ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Elimination of the Certified Maliciousnode in the MANETs with the Vindication Capability

Ranjana B Jadekar[1], Shivanand M Patil[2]

M. Tech Student, Department of CSE, KLE Dr.MSSCET, Belagavi, Karnataka India[1]

Assistant Professor, Department of CSE, KLE Dr.MSSCET, Belagavi, Karnataka, India[2]

ABSTRACT: In survey of providing security to the MANETs, many researchers had come with many methods, Certification revocation is one among them, this technique is widely used and most efficient. So in this paper am also using the certification revocation method with the voting- based mechanism to revoke the malicious node in the network. Here we have a module called Certification Authority CA, this module has the control over the every node in the network, CA has the capability to issue the certificate to nodes wants to enter into our network and also the certificate revocation of the malicious node based on the voting-based mechanism. The certificate verification involves maintaining secure connections against invalid certificates; and the certificate validation by CA or the server examines the certificates to check the recipient's identity. If the certificate of the malicious node is revoked, then it is impossible to communicate with any other nodes in the network. By doing so, it is possible to have Cluster-to-Cluster communication in a secure manner.

KEYWORDS:MANETs, Cluster construction, Certificate Revocation, vindication capability, warning list, blocked list, Certification authority.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a group of devices or nodes that transmit across a wireless communication medium.There will be no centralized control or network infrastructure for a MANET. [18] MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a dynamic wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks. Among all security issues in MANETs, certificate management is a widely used mechanism. Security is one crucial requirement for these network services.Implementing security [3], [4] is therefore of prime importance in such networks. Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure [3], [5] to secure applications and network services. Tremendous amount of research effort has been made in these areas, such as certificate distribution [6], [7], attack detection [8], [9], [10], [11], and certificate revocation [12], [13], [14], [15], [16], [17], [18], [1].

II. RELATED WORK AND MOTIVATION

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting based mechanism and non-voting-based mechanism [1]. In this paper we have concentrated only on the non-voting-based mechanism because of its benefits over the voting based mechanism

DOI: 10.15680/ijircce.2015.0306125

A. Voting-Based Mechanism

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighbouring nodes. Proposed uses a voting-based mechanism to evict nodes. The certificates of newly joiningnodes are issued by their neighbours. The certificate of an attacker is revoked on the basis of votes from its neighbours.Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Determining the threshold, however, remains a challenge. Analyse both advantages and disadvantages of voting-based and non-voting-based schemes, focusing our attention on their merits to improve certificate revocation [1].

B. Non-Voting-Based Mechanism

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate [1].A fully distributed scheme called "suicide for the common good" strategy[17], where certificate revocation can be quickly completed by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously.Cluster based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. The certificate of the malicious attacker node can be revoked by any single neighbouring node [18].

C. Motivation

As discussed above, we compare the advantages and disadvantages between voting-based and non-voting-based mechanisms. The significant advantage of the voting-based mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision process to satisfy the condition of certificate revocation is, however slow. Also, it incurs heavy communications overhead to exchange the accusation information for each other. On the contrary, the non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. It is able to drastically simplify the decision making process for rapid certificate revocation as well as reduce the communications overhead. However, the accuracyof determining an accused node as a malicious attackerthe reliability of certificate revocation will be degradedas compared with the voting-based method. We emphasizethe significant performance difference between votingbasedand non-voting-based methods: the former achieveshigher accuracy in judging a suspicious node, but takes alonger time; the latter can significantly expedite therevocation process.CRVC 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 scheme, improving the reliability and accuracy as compared to the non-voting-based scheme. Our schema can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security [1].

III. CLUSTER CONSTRUCTION IN MANET

A. Architecture of MANETs

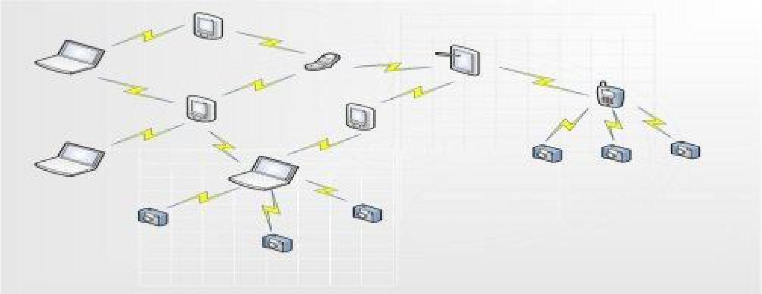

Fig1: Architecture of MANETs

DOI: 10.15680/ijircce.2015.0306125

A mobile ad hoc network is a dynamic wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks [1]. In the proposed system dynamic wireless cluster is constructed, the aim here is to provide security to the running environment, by the static assignment of heads and members in a cluster, and there is a CA certification authority which is authenticates the cluster members.

