ELEVATING SECURITY IN MOBILE ADHOC NETWORK USING CLUSTER-BASED CERTIFICATE REVOCATION WITH VINDICATION CAPABILITY

S.Herman Jeeva[1], D.Saravanan[2], RM.Chandrasekaran[3], Uma M[4]

[1]PG scholar, Department of Computer Science and Engineering, Pavendar Bharathidasan college of Engg. And Tech., Trichy, Tamilnadu, India

[2]Associate Professor, Department of Computer Science and Engineering, Pavendar Bharathidasan college of Engg. And Tech., Trichy, Tamilnadu, India

[3]Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu, India

[4]Assistant Professor Department of Computer Science and Engineering, Pavendar Bharathidasan college of Engg. And Tech., Trichy, Tamilnadu, India

Abstract

Mobile Ad hoc Networks (MANETs) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires and also it is an open network environment where nodes can join and leave the network freely. Hence, the dynamic natures of MANETs is not secure than the wired networks. To overcome this issue, the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed. In the meanwhile nodes forms a cluster consists of a Cluster Head with some Cluster Members (CMs) situated within the transmission range of their cluster Head. Each node should have to acquire valid certificates from the Certification Authority (CA) before it can join the network that is responsible for distribution and management of certificates to all nodes and also CA is responsible for updating two lists, Warning list and Black list. Both the lists are used to hold the accusing and accused nodes information, respectively. Experimental results show that the proposed CCRVC scheme is effective and efficient to provide efficient and secure communication.

Keywords— *Mobile ad hoc networks (MANETs), certificate revocation, and security.*

----------***----------

1. INTRODUCTION

Certificate Management is the widely used mechanism in MANET'S. Since in a public key infrastructure [12] it helps in delivering trust and to protect applications and network services. A complete security solution of certificate management has three components such as prevention, detection, and revocation. Many research efforts took place in some areas such as certificate verification, certificate distribution [14], attack detection [2], [6] and certificate revocation [1]. In order to secure network communications, Certification is essential.

Using the digital signature of the issuer, the public key is encrypted into an attribute. It is used to guarantee that a public key belongs to an individual and also in mobile Adhoc networks it helps to prevent tampering and forging. Many research efforts are made to weaken malicious attacks on the network. For enlisting and removing the certificates of nodes, certificate revocation plays a major task which has been detected to launch attacks on the neighborhood. This all will happen when attacks are identified. Certificate Revocation helps in removing misbehaving nodes from the network and gets blocked from all its activities suddenly. Certificate revocation's basic security problem is aimed at providing secure communications in MANETs.

To elevate the performance of MANET, Cluster-based Certificate Revocation with the scheme of Vindication Capability (CCRVC) is proposed. Topology is constructed as clusters. Some of the nodes joined to form a cluster consist of nodes within the transmission range and each cluster contains Cluster Head (CH) and Cluster Member (CM). To join the network each node should have a valid certificate. Certification Authority (CA) issues the valid certificates. Nodes are arranged as clusters that ensures preloading of certificate which is responsible for issuing and maintaining certificates of all nodes which can communicate with each other without any constraints. For holding the information of accusing and accused nodes, CA updates two lists such as Warned list and Black lists.

Through votes, a malicious attacker's certificate get revokes from valid neighboring nodes using Voting-based mechanism. Neighboring nodes issues certificates for new joining nodes. The certificate of an attacker is revoked, based on votes from its neighbor's nodes.

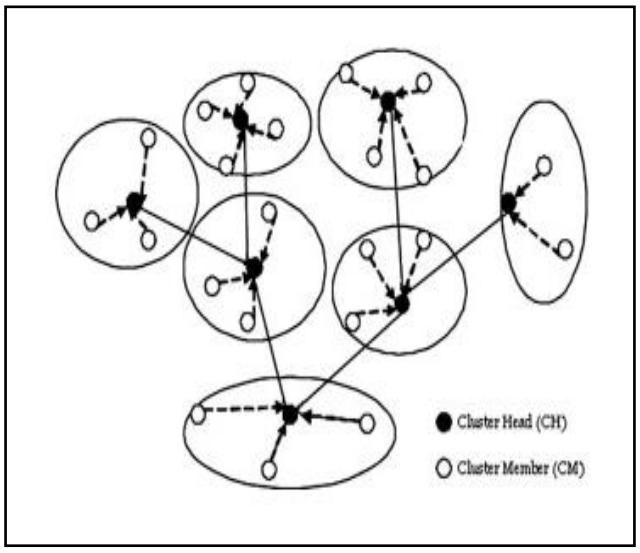

Fig-1: Cluster-Based Architecture

Without a valid certificate nodes cannot communicate with each other and that node gets isolated from network activities using certificate revocation. A main challenge is threshold determination. Nodes that are launching attacks cannot be revoked if it exceeds the network degree and can successively communicate with other nodes.

