Route Discerning and Hop Node Verification to Ensure in Authenticated Data Transmission with High Security Risk

[1]K.Krishnan,d[2]Dr.T.Govindaraj and [3]M.Kalaiyarasi

Abstract - In mobile ad hoc network, Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. These routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. However, current position aided routing protocols were not designed for use in high-risk environments, as position information is broadcasted in the clear allowing anyone within range, including the enemy, to receive. To analyze these methods for route discovery and verification of neighbors' position information in MANET routing protocols, and ways to use the position information to enhance performance and security of MANET routing protocols. We introduce "Neighbor position verification" (NPV), a routing protocol designed to protect the network from adversary nodes by verifying the position of neighbor nodes to improve security, efficiency, and performance in MANET routing.

Index Terms - Mobile ad hoc networks, Neighbor position verification.

I. INTRODUCTION

LOCATION awareness has become an asset in mobile systems, where a wide range of protocols and applications require knowledge of the position of the participating nodes. Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordinationamong autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information.

The correctness of node locations is therefore an all important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In these cases, we need solutions that let nodes,

1) Correctly establish their location in spite of attacks feeding false location information,
2) Verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

[1]K.Krishnan, [2]Dr.T.Govindaraj and [3]M.Kalaiyarasi, [1]Ph.D.Research Scholar, Asst. Professor, 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,

NPV deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. We therefore propose an NPV protocol that has the following features:

- It is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes.
- It leverages cooperation but allows a node to perform all verification procedures autonomously. This approach has no need for lengthy interactions, e.g., to reach a consensus among multiple nodes, making our scheme suitable for both low- and high mobilityenvironments.
- It is reactive, meaning that it can be executed by anynode, at any point in time,without prior knowledgeof the neighborhood
- It is robust against independent and colludingadversaries
- It is lightweight, as it generates low overhead traffic

We deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location based services[1]-[31].

II. SYSTEM AND ADVERSARY MODEL

A. Securely determining own location:

In mobile environments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and noncryptographic defense mechanisms. Alternatively, terrestrial special purpose infrastructure could be used along with techniques to deal with no honest beacons.

B. Secure neighbor discovery (SND):

SND deals with the identification of nodes with which a communication link can be established or that are within a given distance.

SND is only a step toward the solution we are after: simply put, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some SND range), but it could still cheat about its position within the same range. In other words, SND is a subset of the NPV problem, since it lets a node assess whether

another node is an actual neighbor but it does not verify the location it claims to be at.SND is most often employed to counter wormhole attacks.

C. Neighbor position verification (NPV):

NPV was used in ad hoc and sensor networks; however, existing NPV schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbornodes that can be aprioristically trusted are quite unrealistic. Thus, we devise a protocol that is autonomous and does not require trustworthy neighbors.

NPV protocol is first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions. This scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multiround computations involving several nodes that seek consensus on common neighbor verification. Conversely, by exploiting cooperation among nodes, NPV protocol is:

1) Reactive, as it can be executed at any instant by any node, returning a result in a short time span,
2) Robust to fake, yet realistic, mobility patterns announced by adversarial nodes over time.

A fully distributed cooperative scheme for NPV, which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors. For clarity, here we summarize the principles of route discovery and position verification process.

In any node to validate the position of all of its neighbors through a fast, one-time message exchange, which makes it suitable to both static and mobile environments. Additionally, we show that our NPV scheme is robust against several different colluding attacks.

III. SYSTEM ORGANIZATIONS

In this system, this allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier.

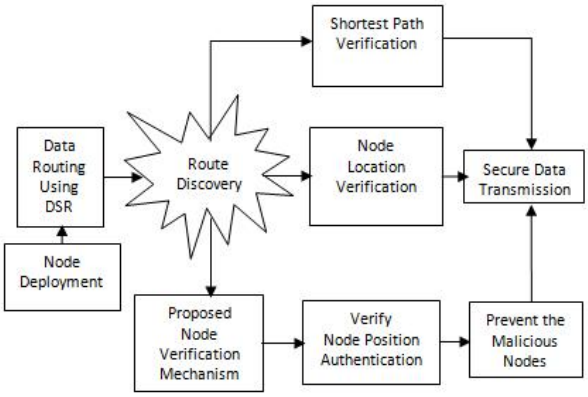


Fig.1: System Architecture

This system includes 3 phases in Fig.1, namely: Here phase 1 includes node deployment and data routing using DSR, phase 2 includes shortest path verification, phase 3 includes verify the node and position and also to prevent the malicious node.

