IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-8 E-ISSN: 2347-2693

Light Weight Security Attack in Mobile Ad Hoc Network (MANET)

H. Muthukrishnan[1*] and S. Anandamurugan[2]

[1*,2]Department of Information Technology, Kongu Engineering College,Perundurai.[1]

www.ijcaonline.org

Received: 02/07/ 2014 Revised: 22/07/ 2014 Accepted: 17/08/ 2014 Published: 31 /08/ 2014

Abstract - Mobile ad hoc network (MANET) is a collection of mobile nodes that communicate with each other without any fixed infrastructure or a central network authority. From a security design perspective, MANETs have no clear line of defense; i.e. no built-in security. Thus, the wireless channel is accessible to both legitimate network users and malicious attackers. Since MANET requires a unique, distinct, and persistent identity per node in order for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network. Here a lightweight scheme is used to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. Through the help of extensive simulations, it is able to demonstrate that this scheme detects Sybil identities with good accuracy even in the presence of mobility.

Keywords: *Legitimate Network, Sybil Identity, Received Signal Strength*

I. INTRODUCTION

1.1 WIRELESS AD HOC NETWORKS

A wireless ad hoc network is a decentralized wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed wireless networks. Instead, each node participates in routing by forwarding data to other nodes. Wireless ad hoc networks can be further classified as:

- Mobile ad hoc networks (MANETs)
- Wireless mesh networks
- Wireless sensor networks

1.2 AD HOC NETWORKS

A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless as shown in Figure 1.1. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each device act as a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

1.2.1 Attack Classifications

The attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Below is the Schematics of various attacks:

- Application Layer : Malicious code, Repudiation
- Transport Layer : Session hijacking, Flooding
- Network Layer : Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC : Malicious Behaviour, Selfish Behaviour, Active, Passive, Internal External
- Physical : Interference, Traffic Jamming, Eavesdropping

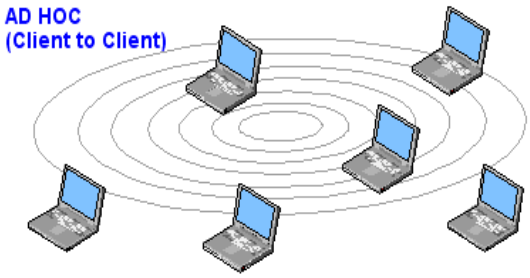

Figure 1.1 Wireless ad hoc networks

1.3 ROUTING IN AD HOC NETWORKS

Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks including the telephone network, electronic data networks and transportation networks. In ad hoc network[14], there is no proper infrastructure. The basic idea is that, a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nearby nodes and how to reach them. It may announce that it can reach them. An ad hoc routing protocol is a standard that controls how nodes decide the way to route packets between computing devices in an ad hoc network. The following is a list of some ad hoc network routing procedures:

- **Table-driven Routing Protocol**

This type of protocol maintains fresh lists of destinations and their routes by periodically distributing routing tables

Corresponding Author: H. Muthukrishnan[1]

throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance
2. Slow reaction on restructuring and failures

- **On-demand Routing Protocol**

This type of protocol finds a route on demand by flooding the nework with route request packets. The main disadvantage of such algorithm is its high latency time in route finding.

- **Geographical Routing protocols**

This type of protocols acknowledges the influence of physical distances and distribution of nodes to areas as significant to network performance. The main disadvantages of such algorithms are:

1. Efficiency depends on balancing the geographic distribution versus occurrence of traffic
2. Any dependence of performance with traffic load thwarting the negligence of distance may occur in overload

1.4 SYBIL ATTACK

In the Sybil attack[3] a single node presents multiple fake identities to other nodes in the network. Sybil attacks pose a great threat to decentralized systems like peer-to-peer networks and geographic routing protocols. A Sybil attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or node-disjoint paths. In reputation and trust-based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing other's reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.

II. LITERATURE REVIEW

2.1 EXISTING SYSTEM

In existing system one of used technique is Trusted Certification. It provides a centralized authority for establishing a Sybil-free domain of identities. Each entity in the network is bound to a single identity certificate. Next is the Resource Testing: These tests are carried out to check the computational ability, storage ability and network bandwidth of a node. A Sybil attack will not possess a sufficient amount of resources to perform the additional tests imposed on each Sybil identity. In the Recurring Costs and Fees approach, identities are periodically re-validated in the network. Each participating identity is periodically or one-time charged with a fee. Piro et al proposed to detect Sybil identities by observing node dynamics. Nodes are keeping track of identities which are often seen together (Sybil identities) as opposed to the honest distinct nodes that move freely in different directions.

The random key distribution technique enables nodes on a wireless sensor network to establish secure links for communicating with each other. In random key predistribution, a set of keys are assigned at random to a node enabling it to discover or compute the common keys that it shares with its neighbouring nodes. Node-to-node[11] secrecy is ensured by using the common keys as a shared secret session key. The main ideas are the association of the identity with the key assigned to a node and the validation of the key. Validation involves ensuring that the network is able to validate the keys that an identity might have. The forged Sybil identity will not pass the key validation test as the keys associated with a random identity will most likely, not have an appreciable intersection with the compromised key set. Sybil attacks may also be used to enable the attacker to obtain an unfair and disproportionately large share of resources that were intended to be distributed amongst all nodes on the network equally. This attack denies legitimate nodes their deserved share of resources and also provides the malicious node with more avenues for other attacks.