False accusations which are malicious are not addressed by URSA from nodes is a critical issue. The scheme which allows all nodes that are connected in the network to vote together is proposed by Arboit et al. [1]. The primary difference from URSA is that nodes vote with different weights but URSA has no Certification Authority present in the network instead of that each node plays a role of monitoring the behavior of its neighbors. Here node's weight is calculated in terms of dependability and truthfulness of the node that can be the number of accusations against other nodes and itself from others. The acquired weight is increased because of its reliability. The accuracy of certificate revocation is enhanced, when the weighted sum from voters against the node exceeds a predefined threshold so the certificate of an accused node is normally revoked. Because of voting between each node, communications overhead used to exchange voting information would be high and it rises the revocation time.

Non-voting-based mechanism states that a given node deemed as a malicious attacker will be decided by any node with a valid certificate. The suicidal strategy which was proposed Clulow et al. [4] proposed that only one accusation completes certificate revocation quickly. Certificates of both the accused node and accusing node have to be revoked simultaneously. Each time accusing node has to sacrifice itself to remove an attacker from the network. Due to its suicidal strategy, the application of this strategy is limited even though this approach reduces both the time required to remove a node and communications overhead. Simultaneously, the accuracy is reduced.

Park et al. [10] proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority manages the control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL) which is maintaining by certification authority. The main advantage of the voting-based mechanism is that the high accuracy in confirming the given accused node as a real malicious attacker or not.

The main disadvantages of non-voting-based method are slow decision process to satisfy the condition of certificate revocation and also it sustains heavy communications overhead to exchange the accusation information for each other.

Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed [10], [8]. In this, clustering plays a major role, where the cluster head is to detecting the falsely accused nodes within its cluster and regaining their certificates to solve the issue of false accusation.

CCRVC achieves immediate revocation and lowering overhead as compared to the voting-based scheme and when compared to the non-voting-based scheme improves the reliability and accuracy.

2. THE PROBLEM

It is difficult to identify the attackers through wireless Ad hoc network since it is a self configured network. Various revocation techniques are used for enhancing network security.

Two types of mechanisms used for certificate revocation are Voting based mechanism and non-voting mechanism.

2.1 Voting based Mechanism

In URSA, each node provides a vote to its neighbor node within the cluster. Here each node performs one-hop monitoring with its neighbor nodes and monitoring information is exchanged with its neighboring nodes. A predefined number is maintained as a threshold for getting negative votes by each node. When the threshold value by exceeds the number of negative votes for a node, the certificate of accused node gets revoked. Then, the node can get isolated from the network activities. However, the accused node would be communicating with other nodes in network when threshold value is assigned larger. The risk factor is that false accusation from malicious node is not addressed.

Arboit et al. [15] proposed that voting varies with the weights. The weight of a node is calculated based on the reliability and trustworthiness which can be derived from its past behaviors.

When the weighted sum from voters against the node exceeds a predefined threshold, the certificate can be

revoked. The certificate revocation accuracy can be enhanced and communication overhead would be high when all nodes are participated in each voting.

2.2 Non-voting based Mechanism

Due to the suicidal strategy, Certificate revocation can be completed by only one accusation that is simultaneously both the accused node and accusing node certificates will be revoked.

In the non-voting based mechanism, the time required removing an accused node and communications overhead of the certificate revocation procedure can be reduced but the accuracy will be low.

3. CONTRIBUTION

Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is proposed. In this, the falsely accused nodes within its cluster are detected using the cluster head and using certification authority recovering their certificates to solve the issue of false accusation. CCRVC scheme compared to the voting-based scheme to achieve prompt revocation and lowering overhead and also CCRVC scheme compared to the non-voting-based scheme to improve the reliability and accuracy. Cluster-based revocation scheme revokes attacker nodes keep receiving only one accusation node from a neighboring node.

