsible for the performance of cluster head with its cluster member. The certificate validation is done by CA for both accusing and accused node to be put into Warned list and Blacklist. The WL contains the accusing node of the cluster and BL contain the accused node which is deemed as a malicious attacker. If the node in the BL is considered as false accusation then it will be recovered and placed in the WL of the network. But in future the accusing nodes, in WL can be used as a cluster member for the communication if it's known to be a legitimate node.

A. Disadvantage

Due to false accusation of the legitimate node as a malicious attacker the effectiveness and robustness and the accuracy of this scheme will be degraded.

IV. Proposed System

The proposed scheme presents a Cluster-based Certificate Revocation with Vindication Capability. The proposed scheme inherits the merits of both the voting-based and non-voting-based schemes in achieving prompt revocation and lowering overhead as compared to the voting-based schemes , improving the reliability and accuracy as compared to the non-voting-based scheme. The proposed scheme won't have false accusation of legitimate node as an attacker. The proposed scheme also contains two lists WL and BL, where BL is composed of completely revoked node of the cluster (i.e.,) the node which can't be recovered in any condition. Initially the WL contains both the accusing and accused node of cluster, the nodes in the WL is analyzed to identify the attacker node of the specific cluster which is revoked completely from the network and stored in BL.

A. Modules of the Cluster-Based Scheme

The proposed CCRVC scheme has three different modules in their design. The entire process is summarized in the Fig. 1.

1) Cluster Construction
2) CA Function
3) Certificate Revocation

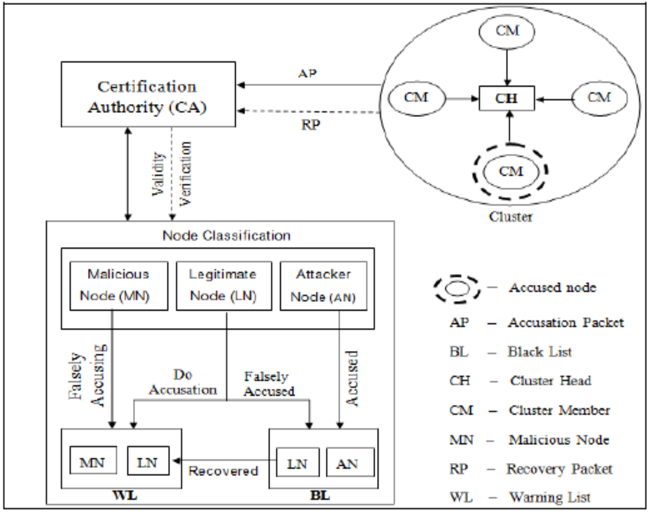


Fig. 1: System Modules

1) Cluster Construction:

Nodes cooperate to form the clusters, and each cluster consists of a CH along with some cluster members. Before nodes can join the network, they have to acquire valid certificates from the CA, which is responsible for managing and distributing certificates of all nodes so that nodes can communicate with each other unrestrainedly in a MANET. When a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. Node clustering provides a means to mitigate false accusations. Fig.2 shows an example of how clusters are constructed in the proposed system.

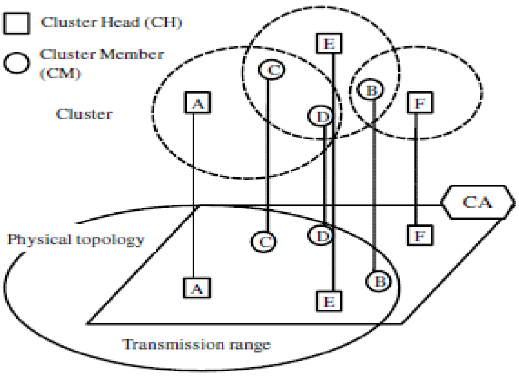


Fig. 2: Node Clustering

Nodes except CH join two different clusters of which CHs exist in the transmission range of them. By constructing such clusters, each CH can be aware of false accusation against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM. To, maintain clusters, CH and CMs frequently confirm their existence by exchanging messages i.e., the CH periodically broadcasts CH Hello Packets to the CMs within its transmission range, and each CM replies to the CH with the CM Hello Packet.