2.2 DRAWBACKS IN EXISTING SYSTEM:

- Trusted certification suffers from costly initial setup, lack of scalability and a single point of attack or failure
- The drawback of Resource testing is that an attacker will get enough hardware resources, such as storage, memory, and network cards to accomplish these tasks
- The scheme will produce high false positives where node density is high, such as a conference hall or nodes moves in a same direction, such as a group of soldier moving toward a target
- It existing extra hardware like antennae and GPS is required to detect the Sybil attacker
- It is a complex task to maintain the Random Distribution Key

2.3 PROPOSED SYSTEM

In the proposed system the concept used to detect the Sybil Attacker is RSS and neighbour joining behavior. This system also identifies the two types of Sybil attack[3] i.e. whitewashing (WID) and Simultaneous attack. The Received Signal Strength (RSS) detection concept is based on the application of the Distance. RSS states that if a node is nearer to the destination node and its distance if found under the particular range then obviously it's RSS value will be high and the node is detected as a Sybil node. Comparatively the Good node (GID) distance will be high enough than the Sybil Node distance. So, it is clear from our approach that if the distance of a particular node to the destination is less, it's RSS will be high whereas if the Distance of a node is High then its RSS value will be Low. Based on this Concept all the attacker node is detected in our network with good accuracy

2.4 ADVANTAGES OF PROPOSED SYSTEM

- No use of centralized trusted third party or any extra hardware
- No complexity in the design of the system since it does not require any random key distribution
- Easy to calculate the distance between the centralized nodes
- Since it uses the concept of RSS it produce 90% true positive,10% false negative
- The implementation is not much costlier based on the design, time consumption, bandwidth usage

III. PROBLEM DESCRIPTION

3.1 PROBLEM DEFINITION

The Sybil attack as a malicious device illegitimately taking on multiple identities. The malicious device's additional identities as Sybil nodes. To better understand the implications of the Sybil attack and how to defend against it, develop a taxonomy of its different forms. This concept include three orthogonal dimensions: direct vs indirect communication, fabricated vs stolen identities, and simultaneity. One way to perform the Sybil attack is for the Sybil nodes to communicate directly with legitimate nodes. When a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Likewise, messages sent from Sybil nodes are actually sent from one of the malicious devices. To defend against the Sybil attack[3], it is necessary to validate that each node identity is the only identity presented by the corresponding physical node.

3.2 PROBLEM SOLUTION

Sybil detection approach is composed of two complementary techniques. The first one is a localization verification technique based on received signal strength variations, under the assumption that all messages are sent with the same signal power. This technique allows a node to verify the authenticity of another node by estimating its future geographical localizations, and compare them to its evaluated localizations. When a node is detected suspect (incoherent signal strengths gradient), our second technique should be used. The second type is indirect validation, in which nodes that have already been verified are allowed to vouch for or refute other nodes.

3.3 MODULES OF PROPOSED SYSTEM

3.3.1 Topology Formation with Neighbour discovery phase

Initially the nodes are created in ns2 simulator with a unique identity. Here each node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous neighbor establishment. Next is neighbor discovery[11], in this each source node identifies its neighbor nodes through broadcasting packets, through this process each node detects its neighbor nodes corresponding to location and distance. Based on the neighbour discovery phase each node forms a stable path to destination.

3.3.2 Detection of Attack Models

There are two types of Sybil attacks. In the first one, an attacker creates new identity while discarding its previously created one hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities. This attack potentially promotes lack of accountability in the network. In the second type of Sybil attack[3], an attacker concurrently uses all its identities for an attack, called simultaneous Sybil attack[3]. The motivations of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network. The difference between the two is only the notion of simultaneity. However their applications and consequences are different.

3.3.3 Sybil Detection based on RSS

The RSS[5] concept is enhanced to detect the Sybil nodes in the network. The destination receives data from each mobile node. The RSS value is calculated by the destination for every mobile node under different speed. Then the destination is capable to analyze the distance of each node, the Sybil node distance value will be low enough but its RSS will be high whereas the legitimated node distance value will be high so its RSS value will be low.

The Sybil detection approach is based on a relative localization technique[5] using received signal strength variations, under the assumption that all messages are sent with the same signal power. There is an assumption that Sybil node should use a steady transmission power. The Sybil detection concept is composed of two complementary techniques. The first one is a localization verification technique based on received signal strength. This technique allows a node to verify the authenticity of another node by estimating its future geographical localizations, and compare them to its evaluated localizations. When a node is detected suspect (incoherent signal strengths gradient), our second technique should be used. This technique is a Sybil detection mechanism, based on the definition of a neighbour nodes. This mechanism is launched individually by every node in the network in order to detect Sybil identities based on their distance and hop count.