The Certification authority scheme maintains two types of lists called warning list and blacklist to guard against malicious nodes from further framing other legitimate nodes. Moreover, false accusation can be addressed by the cluster head which is in the clustering architecture to revive the falsely revoked nodes. In this, the main focus is that once a malicious attacker has been identified, the certificate revocation procedure is done, rather than the attack detection mechanism itself. Within one-hop away, each node has the ability to detect its neighboring attack nodes.

Clusters are formed with cooperation of nodes and within the transmission range each cluster consists of a Cluster Head with some Cluster Members (CMs). Before joining the network each nodes have to acquire valid certificates from the Certification Authority, which is responsible for issuing and maintaining certificates of all nodes, so that nodes can easily communicate with each other.

Based on their reliability, nodes are termed as normal node, warned node, and revoked node

Normal Node: Normal Node is a node which joins the network and does not launch attacks. This type of nodes has high reliability and also has the capacity to accuse other nodes and to proclaim itself as a CH or a CM.

Warned Node: Warned nodes are the nodes which are in the warning list with low reliability They are considered doubtful because the warning list contains a mixture of legitimate nodes and a few malicious nodes.

Revoked Node: Revoked nodes are the accused nodes that are listed in the blacklist with little reliability. They are considered as malicious attackers destitute of their certificates and removed from the network.

4. SYSTEM DESIGN

The system design involves the different steps involved in the proposed CCRVC scheme. The entire process is summarized in the Fig.2 which gives a clear cut idea about the proposed method.

4.1 Process

Each of the nodes sends an accusation packet to the certificate authority (CA) against attacker node when the neighboring nodes detect attacks from any one node. Based on the first received packet, the CA holds neighboring node in the Warning List (WL) and attacker node in the Black List (BL). The CA disseminates the revocation message to all nodes in the network after verifying the validity of neighboring node. To revoke attacker's certificate each node update their local WL and BL only after receiving the revocation message. At the same time, CH determine that one of the node was framed by updates their WL and BL. Then CA receives recovery packet from some of the neighbor nodes to revive the falsely accused node. The CA removes the falsely accused node from the BL and holds both the falsely accused node and normal node in the WL only after receiving the first recovery packet and then disseminates the information to all the nodes. Finally the nodes update their WL and BL to recover the falsely accused node.

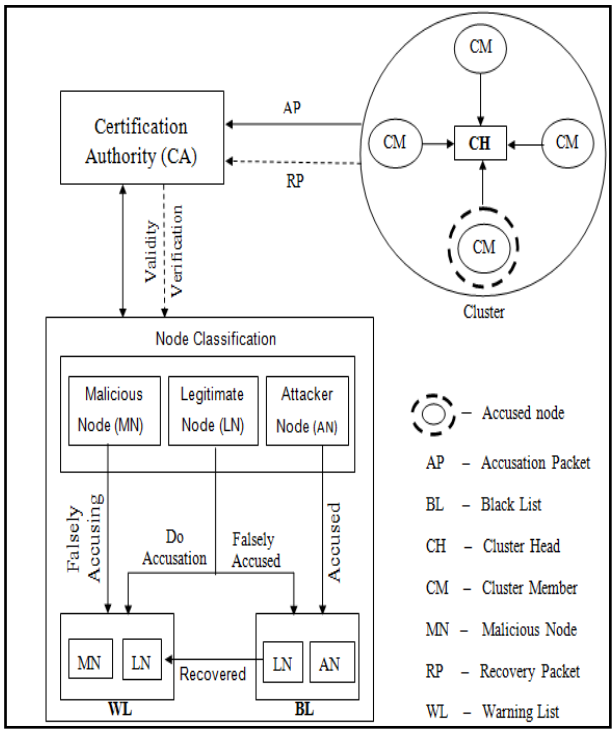

Fig-2: System Architecture.