2) *CA Function:*

To enable each mobile node to preload the certificate, Certification Authority (CA), is deployed in the cluster-based scheme. The CA is also responsible for revocation of nodes in network and maintains WL and BL for accusing and accused node. The CA updates each list according to received control packets.

In the proposed scheme, nodes are differentiated according to their reliability into three types of nodes: legitimate, malicious, and attacker nodes

- A legitimate node is deemed to secure communication with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively and for revoking their certificates.
- A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attacker.
- An attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communication in the network.

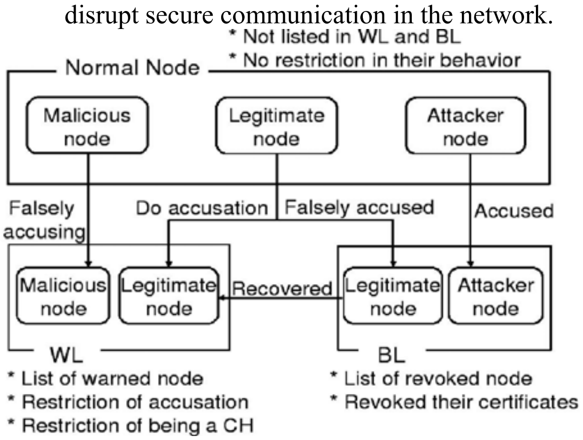


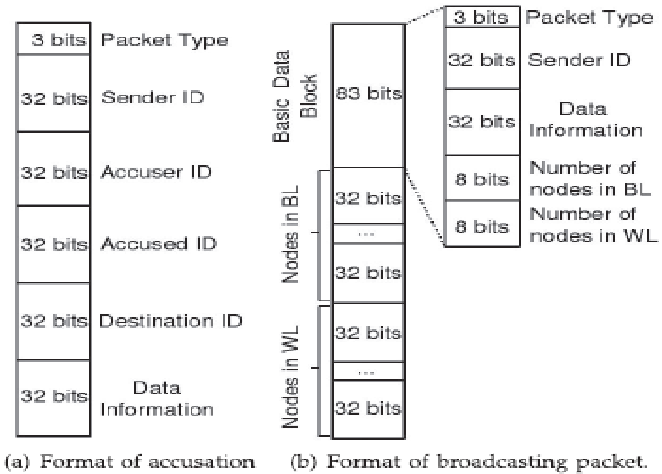
Fig. 3: Classification of Nodes

Fig. 3 shows the classification of nodes in our proposed scheme. Nodes in a cluster can be further classified into three categories based on their reliability, i.e., *normal nodes* have a high reliability, *warned nodes* are suspected as potential attackers, and *revoked nodes* have been accused by a normal node. When nodes join the network, they are assumed to be normal nodes. Warned nodes and revoked nodes are listed in the Warning List (WL) and Black List (BL), respectively. The certificates of the nodes listed in BL are revoked whereby they are removed from the network. While the nodes included in WL can communicate with other nodes in the same way as normal nodes, there are a few restrictions placed on their behavior, i.e., unable to become a cluster head and not allowed to make any accusation

3) *Certificate Revocation:*

3.1 Revoking Malicious Certificates

The revocation procedure begins at detecting the presence of attacker from the node. When the neighboring nodes detect attacks from any one node then each node sends out an accusation packet Certificate Authority (CA) against the attacker node, the format of accusation packet is sown in Fig. 4a. After receiving the first AP, the CA verifies the certificate validation of the accusing node, and the accused node is deemed as a malicious attacker to be put into the BL. While the accusing node is held in the WL. Finally, by broadcasting the revocation message (as shown in the format of broadcasting packet in Fig. 4b) including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.



(a) Format of accusation and recovery packets. (b) Format of broadcasting packet.

Fig. 4: Control Packets

The procedure of revocation is described with the following example, such that when a malicious attacker A launches attacks within one-hop range as shown in Fig. 5.

- Node A is a malicious node and launches attacks on its neighbors i.e., nodes B,C,D and E
- Each of the neighboring node detects the attacks and sends an accusation packet to the CA against A.

