MANET Based Locality Trust Extended Authentication Using LAM

K.Krishnan, Dr.T.Govindaraj and P.Kanmani

Abstract - Security and protection of private user information are a prerequisite for the deployment of the mobile network technologies. Nevertheless, the establishment of secure communication architecture within mobile ad hoc networks addresses special challenges, due to the characteristic and specific cities of such environment (high dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighborhood, broad-cast/geo-cast communication nature). A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. In this paper, we address someinteresting issues arising in such MANETs by designing an anonymous routing framework (ALERT) extended to key server management and digital signature algorithm. It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other relay nodes it wants to communicate with. ALERT takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and intractability (tracking-resistance). It also offers resistance to certain insider attacks.resistance). It also offers resistance to certain insider attacks.

Index Terms—Mobile ad hoc networks, anonymity, routing protocol, geographical routing

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. Identity and location anonymity of sources and destinations means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations.

[1]K.Krishnan, [2]Dr.T.Govindaraj and [3]P.Kanmani, [1]Ph.D, Scholar, Asst. Prof , Department of IT , Jayam College of Engg. & Tech., Dharmapuri, gurukrishnan.priyan@gamil.com, [2]Professor and Head, Department of EEE, Muthayammal Engineering College, Rasipuram, [3]P.G Scholar, M.Tech,, Department of IT, Jayam College of Engineering and Technology, Dharmapuri,India

For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes in route. Also, in order to dissociate the relationship between source and destination, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories hop by hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections. Limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. In order to provide high anonymity protection with low cost, we propose an Anonymous Location-based and Efficient Routing protocol (ALERT).

ALERT dynamically partitions a net work field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source.

ALERT is also resilient to intersection attacks and timing attacks. We theoretically analyzed ALERT in terms of anonymity and efficiency. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols[1]-[30].

II. ALERT: AN ANONYMOUS-LOCATIONBASED EFFICIENT ROUTING ROTOCOL

A. Networks and Attack Models and Assumptions

ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model.

B. The ALERT Routing Algorithm

In existing system, the undetectable route path and secure data transmission is achieved through ALERT an anonymous location based efficient routing protocol.ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message transmission.

In the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until source and destination are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF) which takes a path way to destination.

III. ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

This section discusses the performance of ALERT in providing anonymity protection and its performance and strategies to deal with some attacks.

A. Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing which always takes the shortest path, ALERT makes the route between an S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

IV. RELATED WORKS

The proposed work is carried on the extension of ALERT routing. A group signature concept of key server management is introduced to provide a secure and authenticated data transmission in the mobile network in addition to ALERT algorithm. Source encrypt the data using the public key of destination, then destination request a key server to provide a private key for decrypting the encrypted data.

The key server provides a private key only after verification from source node. Group signatures can be viewed as traditional public key signatures with additional privacy features. In a group signature scheme, any member of a potentially large and dynamic group can sign a message thereby producing a group signature. A group signature can be verified by anyone who has a copy of a constant length group public key. A valid group signature implies that the signer is a bonafide group member. However, given two valid group signatures it is computationally infeasible to decide whether they are generated by the same (or different) group members. However, if a dispute arises over a group signature, a special entity called a Group Manager can force open a group signature and identify the actual signer.

A mobile node can periodically sign its current location (link state) information without any fear of being tracked, since multiple group signatures are not linkable. At the same time, anyone can verify a group signature and thus be assured that the signer is a legitimate MANET node through Location Announcement Message (LAM).