5. SYSTEM IMPLEMENTATION

5.1 Simulation of AODV Protocol

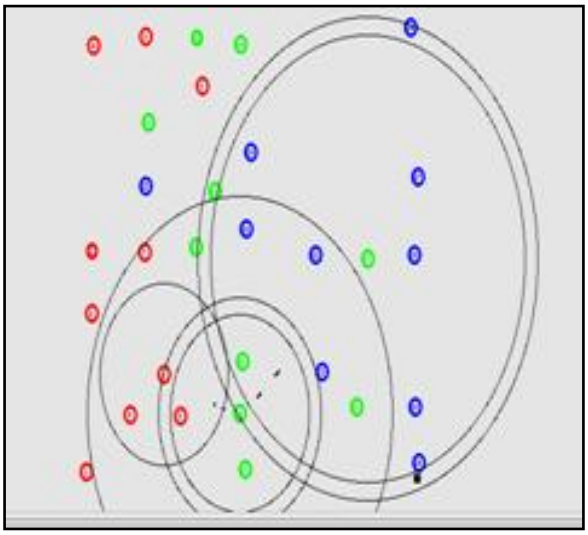

Fig-3: Creation of nodes and Transmission of packets using AODV protocol

Creation of nodes and transmission of packets between those nodes is made by Normal Network with AODV protocol. The calculation of parameters such as end to end delay (EED), throughput (Tp), packet delivery ratio (PDR), energy (E) spent is done.

5.2 Simulation of DoS Attack

Implementation of DoS Attack during packet transmission makes the performance degradation. The parameters such as end to end delay (EED), throughput (Tp), packet delivery ratio (PDR), energy (E) spent are calculated.

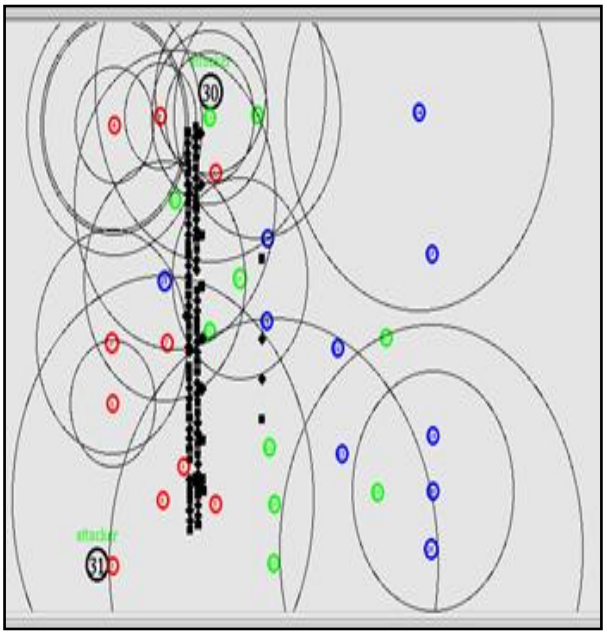

Fig-4: Dropping of packets

5.3 Simulation of CCRVC Scheme

Using proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme, transmission of packets between the nodes is done to avoid attack and to increase network performance. The Calculation of parameters such as end to end delay (EED) , throughput (Tp), packet delivery ratio (PDR), energy (E) spent is made.

6. RESULT ANALYSIS

Comparison between AODV, ATTACK and CCRVC with various parameters is done and output is shown using graphs.