- According to the first received packet from node B, the CA holds B into WL as an accuser and A into the BL as an attacker.
- The CA broadcast the revocation message to all nodes in the network.
- Nodes in each cluster update their local WL and BL to revokes A's certificate.

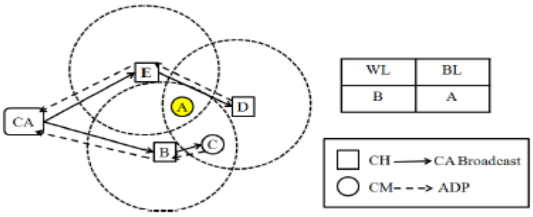


Fig. 5: Revoking a node's certificate

3.2 False Accusation

The accuracy and robustness of cluster-based scheme will be degraded due to false accusation. By adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes. As each CH can detect all attacks from its CMs, request for the CA to recover the certificate of the falsely accused node by sending Recovery Packet (RPs) (as seen in the Fig. 4a) to the CA. After receiving the recovery packet from the CH, the falsely accused node can be removed by CA.

CH updates their WL and BL and determines that one of the nodes was framed. Since the CH does not detect any attacker from a particular accused member enlisted in the BL from the CA, the CH becomes aware of the occurrence of false accusation against its CM. Then, the CH sends a recovery packet to the CA in order to vindicate and revive this member from the network. Then the falsely accused node will be released from the BL and held in the WL. The CA propagates this information to all the nodes through the network. Fig. 6 illustrates the process of addressing false accusation as follows.

- CA broadcasts the information of the WL and BL to all nodes in the network.
- Node E and F which are CH of node A update their WL and BL, and determine that node A was framed.
- E and F send a recovery packet to the CA to recover node A's certificate that was falsely accused.
- Upon receiving the first recovery packet from node E, the CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E.
- The nodes update their WL and BL, the certificate of node A will be recovered.

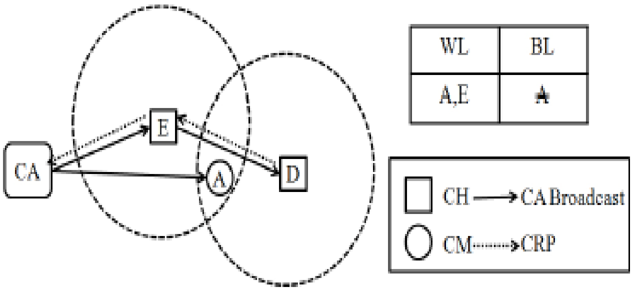


Fig. 6: False accusation

V. System Design

Our Certificate revocation scheme employs threshold based mechanism to effectively construct the revocation procedure. Therefore, here we present the detailed design of three elements in our scheme:

A. Depreciation of Normal Nodes
B. Node Release Method
C. Determining the Threshold

A. *Depreciation of Normal Nodes*

Our proposed scheme can effectively reduce the revocation time and communication overhead. However, there exists an issue which affects the performance of the scheme. Since the CA does not accept accusation packets from nodes enlisted in WL in order to prevent further damage from malicious nodes. Hence nodes enlisted in the WL lose the function of accusation. Therefore the revocation and recovery operations incur an increasing number of normal nodes to be held in the WL, subsequently leading to the reduction of the number of normal nodes over time. Such scenario will affect the reliability of the scheme.

Intuitively, if there are sufficient normal nodes around malicious attackers, the scheme is efficient in revoking attackers rapidly. On the contrary, the efficiency degrades when there are not enough normal nodes in the network. The scheme cannot detect and revoke this attacker immediately until a normal node roams into the attacker's transmission range.

In a MANET, mobile nodes are assumed to be uniformly distributed over a coverage area so as to satisfy the binomial distribution $B(n,p)$ which denotes the probability of a number of nodes existing in a specified network area, where n denotes the total number of cells in the network; p is the probability that one cell is occupied by a single node. The binomial distribution $B(n,p)$ is approaching the Poisson distribution with parameter λ, when n is very large and p is very small, which is equal to the number of nodes, np.