V. SYSTEM ORGANIZATION

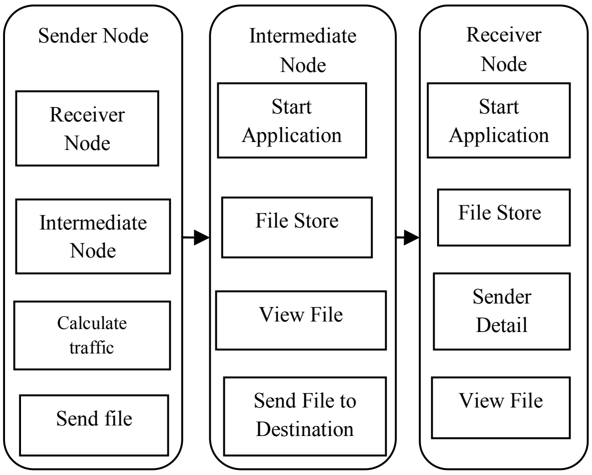

Fig. 1: System Organization

The nodes involved are admin and clients which stands as UI for the system. The deployment is performed as per the requirements of Hardware and software specified in the requirements phase. In this System diagram ,we explain about how over all process will complete based on user receiver node, select intermediate node calculate traffic between low nodes and send file to intermediate node The intermediate will receive the file and send to correct destination. The receiver will receive file, view file and sender detail.

VI. SYSTEM IMPLEMENTATION

The following process are done in my proposed system

1. NODE CREATIING
2. ZONE PARTITION
3. DATA ROUTING
4. ALERT WORKING PROCESS
5. KEY SERVER MANAGEMENT

A. Node Creating

This module is developed to node creation and more than 50 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

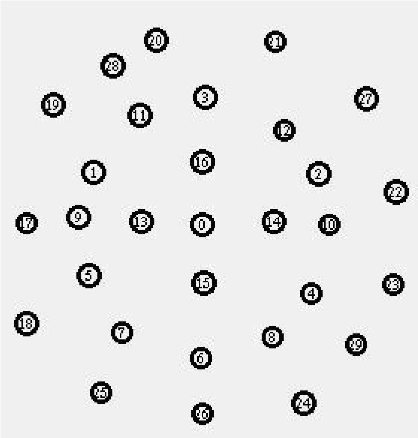

Fig. 2: Node Creating

B. Zone Partition

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner.

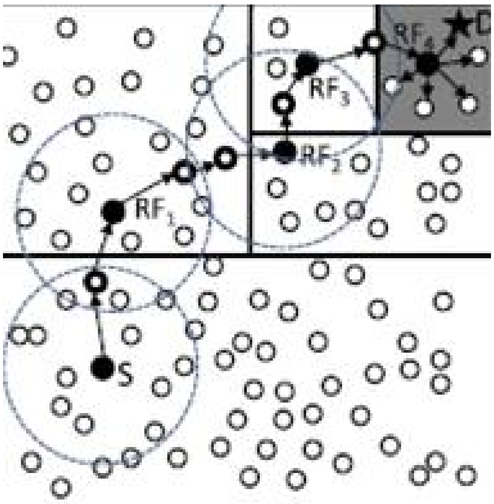

Fig.3: Zone Partition

C. Data Routing

After the hierarchical zone partition process, the source and destination claimed to be in different zones. The source node sends the data to destination through the intermediate relay nodes. The user data gram protocol is used to transfer the data routing from one relay node to next relay node.

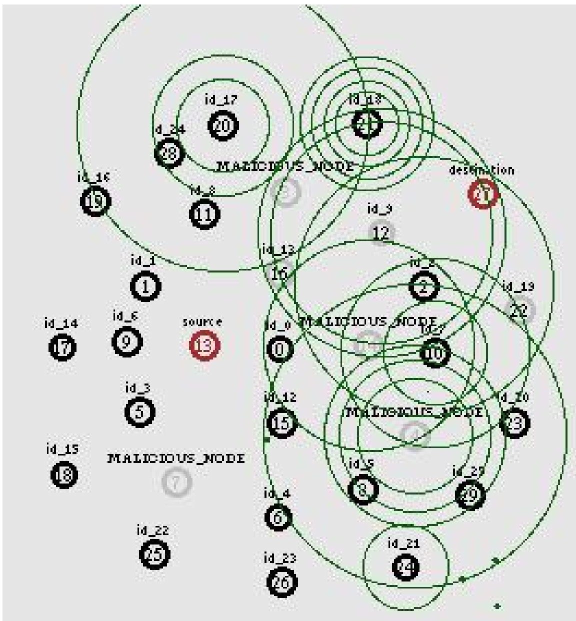

Fig. 4: Data Routing

D. Alert Working Process

The main objective of the ALERT algorithm is to provide a security to the MANET by means of trust extended authentication mechanism. The ALERT setup a temporary destination TD and informs to all mobile nodes in the network, so that the attacker concentrates only on TD to hack the data. By means of diverting the attacker's concentration the data from source is delivered to original destination in secure manner.