The following processes are done in a system organization:

- **Phase 1:** To work a mobile node, the nodes are post of different places and to find how many nodes are interconnected in a source to destination.
- **Phase 2:** To discover the routing path in a shortest way
- **Phase 3:** To verify the node, using NV mechanism and NPV mechanism for sending the information in an authenticated way and also to prevent the malicious node for secure data transmission.

IV. COOPERATIVE DSCR: AN OVERVIEW

Our proposed system the NPV protocol is extended to dynamic source configuration routing protocol, which results in the mobile node verification instead of node position verification.Md5 algorithm was generate an private key,is provide an security of all the nodes.

A. MD5 (message-digest algorithm 5):

MD5 algorithm is a widely used cryptographic function with a 128- bit hash value. MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

MD5 processes a variable-length message into a fixed-length output of128 bits.

Step1: The input message is broken up into chunks of512-bit blocks; the message is padded so that its length is divisible by 512.

Step2: The padding works as follows: first a single bit 1, is appended to the end of the message.

Step3: This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512.

Step4: The remaining bits are filled up with a 64-bit integer representing the length of theoriginalmessage, in bits.

Step5: The MD5 algorithm uses 4 state variables each of which is a 32 bit integer (an unsignedlong on most systems). These variables aresliced and diced and are (eventually) the message digest. The variables are initialized as follows:

A = 0x67452301
B = 0xEFCDAB89
C = 0x98BADCFE
D = 0x10325476.

Step6: Now on to the actual meat of the algorithm: the main part of the algorithm uses four functions to thoroughly goober the above state variables. Those functions are asfollows:

F(X, Y, Z) = (X & Y) | (~(X) & Z)
G(X, Y, Z) = (X & Z) | (Y & ~ (Z))
H(X, Y, Z) = X ^ Y ^ Z

I(X, Y, Z) = Y ^ (X | ~ (Z))
Where &, |, ^, and ~ are the bit-wise AND, OR, XOR, and NOT operators

Step7: These functions, using the state variables andthe message as input, are used to transformthe state variables from their initial state intowhat will become the message digest. Foreach 512 bits of the message, the rounds performed (this is only pseudo-code, don't try to compile it).

After this step, the message digest is stored in the state variables (A, B, C, and D). To get it into the hexadecimal form you are used to seeing, output the hex values of each the state variables, least significant byte first.For example, if after the digest:

A = 0x01234567;
B = 0x89ABCDEF;
C = 0x1337D00D
D = 0xA5510101

Then the message digest would be:
67452301EFCDAB890DD03713010151A5 (required hash value of the input value).The node verification achieved through hash function., which states that if source node wants to verify the neighbor nodes the source S generates a hash id through hash function H(n)=PUB_KEY/IDENTITY, the public key and id of source node generates hash id. In the same way the neighbor nodes generate the hash id, if the source node hash id and neighbor node hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.

The process of DSCR protocol is:

a) Node configuration setting
b) Nodes unique identity
c) Message Exchange process for route discovery
d) Distance computation
e) Node position verification
f) Node verification process

B. Node Configuration Setting

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

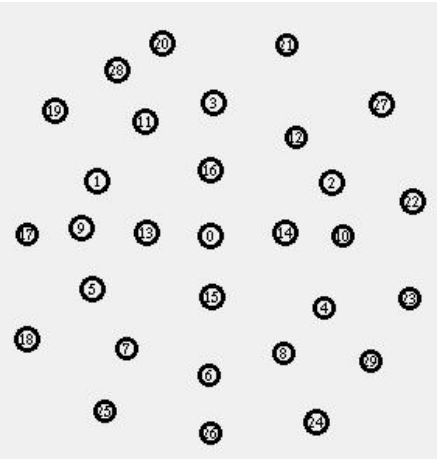


Fig.2: Nodes configuration

B. Nodes Unique Identity

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id.