B. Function of Certification Authority

Certification Authority CA is a module in our system which plays a very major role, CA maintains the central based authority which performs the id distribution to nodes in which they wish to come to our environment, and also maintains the transactions of the every node in the network, [18]a trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Blacklist, which are used to hold the accusing and accused nodes' information, respectively. Concretely, the BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node. The CA updates each list according to received control packets. Note that each neighbour is allowed to accuse a given node only once. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network.

C. Node Classification

According to the behaviour of nodes in the network, nodes are classified according to their behaviours:legitimate, malicious, and attacker nodes[18]. The classification of these kinds of nodes is summarized in Fig. 2 [1],

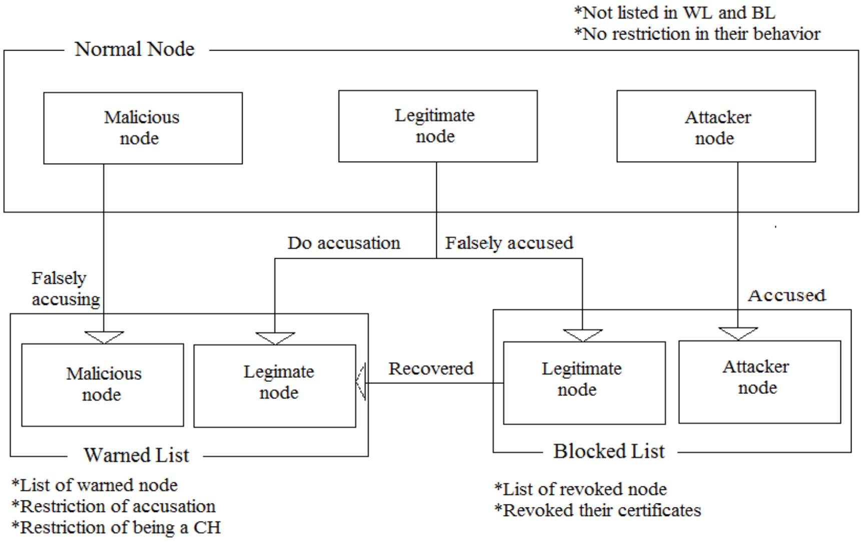

Fig.2. Classification of nodes in our scheme.

D. Certificate Revocation

Certificate revocation is a process of revoking a malicious attacker's certificate;when a node gives accusation on the neighbour node into the CA [15], [16], [17], [18]; CA first verifies the id of the accusing node, if it is a member of the organization means registers the complaint. The accused node will be moved to the warning list which is maintained in the CA database,later It will ask for the votes, suppose member node has given the complaint on the head(server) CA will get votes from the nodes which are connected to that head, after getting votes from the members CA will verifies the threshold value suppose the positive votes are more than the negative votes means threshold value doesn't reaches and the certificate is not revoked. Suppose positive votes are equal to negative vote's means threshold value reaches and certification revocation process is carried out. Suppose positive votes are less than the negative vote's means threshold value reaches and certification revocation process is carried out. ID revoked node will be moved to the blocked list from the warning list. That node will not be capable of doing any transaction in that organisation or open environment.

IV. IMPLEMENTATION

The various modules of our systems are:

- User System / Client System (Member)
- Implementing Server System(Head)
- Implementing Certificate Authority

Steps carried out

Our system has 3 modules, these modules plays an important roles, There are 5 major steps,

1. **Authentication**, it includes getting id from CA, after getting id from the CA the nodes in environment will be capable of doing further transaction.
2. **Connecting to the server node or head,** this step includes connecting the member node to the head, then it forms a cluster with the members
3. **Transactions in the cluster**, this step includes the members and head transaction within the cluster, head verifies the member node register details before serving.
4. **Registering complaint,** this step is carried out by any member in the cluster, when the nodes have un-successful transaction; it registers the complaint on malicious node to the CA, and that accused node will be maintained in WL.
5. **Requesting for votes,**this function is handled by CA, after registering the complaints, it asks for the votes from the members in the cluster to verify the threshold value.

V. MANAGEMENT OF LISTs BY CA

A. Warning List

Warning list plays an important role in our module, it WL is a table which is maintained in the centralized database of CA, CA maintains the WL, WL includes the accused nodes, means it includes the both accused and accusation node information, when member gives the complaint on the neighbour node, CA registers the complaint, and that node will be sent to the WL. It loses the function of accusation since the CA does not accept accusation packets from nodes enlisted in the WL.