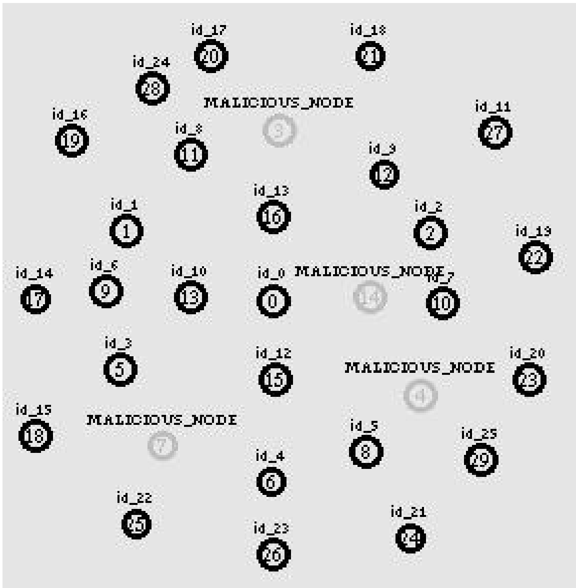

Fig.5: Alert Working Process

E. Key Server Management

The extended technique or proposed technique of ALERT is key server management. ALERT mechanism doesn't suitable for heavier traffic condition since ALERT is a light weight trusting mechanism. So in order to overcome this issue key server management technique is proposed.

Through KSM (key server management) technique provides a more authentication and secure transmission than ALERT mechanism through data encryption and decryption technique.

F. Algorithm

Let L -1 = n* 160 + b, where both b and n are integers and $0 \le b < 160$.

Step 1: Choose an arbitrary sequence of at least 160 bits and call it SEED. Let g be the length of SEED in bits.

Step 2: Compute U = SHA-1[SEED] XOR SHA-1[(SEED+1)mod2g].

Step 3: Form q from U by setting the most ignificant bit (the 2^{159} bit) and the least significant bit to 1. In terms of

Boolean operations, q = U OR 2^{159} OR 1. Note that $2^{159} < q < 2^{160.}$

Step 4: Use a robust primality testing algorithm to test whether q is prime 1.

Step 5: If q is not prime, go to step 1.

Step 6: Let counter = 0 and offset = 2.

Step 7: For k = 0... n let Vk = SHA-1[(SEED + offset + k) mod 2^g]. 1 A robust primality test is one where the probability of a non-prime number passing the test is at most 2^{-80}

Step 8: Let W be the integer $W = V_0 + V_1 * 2^{160} + ... + V_{n-1} * 2^{(n-1)* 160} + (V_n \bmod 2^b) * 2^{n* 160}$ and let $X = W + 2^{L-1}$. Note that $0 \le W < 2^{L-1}$ and hence $2^{L-1} \le X < 2^L$.

Step 9: Let c = X mod 2q and set p = X -(c -1). Note that p is congruent to 1 mod2q.

Step 10: If $p < 2^{L-1}$, then go to step 13.

Step 11: Perform a robust primality test on p.

Step 12: If p passes the test performed in step 11, go to step 15.

Step 13: Let counter = counter + 1 and offset = offset +n+1.

Step 14: If counter $\ge 2^{12}$ = 4096 go to step 1,otherwise (i. e. if counter < 4096) go to step 7.

Step 15: Save the value of SEED and the value of counter for use in certifying the proper.

VII. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity.

ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks.

REFERENCES

1) Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.
2) S. Vishnu and Dr.T.Govindaraj, "Simulation Modeling of Sensor less Speed Control of BLDC Motor Using Artificial Neural Network," International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569), vol. 10, pp. 7-15, 2014.
3) PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.
4) K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2007.
5) C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.
6) B. Gokulakrishnan and Dr.T.Govindaraj, "Simulation of PWM based AC/DC Converter control to improve Power Quality", International Journal of Advanced and Innovative Research. ISSN (2278-7844), 2012.
7) Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp.Applications on Internet (SAINT), 2006.
8) Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
9) N.M.Dhivya and Dr.T.Govindaraj, "Simulation Modeling on Artificial Neural Network Based Voltage Source Inverter Fed PMSM", INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING, Volume 2, Issue 1, Pages 785-791, 2014.

10) Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

11) K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.

12) Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.

13) Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

14) Dr.T.Govindaraj, and T.Keerthana," DFC And DTC Of Special Electric Drive Using PI And FLC, " International Journal Of Advanced And Innovative Research.ISSN: 2278-7844, Dec-2012 ,pp 475-481.

15) R.Narmatha and T.Govindaraj, "Inverter Dead-Time Elimination for Reducing Harmonic Distortion and Improving Power Quality", International journal of Asian Scientific Research, vol.3, April 2013

16) Dr.T.Govindaraj, and A.Kanimozhi," Instantaneous Torque control of Small Inductance Brushless DC Drive,"International Journal Of Advanced and Innovative Research.ISSN: 2278-7844, Dec-2012 ,pp 468- 474.

17) Govindaraj Thangavel,"Finite Element Analysis of the Direct Drive PMLOM" In book: Finite Element Analysis - New Trends and Developments Chapter:6,InTech - Publisher, Oct 2012(ISBN 978-953-51-0769-9)

18) Dr.T.Govindaraj, and M. Gunasegaran," PV Micro inverter System based Electric Drive , " International Journal Of Advanced and Innovative Research.ISSN: 2278-7844, Dec-2012, pp 458-46.

19) Govindaraj Thangavel, Debashis Chatterjee, and Ashoke K. Ganguli," Modelling and Simulation of Microcontroller based Permanent Magnet Linear Oscillating Motor,"International Journal of Modelling and Simulation of Systems, Vol.1, Iss.2, pp. 112-117, 2010

20) T.Govindaraj, Debashis Chatterjee, and Ashoke K. Ganguli, "A Permanent Magnet Linear Oscillating Motor for Short Strokes," Proc. International Conference on Electrical Energy Systems & Power Electronics in Emerging Economies ,ICEESPEEE-2009, SRM University, India, April 16-18, 2009, pp. 351- 355

21) Dr.T.Govindaraj,and N.Lavanya,"Fuzzy Controller for Solar Reconfigurable Converter Fed BLDC Drive" Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering Vol. 2, Issue 2, February 2014

22) Dr.T.Govindaraj, Jithin P," Simulation Modeling on High Performance FLC based Induction Drive" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 6, Dec-Jan, 2014 ISSN: 2320 – 8791

23) G. Thangavel and A. K. Ganguli,"Dynamic Modeling of Directive Drive Axial Flux PM Linear Oscillatory Machine Prototype Using FE Magnetic Analysis",Iranian Journal of Electrical and Computer Engineering, Vol. 10, No. 2, Summer-Fall 2011

24) Govindaraj Thangavel, Debashis Chatterjee, and Ashoke K. Ganguli," Design, Development and Finite Element Magnetic Analysis of an Axial Flux PMLOM," International Journal of Engineering and Technology, Vol.2 (2), 169-175 , 2010

25) Govindaraj Thangavel, Ashoke K. Ganguli and Debashis Chatterjee,"Dynamic modeling of direct drive axial flux PMLOM using FEM analysis" International journal of Elixir Electrical Engineering Vol.45 pp 8018- 8022, April 2012 (ISSN 2229-712X)

26) Govindaraj Thangavel, Debashis Chatterjee, and Ashoke K. Ganguli,"Design, Development and Control of an Axial Flux Permanent Magnet Linear Oscillating Motor using FE Magnetic Analysis Simulation Models," Int. Journal of Electrical and Electronics Engineering, Oradea, Romania, October 2010(ISSN 1844-6035

27) Govindaraj Thangavel, Debashis Chatterjee, and Ashoke K. Ganguli,"FEA based Axial Flux Permanent Magnet Linear Oscillating Motor," International Journal THE ANNALS OF "DUNAREA DE JOS" UNIVERSITY OF GALATI FASCICLEIIIELECTROTECHNICS,ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS , July 2010 (ISSN 1221-454X)