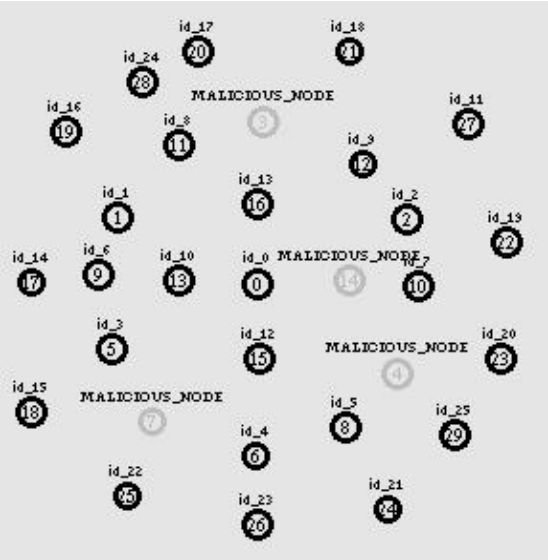


Fig.3: Nodes unique id

If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

C. Message exchange process for Route discovery

A verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange depicted in Fig. 2, within its 1-hop neighborhood. The aim of the message exchange is to let S collect information it can use to compute distances between any pair of its communication neighbors. To that end, POLL and REPLY messages are first broadcasted by S and its neighbors, respectively.

These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities. Then, after a REVEAL broadcast by the verifier, nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected.

The verifier S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood. Once S has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either:

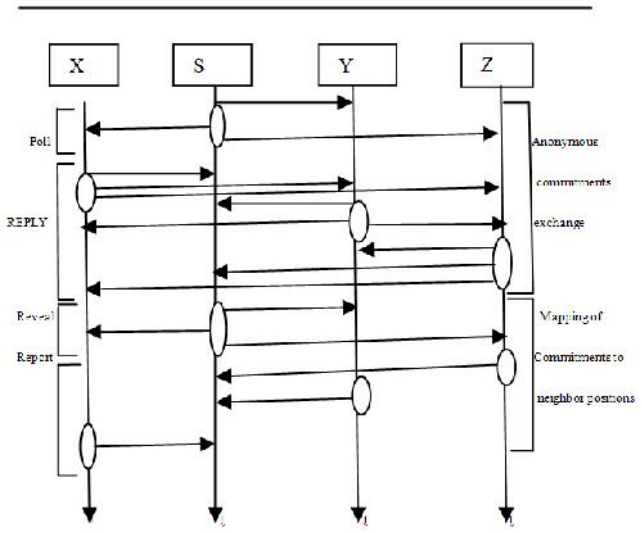


Fig.4: Message exchange process

1) Verified, i.e., a node the verifier deems to be at the claimed position;
2) Faulty, i.e., a node the verifier deems to have announced an incorrect position;
3) Unverifiable, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information.

Clearly, the verification tests aim at avoiding false negatives (i.e., adversaries announcing fake positions that are deemedverified) and false positives (i.e., correct nodes whose positions are deemed faulty), as well as at minimizing the number of unverifiable nodes.

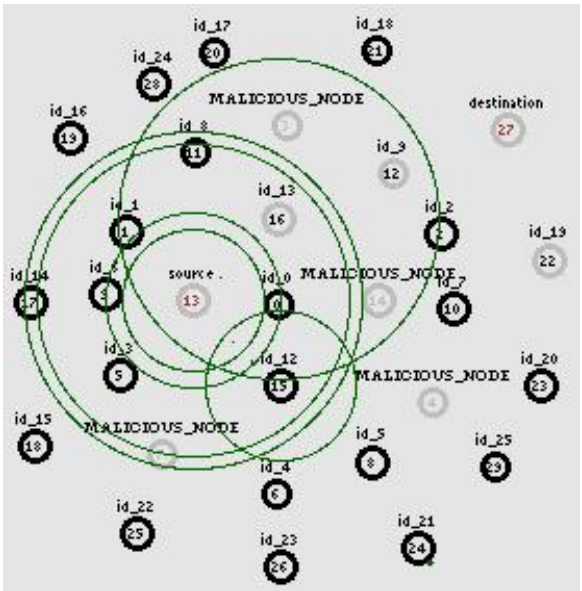


Fig.5: Message exchange process (Poll, Reply, Reveal, Report)

D. Distance computation

In order to compute the distance range, after a POLL and REPLY message a REVEAL message broadcast by the source nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected. The source S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood.

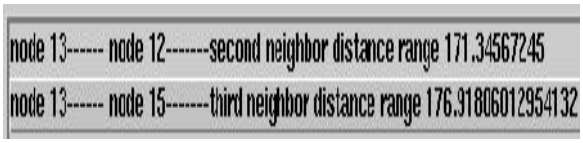


Fig.6: Calculate the distance

E. Node Position Verification

Once Source node has derived such distances, it runs several position verification tests in order to classify each candidateneighbor as either: Verified node, i.e., a node the verifier deems to be at the claimed position or Faulty node, i.e., a node the verifier deems to have announced an incorrect position or Unverifiable node, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information. The position verification isperformed by direct symmetric test, cross symmetry test and multilateration test.