Therefore, the probability that there are exactly k normal nodes (k being a non-negative integer, $k = 0,1,2 ...$) in a specific area in MANETs is equal to

$$\Pr(k) = \frac{\lambda^m e^{-\lambda}}{m!} = \frac{(\theta\rho S)^m e^{-\theta\rho s}}{m!} \qquad (1)$$

Where ρ is the node density, which is dependent on the location in space; θ is the proportion of normal nodes in the network; S represents the transmission area of a malicious node.

As the number of accused malicious nodes increases, the number of normal nodes decreases in the network. If $k = 0$ i.e., there are no normal nodes within the transmission range of a malicious node, the probability is

$$\Pr(k = 0) = e^{-\theta\rho s} \qquad (2)$$

From (2) the probability $\Pr(k = 0)$ greatly increases with the decrease of density ρ; the efficiency of detecting attacker is significantly reduced. Therefore the performance of the scheme is dependent on the density of normal nodes.

Hence, to enhance the robustness and reliability against the decreasing number of normal nodes, the legitimate nodes should be released from the WL and be restored of their accusation function.

B. *Node Release Method*

To release the node from the WL, we consider the two different ways for nodes that are to be listed in the WL as shown in the Fig. 3

- In the first case a legitimate node correctly accuses an attacker node, with the accusing node and accused node being listed in the WL and BL, respectively.
- Second has the enlisting of a malicious node in the WL because it sends false accusation against a legitimate node.

Hence to improve the reliability and accuracy of the scheme, nodes must be differentiated between legitimate nodes and malicious nodes.

We propose a node releasing mechanism to evaluate and release legitimate nodes from the WL by distinguishing legitimate nodes from malicious nodes as follows

- A counter is designed for the CA to record the number of accusations against each accused node.
- CA continues to receive accusations against the accused node with a voting period of time T_v.
- Voting period T_v is used for collecting accusations and releasing legitimate nodes from the WL and subsequently compare the number of received accusation with the threshold K.

If the number of accusation reaches threshold K then the accused node is considered as a real attacker. In the mean time, we can finally vindicate the corresponding accusing node as a legitimate node so as to release it from the WL and restore its function as the normal node. If the number of accusations fails to reach threshold K, the related accusing node will be detained in the WL.

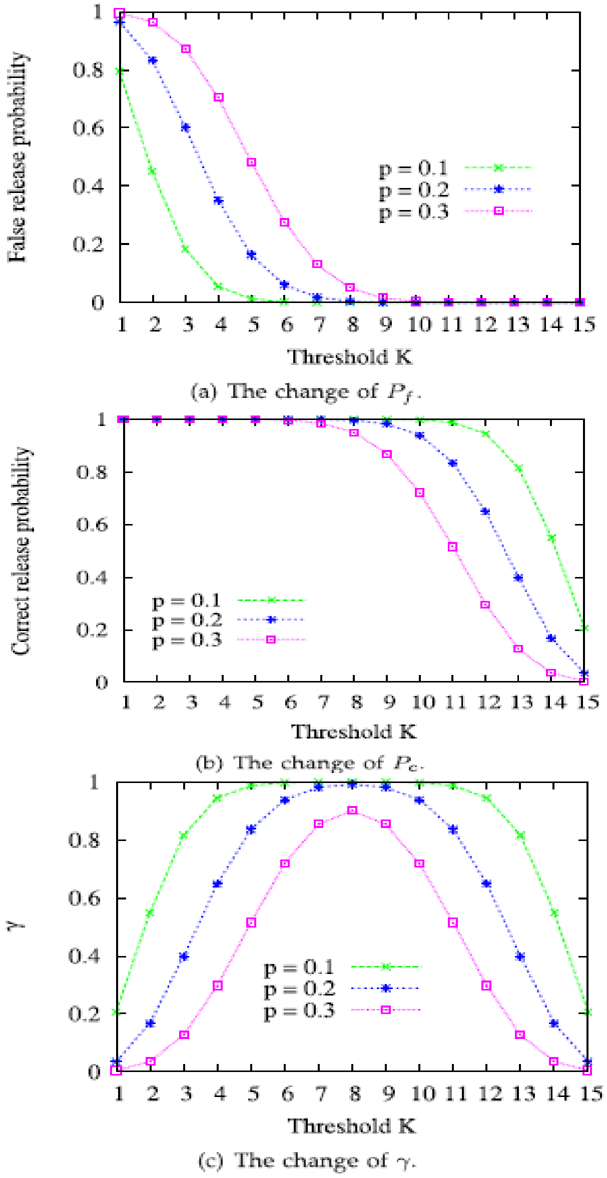
In the conventional voting mechanism the threshold K is set to a constant value. If the threshold is set too big, it will take long time to determine whether a warned node is a legitimate node because the scheme has to wait for more accusation to reach the verdict. Conversely, if threshold is set too small, revoked malicious nodes can be released from the WL by other malicious nodes through collusion.