28) Govindaraj Thangavel," Design, Development, Analysis and Control of an Axial Flux Permanent Magnet Linear Oscillating Motor suitable for short strokes using Finite Element Method," International Journal of Electronic Engineering Research Volume 2 Number 3 pp. 419–428, 2010

29) Govindaraj Thangavel ,"Low Frequency Axial Flux Linear Oscillating Electric Drive Suitable for Short Strokes" International Journal ISRN Electronics Volume 2014, Article ID 765161,2014

30) Govindaraj Thangavel, Debashis Chatterjee, and Ashoke K. Ganguli,"FEA Simulation Models based Development and Control of An Axial Flux PMLOM,"International Journal of Modelling and Simulation of Systems, Vol.1, Iss.1, pp.74-80, 2010 (ISSN 1737-9377)

Krishnan.K received his B.Sc., Computer Science, M.C.A., and M.Phil, from Periyar University, Salem,India.He received M.E Degree in Computer Science and Engineering from Jayam College of Engineering and Technology, His pursuing Ph.D, Information and Communication Engineering in Anna University, Chennai. Life Member of Indian Society for Technical Education. His area of Interest are Mobile Sensor Networks, Web Mining, and Cloud Computing.

Dr.Govindaraj Thangavel born in Tiruppur, India in 1964. He receivedthe B.E. degree from CoimbatoreInstitute of Technology, M.E. degreefrom PSG College of Technology andPh.D. from Jadavpur University, Kolkatta, India in 1987, 1993 and 2010respectively. His Biography is includedin Who's Who in Science andEngineering 2011-2012 (11th Edition). Scientific Award ofExcellence 2011 from American Biographical Institute (ABI).Outstanding Scientist of the 21st century by International Biographical centre of Cambridge, England 2011.Since July 2009 he has been Professor and Head of theDepartment of Electrical and Electronics Engineering, Muthayammal Engineering College affiliated to AnnaUniversity, Chennai, India. His Current research interestsincludes Permanent magnet machines, Axial flux Linearoscillating Motor, Advanced Embedded power electronics controllers, finite element analysis of special electricalmachines,Power system Engineering and Intelligentcontrollers.He is a Fellow of Institution of Engineers India(FIE)and Chartered Engineer (India).Senior Member of InternationalAssociation of Computer Science and Information Technology(IACSIT). Member of International Association of Engineers (IAENG), Life Member of Indian Society forTechnical Education (MISTE). Ph.D. Recognized ResearchSupervisor for Anna University and Satyabama University, Chennai. Editorial Board Member for journals like InternationalJournal of Computer and Electrical Engineering,InternationalJournal of Engineering and Technology,International Journal ofEngineering and Advanced Technology (IJEAT).InternationalJournal Peer Reviewer for Taylor &Francis InternationalJournal "Electrical Power Components & System", UnitedKingdom,Journal of Electrical and Electronics EngineeringResearch,Journal of Engineering and Technology Research (JETR), International Journal of the Physical Sciences, Association for the Advancement of Modeling and Simulation Techniques in Enterprises, International Journal of Engineering & Computer Science (IJECS), Scientific Research and Essays, Journal of Engineering and Computer Innovation, E3 Journal of Energy Oil and Gas Research, World Academy of Science, Engineering and Technology, Journal of Electrical and Control Engineering (JECE), Applied Computational Electromagnetic Society etc. He has published 176 research papers in International /National Conferences and Journals. Organized 40 National / International Conferences/ Seminars/ Workshops. Received Best paper awardfor ICEESPEEE 09 conference paper. Coordinator for AICTE Sponsored SDP on special Drives, 2011. Coordinator for AICTE Sponsored National Seminar on Computational IntelligenceTechniques in Green Energy, 2011. Chief Coordinator and Investigator for AICTE sponsored MODROBS – Modernizationof Electrical Machines Laboratory. Coordinator for AICTESponsored International Seminar on "Power QualityIssues in Renewable Energy Sources and HybridGenerating System", July 2013.