B. Blocked List

Blocked list also plays a major role in the certificate revocation process, certification revocation is done based on the voting mechanism, after registering complaint in CA, CA will asks for the votes from every member, and it will wait for the votes, after considering the votes from the members, if the threshold value reaches CA will revoke the id or certification of the particular node, revoked node details will be maintained in the BL, nodes which are in BL are not capable of doing any transaction in the certified environment of cluster.

.

C. Policies for Determining the Threshold

In a MANET, mobile nodes are assumed to be uniformly distributed over a coverage area so as to satisfy the binomial distribution B (n ,q) , which denotes the probability of a number of nodes existing in a special area[18]. Here in, n denotes the total number of cells where a MANET is divided into; q is the probability that one cell is occupied by a single node. When n is very large and q is very small, the binomial distribution B (n, q) is approaching the Poisson distribution with parameter λ, which is equal to the number of nodes, nq. Consequently, the probability that there are exactly m normal nodes (m beinga nonnegative integer, (m= 0, 1, 2, . . .) within the transmission area S of an attacker node, is [1], equal to

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

Where ρdenotes the node density and λ means the proportion of normal nodes in the network.
As analysed above, the number of normal nodes is decreasing over time. When m=0, i.e., no normal nodes within an attacker's transmission range, the probability is [1],

$$\Pr(m = 0) = e^{-\theta\rho S}. \qquad \cdots\cdots \qquad (2)$$

From (2), the probability Pr (m = 0) greatly increases with the decrease of density ρ the efficiency of detecting malicious attackers is significantly reduced. In other words, the probability Pr (m = 0) must be reduced to guarantee a certain number of normal nodes in the network to revoke malicious attackers quickly.

We first design a simplified mechanism to determine the number of neighbouring nodes for any given node. Within time Tv, the given node crosses through an area and meets a number of neighbours N. Since mobile nodes are assumed uniformly distributed in the network, we may approximate N [1],

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

Where r denotes the transmission range of nodes, v is the velocity, and ρ is the density of nodes in the network. Based on the obtained number of neighbouring nodes N, we can confirm the value of threshold K. In the following, we detail three policies in determining the optimal value of threshold K.

- **Policy 1: Minimizing False Release Probability**

In the first policy, we decide K in terms of the probability Pf that no less than K out of N neighbours falsely accuse the given node. In other words, Pf denotes the probability that a legitimate node is framed by at least K colluding nodes so that the malicious node is released erroneously. probability is expressed as follows [18].

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

p denotes the probability of a node which participates in false accusation. Consequently, we expect to acquire the minimum value of Pf to reduce the probability of falsely releasing nodes from the WL. We can acquire the value K based on an acceptable range of Pf [1] .

- **Policy 2: Maximizing Correct Release Probability**

In the second policy, we determine the value of K on the basis of the probability Pc that no less than K out of N neighbouring nodes can correctly accuse the attacker so that a legitimate node will be successfully released from the WL.
We have the expression[1],

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

Where (1 – p) means the probability of a node whichparticipates in correct accusation. In order to achieve a highprobability of successfully releasing legitimate nodes fromthe WL, the value of Pc should be large.

- **Policy 3: Maximizing Accuracy**

We know that there is a trade-off between the false release probability Pf and correct release probability Pc in determining the value of threshold K. We would like 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. To this end, we propose to use γ(K) to determine the optimum threshold, where γ(K) equals the difference between Pc and Pf[1],

- **Numerical results for K (N=15) shown in the below table,**

	Policy 1($p_{f\leq}\alpha$)		Policy 2 ($p_c \geq \beta$)		
p	α = 0.1	α = 0,2	β = 0.9	β = 0.8	Policy 3
0.1	4	3	12	13	8
0.2	6	5	10	11	8
0.3	8	7	8	9	8

$$\gamma(K) = p_c(K) - p_f(K)$$
$$= \sum_{i=K}^{N} \binom{N}{i} \{(1-p)^i p^{N-i} - p^i (1-p)^{N-i}\}. \cdots \quad (6)$$

Note that, in the CRVC scheme, the total number of malicious nodes and attacker nodes is supposed to be less than the number of legitimate nodes in MANETs. Namely, (1 – p) isgreater than p [1].

VI. SIMULATION AND RESULTS

A. Comparison of Effectiveness of the Certificate Revocation

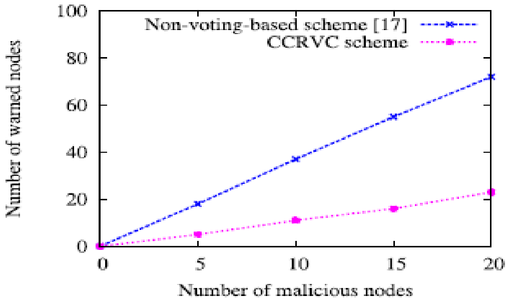

Fig 3: No. of warned nodes in WL

Fig. 3 clearly demonstrates that it can effectively reduce the number of nodes listed in the WL, i.e., the number of available nodes in the network has been improved by using the CCRVC scheme. We can see that the number of nodes listed in the WL is almost equal to the number of malicious nodes. Actually, almost all the malicious nodes are successfully kept in the WL. Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an attacker node’s launching the attack until its certificate is revoked [1].