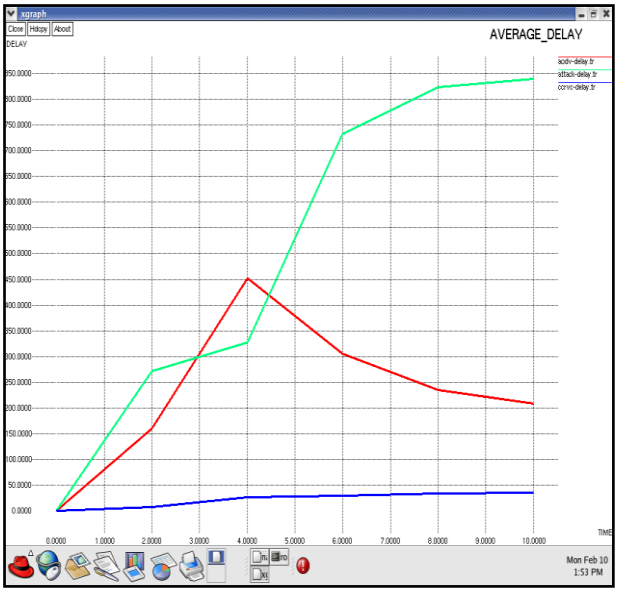

Fig-5: Graph Representing Variations of Delay

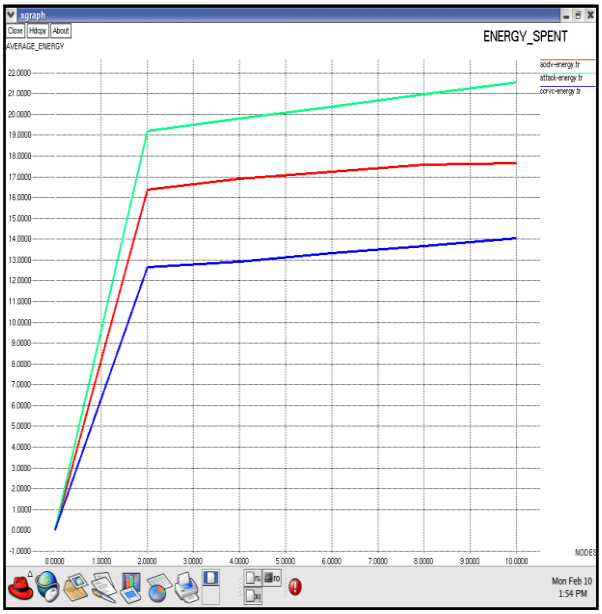

Fig. 6 Graph Representing Variations of Energy

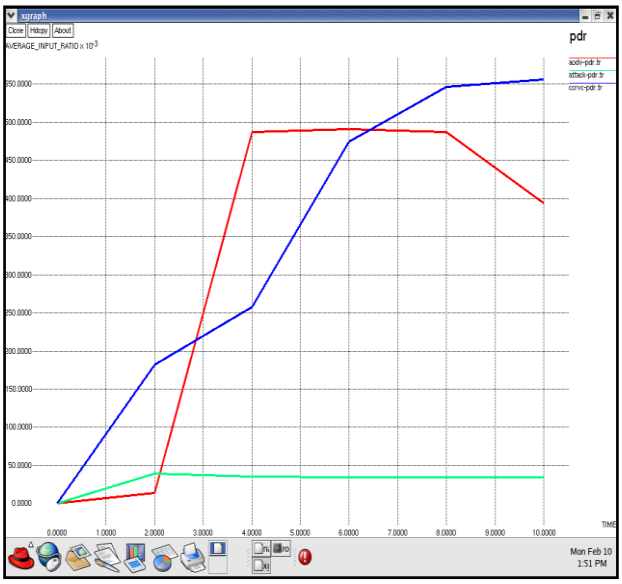

Fig-7: Graph Representing Variations of Packet Delivery Ratio

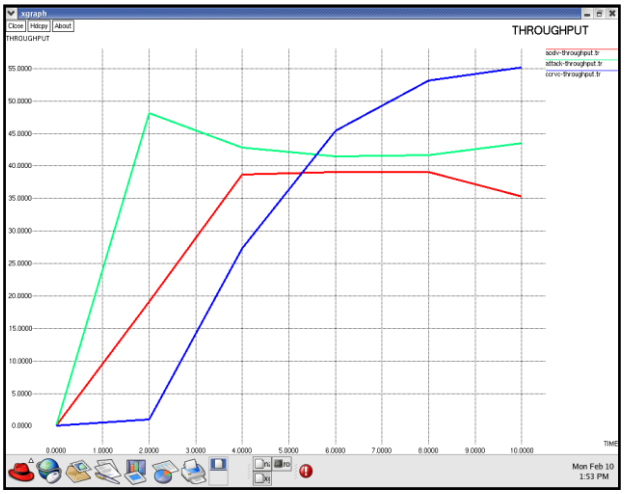

Fig-8: Graph Representing Variations of Throughput

All the above graphs show the variation of delay (D), energy (E), packet delivery ratio (PDR) and throughput (Tp) with respect to time.

7. CONCLUSIONS

A major issue is to ensure a secure communications in MANET, certificate revocation of attacker nodes is addressed. Cluster-based certificate revocation with vindication capability scheme has advantages of both voting-based and non-voting based mechanisms in which malicious certificate is revoked and false accusation problems are solved. This CCRVC scheme reduces the revocation time as compared to the voting-based mechanism.