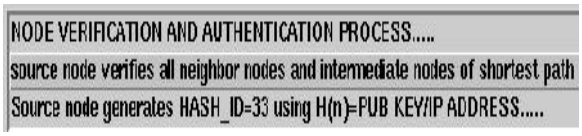


Fig. 7: Verify the node position

F. Node Verification Process

In this module a proposed work of node verification technique is introduced to detect the adversary nodes in the network. The node verification is done by hash function technique the public key and id of source node generates hash id.

In the same way the neighbor nodes generate the hash id, if the source node hash id and neighbor node hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.

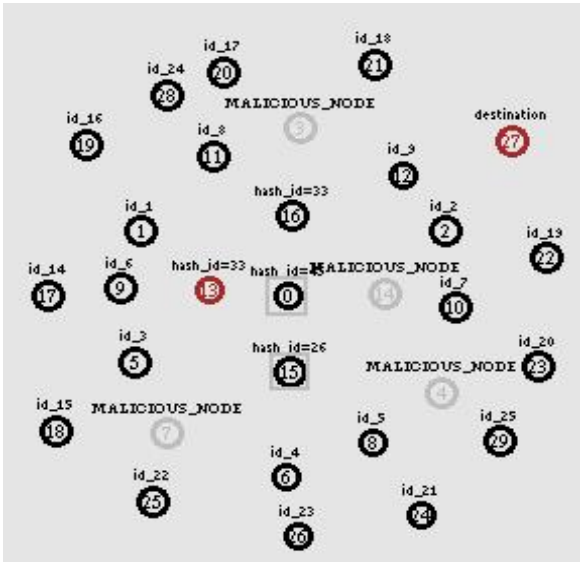
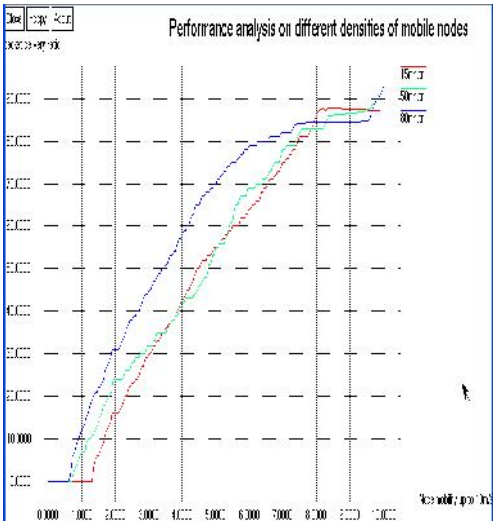


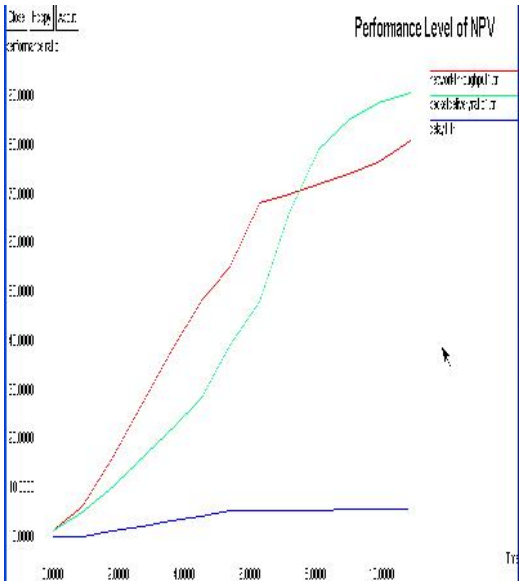
Fig. 8: Node Verification

V. GRAPH EXAMINATION

The performance analysis of the existing and proposed work is examined through graphical analysis.



(a). Mobile Nodes of different Density performance



(b). NPV Performance

Fig. 9: Performance analysis of mobile nodes density and NPV

VI. CONCLUSION

Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier. Simulation results confirm that our solution is effective in identifying nodes advertising false positions, while keeping the chance of false positives low. Only an awesome occurrence of colluding adversaries in the neighborhood of the verifier, or the unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NPV.