C. *Determining the Threshold*

We determine the number of neighboring nodes for a given node through a simplified mechanism. Within timeT_v, the given node crosses through an area and meets a number of neighbors N. As mobile nodes are assumed to be uniformly distributed in the network, we may approximate N by

$$N = (\pi r^2 + 2rvT_v)\rho \qquad (3)$$

Where r denotes the transmission range of nodes, v is the velocity, and ρ is the density of nodes in the network. According to the obtained number of nodes N, we can confirm the value of threshold K. In our proposed scheme we determine the threshold K in three different cases as.



(a) The change of P_f.

(b) The change of P_c.

(c) The change of γ.

Fig. 7: Impact of threshold K *on* P_f, P_c, γ for different values of p with $N = 15$

Case1: Minimizing the False Release Probability

In this case we set the value of threshold K such that the probability P_f is not less than K out of N neighbors falsely accuse the given node:

$$P_f(K) = \sum_{i=K}^{N} \binom{N}{i} p^i (1-p)^{N-i} \qquad (4)$$

Where P_f denotes the probability that a legitimate node is framed by K colluding nodes so that the malicious node is released erroneously p denotes the probability of a node which participates in false accusation. From Fig. 7a shows that (4) is a monotonically decreasing function where $N = 15$. It also demonstrate that greater the threshold K is, fewer the malicious node is falsely released; and thus higher the accuracy is. Therefore, we expect to acquire the minimum value of P_f to reduce the probability of falsely releasing nodes from the WL.

Case 2: Maximizing Correct Release Probability

For this correct release probability the value of K is determined on the basis of the probability P_c not less than K out of N neighboring nodes can correctly accuse the attacker so that a legitimate node will be successfully released from the WL.

$$P_c(K) = \sum_{i=K}^{N}\binom{N}{i}(1-p)^i p^{N-i} \qquad (5)$$

where $(1-p)$ means the probability of a node which participates in correct accusation. For successfully releasing legitimate nodes from the WL, the value of P_c should be large. As shown in Fig. 7b P_c drops as the threshold K increases, it also illustrates the probability that a legitimate node is permanently held in the WL increases when K becomes large.

Case 3: Maximizing Accuracy

To choose an appropriate value of K to achieve the maximum accuracy of releasing nodes that can increase correct release probability while simultaneously maintain low false release probability. Hence, we propose $\gamma(K)$ to determine the optimum threshold, where $\gamma(K)$ equals the difference between P_c and P_f

$$\gamma(K) = P_c(K) - P_f(K)$$
$$= \sum_{i=K}^{N}\binom{N}{i}\{(1-p)^i p^{N-i} - p^i(1-p)^{N-i}\}$$
(6)

In our scheme, the total number of malicious nodes and attacker nodes is supposed to be less than the number of legitimate nodes in MANETs i.e., $(1-p)$ is greater than p. Taking $N = 15$, Fig. 7c shows that the curve of $\gamma(K)$ is maximum when K is equal to $\frac{N}{2}$.

To prove that $\gamma(K)$ achieves the maximum when K is equal to $\frac{N}{2}$. From (6) we need to show that $\gamma(K)$is monotonically increasing for K belongs to [0, $\frac{N}{2}$] and is monotonically decreasing for K belongs to [$\frac{N}{2}$, N]. We assume $K1 < K2$ such that$0 \le K1 < K2 \le N$.

$$\gamma(K2) - \gamma(K1)$$
$$= \sum_{K=K1}^{K2-1}\binom{N}{K}\{(1-p)^K p^{N-K} - p^K(1-p)^{N-K}\} \qquad (7)$$
$$= \sum_{K=K1}^{K2-1} A\{p^{\frac{N}{2}-K} - (1-p)^{\frac{N}{2}-K}$$

Where

$$A = \binom{N}{K}\{(1-p)^K p^{\frac{N}{2}} + (1-p)^{\frac{N}{2}} p^K\}$$

.