In the cluster based model falsely accused nodes are restored by the CH, which improves the accuracy when compared to the non-voting based Mechanism. The legitimate nodes are released and restored in a new stimulant method which also enhances the number of available normal nodes in the network for protecting the efficiency of quick revocation. Thus the scheme of CCRVC is more potential and coherent in certificate revocation of malicious attacker nodes, reducing revocation time, and improving the validity and reliability of certificate revocation.

REFERENCES

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

[2]. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato. (2007) "A survey of routing attacks in mobile Adhoc networks"

[3]. Camp T., Boleng J. and Davies. (2002) "The survey of mobility models for Adhoc network research," Wireless Communication and Mobile Computing, vol.2, no.5, pp. 483-502.

[4]. Clulow J. and Moore T. (2006) "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.

[5]. Hegland A.M., Winjum E.,Rong C. and Spilling P. (2006) "A survey of key management in Adhoc Networks," IEEE Communications Surveys and Tutorials, vol 8, no. 3, pp. 48-66.

[6]. Herman Jeeva S. and Saravanan D.(2014)"Integral Component CCRVC Scheme for Enhancing Security in MANET" in IJIRSET, Vol.2, Special Issue 1, pp. 425 - 429.

[7]. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei Kato.(2009) "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Adhoc Networks".

[8]. Jie Lian, Kshirasagar Naik, Gordon B. and Agnew (2004) "A Framework for Evaluating the Performance of Cluster Algorithm for hierarchical Networks"

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

[10]. Luo J., Kong P., Zerfos S., Lu and Zhang L. (2004) "URSA: Ubiquitous and Robust Access Control for Mobile Adhoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063.

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

[12].Sakarindr P. and Ansari N. (2007) "Security Services in group communications over wireless infrastructure, mobile Adhoc, and wireless sensor networks," IEEE Wireless Communications14(5), pp. 8-20.

[13]. Saravanan Dhavamani. and Chandarasekaran Ramasamy(2014)"Trustworthy Enabled Reliable Communication Architecture in Mobile Ad Hoc Network" in Journal of Computer Science, pp. 1120 - 1129.

[14]. Yang H., Luo H., Ye F., Lu S. and Zhang L. (2004) "Security in Mobile Adhoc Networks: challenges and

solutions," IEEE Wireless Communications,11(1), pp. 38-47.
[15]. Yang H., Shu J., Meng X. and Lu S. (2006) "SCAN: Self-Organized Network Layer Security in Mobile Adhoc Networks," IEEE J. Selected Areas in Comm., vol.24, no.2, pp. 261-273

BIOGRAPHIES

Mr. Herman Jeeva S received the B.E degree in Computer Science and Engineering from St.Joseph's College of Engineering and Technology, Thanjavur in 2012. He is currently doing the M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Mathur, Tiruchirappalli.

Mr. Saravanan D received the B.E degree in Electrical and Electronics Engineering from Maharaja Engineering College, Tiruppur in 2000 and received the M.E degree in Computer Science and Engineering from Annamalai University, Chidambaram in 2005. He is currently doing the Ph.d in the area of MANET and also working as an Associate Professor in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli with 11 years of teaching experience and his area of interest include MANET.

Dr.RM.Chandraekaran is working as a Professor at the Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India. From 1999 to 2001 he worked as a software consultant in Etiam, Inc, California, USA. He has conducted Workshops and Conferences in the Areas of Multimedia, Business Intelligence and Analysis of algorithms, Data Mining. He has presented and published more than 32 papers in conferences and journals and is the author of the book Numerical Methods with C++ Program (PHI, 2005). His Research interests include Data Mining, Algorithms and Mobile computing. He is Life member of the Computer Society of India, Indian Society for Technical Education, Institute of Engineers, Indian Science Congress Association.

Mrs.Uma M received the B.Tech degree in Computer Science and Engineering from VIT University, Vellore in 2003 and received the M.E degree in Computer Science and Engineering from Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli in 2006. She is currently doing her Ph.d in the area of MANET and also working as an Assistant Professor in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli with 8 years of teaching experience and her area of interest include MANET.