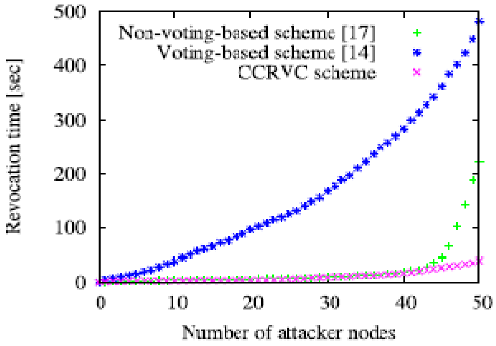

Fig 4: Revocation Time

Fig. 4 presents how the revocation time changes with different numbers of attacker nodes between the existing schemes (i.e., voting-based scheme [15] and non-voting based scheme [18]) and the CCRVC scheme. Suppose the number of attacker nodes is not larger than the number of legitimate nodes, the results always converge because there are enough legitimate nodes to revoke attackers' certificates within finite time in the simulation. Obviously, the voting-based scheme requires longer revocation time than that of CRVC scheme.

VII. SUMMARY

In summary, the CCRVC scheme exhibits more reliable and higher efficiency as compared to the existing ones, because it guarantees sufficient normal nodes to revoke the certificates of the attackers and takes a short revocation time, it achieves high accuracy in releasing legitimate nodes.To demonstrate the optimal threshold K, we design the experiment to measure Pf and Pc in comparison with those of numerical results, and observe the impact of different threshold values.In our system CA will verifies the threshold value suppose the positive votes are more than the negative votes means threshold value doesn't reaches and the certificate is not revoked. Suppose positive votes are equal to negative vote's means threshold value reaches and certification revocation process is carried out. Suppose positive votes are less than the negative vote's means threshold value reaches and certification revocation process is carried out. ID revoked node will be moved to the blocked list from the warning list. That node will not be capable of doing any transaction in that organisation or open environment [1].

VIII. CONCLUSION

In this paper the issue related to security of the MANETs is addressed usingCertification revocation by using CRVC mechanism. Cluster based certificate revocation method uses the voting mechanismto revoke the malicious node certificate and improves the accuracy as compared to the non-voting based mechanism. Used the proposed new incentive method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. The extensive results have demonstrated that, in comparison with the existing methods, our certificate revocation by using voting based scheme is more effectiveand efficient in revoking certificates of malicious attackernodes, reducing revocation time, and improving theaccuracy and reliability of certificate revocation.

REFERENCES

[1]Wei Liu, Nirwan Ansari, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks vol. 24, NO. 2,pp 243-245,February 2013.

[2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[3] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.

[] 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.
[5] L. Zhou and Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, “A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks,” IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.
[11] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil Attack in Sensor Network: Analysis &Defenses,” Proc. Third Int’l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.
[12] S. Micali, “Efficient Certificate Revocation,” Massachusetts Inst. Of Technology ,Cambridge, MA, 1996.
[13] C. Gentry, “Certificate-Based Encryption and the Certificate Revocation Problem,” EUROCRYPT: Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques, pp. 272- 293, 2003.
[14] H. Yang, J. Shu, X. Meng, and S. Lu, “SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks,” IEEEJ. Selected Areas in Comm.,vol. 24, no. 2, pp. 261-273, Feb. 2006.
[15] 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.
[16] 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.
[17] 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.
[18] 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.

BIOGRAPHY

Ranjana B Jadekar is a M Tech Student in Computer Science and Engineering Department, College of KLEDrMSSheshagiri College of Engg and Tech., VTU, She received Bachelor of Engineering Degree in 2013 BIET, VTU, Davanagere, Karnataka. Her research interests in Computer Networks (wireless Networks).

Prof.Shivanand M. Patilis a faculty in the Department of Computer Science &Engg., KLE Dr.M.S.Sheshgiri College of Engg. & Tech., Belagavi. He did his Bachelors in Computer Science &Engg. from MMEC, Belagavi and M.Tech in Computer Science &Engg. fromBasaveshwar Engineering College, Bagalkot. His research interests include Image Processing and Pattern Recognition. He has number of publications in to his credit in peer reviewed international journals and conferences.

DOI: 10.15680/ijircce.2015.0306125