VI. Evaluation

A. *Investigation of Threshold Value K*

By using the above case 1 or 2, we first set the value of α or β to get the threshold value K. If we choose less α, the larger the threshold will be i.e., P_f decreases as α decrease. However, while P_f is decreasing, P_c is also decreasing thus leading to decreasing thus leading to decreased probability of releasing legitimate nodes from the WL, and vice versa. As shown in Table 1, with different values of α and β *K* varies with different settings. Therefore to determine the optimal threshold K to keep balance between P_f and P_c. We use case 3 to achieve maximum accuracy to judge the identity of nodes in the WL, thus enhancing the correct release probability while maintaining low false release probability simultaneously. From Table 1, the results show that K is constant and equal to $\frac{N}{2}$ where γ obtains the maximum accuracy by using case 3.

TABLE I
NUMERICAL RESULTS FOR $K(N = 15)$

p	Policy1($P_f \le \alpha$)		Policy 2($P_c \ge \beta$)		Policy 3
	$\alpha = 0.1$	$\alpha = 0.2$	$\beta = 0.9$	$\beta = 0.8$	
0.1	4	3	12	13	8
0.2	6	5	10	11	8
0.3	8	7	8	9	8

B. *Advantages*

1. The threshold K=$\frac{N}{2}$ is the optimum value to distinguish legitimate nodes from malicious nodes.
2. The proposed scheme exhibits more reliable and higher efficiency as compared to the existing ones.
3. It guarantees sufficient normal nodes to revoke the certificates of the attackers and takes a short revocation time.
4. It achieves high accuracy in releasing legitimate nodes.

VII. Conclusion

In this paper, we have addressed the issue of Secure Communication for mobile ad-hoc networks by using the certificate revocation of attacker nodes. The proposed cluster-based certificate revocation with vindication capability scheme combined with merits of both voting-based and non-voting-based mechanism to revoke malicious certificate and solve the problem of false accusation.

The scheme can revoke an accused node based on a single nodes accusation, and reduce the revocation time as compared to the voting-based mechanism. In addition, falsely accused nodes are restored by the CH in the cluster based model, which improves the accuracy as compared to the non-voting based mechanism. The legitimate nodes are released and restored in a new incentive method which also improves the number of available normal nodes in the network for ensuring the efficiency of quick revocation.

ACKNOWLEDGEMENTS

I would like to express my sense of proud gratitude and indebtedness to my guide, for his valuable guidance, suggestions, timely supervision for successful completion of my paper. Above all I would like to thanks all my family members and friends for their constructive criticism and construct support in making this grand success.

REFERENCES

[1] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "*A Survey of Key Management in Ad Hoc Networks,"* IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[2] L. Zhou and Z.J. Haas, *"Securing Ad Hoc Networks,"* IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[3] L. Zhou, B. Cchneider, and R. Van Renesse, *"COCA: A Secure Distributed Online Certification Authority,"* ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[4] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan*, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks,"* IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp. 233-247, July 2005.

[5] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, *"Resisting Flooding Attacks in Ad Hoc Networks,"* Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

[6] B. Kannhavong, H. Nakayama, A. Jamalipour, Y.Nemoto, and N. Kato, *"A Survey of Routing Attacks in MANET,"* IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

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

[8] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran*, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks,"* Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[9] J. Clulow and T. Moore*, "Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,"* ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

[10] K. Park, H. Nishiyama, N. Ansari, and N. Kato, *"Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks,"* Proc. IEEE 71st Vehicular Technology Conf. (VTC '10), May 16-19, 2010.

[11] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, *"A Study on Certificate Revocation in Mobile Ad Hoc Network,"* Proc. IEEE Int'l Conf. Comm. (ICC), June 2011.