We presented a distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. The NPV protocol is higher layer protocols, as well as at extending it to proactive paradigm, useful in presence of applications that need each node to constantly the position of its neighbors.

REFERENCES

1) R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
2) J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
3) T. Govindaraj, and J. Jayasujitha," A Wide Area Monitoring System Using Neuro Control Technique for Load Restoration", IJIREEICE, 2014.
4) P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.
5) P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. _Capkun, and J.-P.Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.
6) T. Govindaraj, M. Vidhya,"Optimal Economic Dispatch for Power Generation Using Genetic Algorithm", IJIREEICE, 2014.
7) S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations," IEEE Trans. Mobile Computing, vol. 7, no. 4, pp. 470-483, Apr. 2008.
8) E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209,2008.
9) M. Poturalski, P. Papadimitratos, and J.-P.Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2008.
10) Dr.T.Govindaraj and Suresh kumar C, "Solving Environmental Power Unit Commitment with POZ Constraint Using Memetic Evolutionary Algorithm", IJIREEICE, Volume 2, Issue 2, Pages 1122-1129, 2014.
11) M. Poturalksi, P. Papadimitratos, and J.-P.Hubaux, "Towards Provable Secure Neighbor Discovery in Wireless Networks," Proc. Workshop Formal Methods in Security Eng., Oct. 2008.
12) P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.

13) R. Maheshwari, J. GAO, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.
14) L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2,pp. 233-246, Feb. 2006.
15) J. Ha¨rri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation with VanetMobiSim," Trans. Soc. Modeling & Simulation, 2009.
16) 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.
17) 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
18) 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.
19) 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)
20) 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.
21) 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
22) 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
23) 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
24) 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
25) 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
26) 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
27) 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 Indexed with Index Copernicus, Poland with Current Index Copernicus Value ICV of 5.09)
28) 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 Indexed with Index Copernicus, Poland with Current Index Copernicus Value ICV of 4.80, Scopus indexed)
29) 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 F ASCICLE III,ELECTROTECHNICS,ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS , July 2010 (ISSN 1221-454X)
30) 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
31) Govindaraj Thangavel ,"Low Frequency Axial Flux Linear Oscillating Electric Drive Suitable for Short Strokes" International Journal ISRN Electronics Volume 2014, Article ID 765161,2014

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 Coimbatore Institute of Technology, M.E. degreefrom PSG College of Technology and Ph.D. from Jadavpur University, Kolkatta, India in 1987, 1993 and 2010 respectively. His Biography is included in Who's Who in Science and Engineering 2011-2012 (11th Edition). Scientific Award of Excellence 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 the Department of Electrical and Electronics Engineering, Muthayammal Engineering College affiliated to Anna University, Chennai, India. His Current research interests includes Permanent magnet machines, Axial flux Linearoscillating Motor, Advanced Embedded power electronics controllers, finite element analysis of special electrical machines, Power system Engineering and Intelligent controllers. He is a Fellow of Institution of Engineers India (FIE) and Chartered Engineer (India). Senior Member of International Association of Computer Science and Information Technology (IACSIT). Member of International Association of Engineers (IAENG), Life Member of Indian Society for Technical Education (MISTE). Ph.D. Recognized Research Supervisor for Anna University and Satyabama University, Chennai. Editorial Board Member for journals like International Journal of Computer and Electrical Engineering, International Journal of Engineering and Technology, International Journal of Engineering and Advanced Technology (IJEAT). International Journal Peer Reviewer for Taylor & Francis International Journal "Electrical Power Components & System", United Kingdom, Journal of Electrical and Electronics Engineering Research, 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, E3Journal 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 award for ICEESPEEE 09 conference paper. Coordinator for AICTE Sponsored SDP on special Drives, 2011. Coordinator for AICTE Sponsored National Seminar on Computational Intelligence Techniques in Green Energy, 2011. Chief Coordinator and Investigator for AICTE sponsored MODROBS – Modernization of Electrical Machines Laboratory. Coordinator for AICTE Sponsored International Seminar on "Power Quality Issues in Renewable Energy Sources and Hybrid Generating System", July 2013.

Kalaiyarasi.M received her B.Tech, Degree in Information Technology from Anna Unveristy of Technology, Coimbatore, Tamil Nadu and also Pursuing M.Tech, Degree in Information Technology from Jayam College of Engineering and Technology, which is affiliated to Anna University, Chennai. The area of Interest is Cryptography and Network Security, Wireless Sensor Networks, and Cloud Computing.