IV. SYSTEM IMPLEMENTATION

4.1 INTRODUCTION

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator, partly because of the range of features it provides and partly because it has an open source code that can be modified and extended.

4.1.1 Network Simulator

Network simulator is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is

not a polished product yet and bugs are being discovered and corrected continuously. NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios.

NS can simulate the following:

1. **Topology:** Wireless
2. **Scheduling Algorithms:** AODV
3. **Transport Protocols:** UDP
4. **Routing:** Static and dynamic routing

4.2 NODE AND ROUTING

A node is a compound object composed of a node entry object and classifiers as shown in Figure 5.1. There are two types of nodes in NS. A unicast node has an address classifier that does unicast routing and a port classifier. A multicast node, in addition, has a classifier that classify multicast packets from unicast packets and a multicast classifier that performs multicast routing.

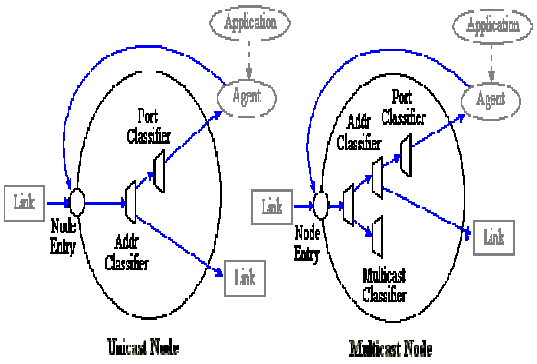

Figure 4.1 Node (Unicast and Multicast)

In NS, Unicast nodes are the default nodes. To create Multicast nodes, the user must explicitly notify in the input OTcl script, right after creating a scheduler object, that all the nodes that will be created are multicast nodes. After specifying the node type, the user can also select a specific routing protocol other than using a default one.

- **Unicast**
  - $ns rtproto type
  -type: Static, Session, cost, multi-path
- **Multicast**
  - $ns multicast (right after set $ns [new Scheduler])
  - $ns mrtproto type
  - type: CtrMcast

5.2.1 Topology Formation

Constructing project design in NS2 should takes place. In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous neighbor establishment.

5.2.2 Neighbor discovery

Here each source node identifies its neighbor nodes through broadcasting packets, through this process each node detects its neighbor nodes corresponding to location and distance. Based on the neighbor discovery phase each node forms a stable path to destination.

5.2.3 Data Transmission

After the source node S successfully finds out a route to the destination source node S, successfully finds out a route to the destination node D, S will start data transmission under the mobility factor.

5.2.4 Sybil detection

The RSS algorithm is enhanced to detect the Sybil nodes in the network. The destination receives data from each mobile node. The RSS value is calculated by the destination for every mobile node under different speed of mobile nodes. The Sybil nodes doesn't have any neighbors list and hop count, based on this RSS value determination the Sybil node is detected.

4.2.5 Graph Based Result

Graph is an essential part of display a result, so to plot a graph to show a various result comparison with packets, throughput, RSS for arbitrary nodes, RSS with different speed and etc.

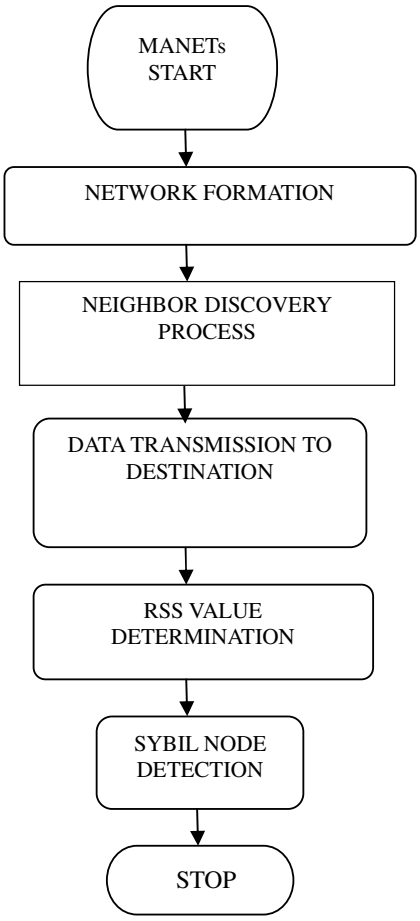

Figure 4.2 Data Flow Diagram

4.3 AD HOC ON-DEMAND DISTANCE-VECTOR PROTOCOL

AODV is routing algorithm used in ad hoc networks. Unlike DSR, it does not use source routing, but like DSR it is on-demand. In AODV, each node maintains a routing table which is used to store destination and next hop IP addresses as well as destination sequence numbers. Each entry in the routing table has a destination address, next hop, precursor nodes list, lifetime, and distance to destination. The concepts of AODV that make it desirable for MANETs with limited bandwidth include the following:

- Minimal space complexity: The algorithm makes sure that the nodes that re not in the active path do not maintain information about this route. After a node receives the RREQ and sets a reverse path in its routing table and propagates the RREQ to its neighbors, if it does not receive any RREP from its neighbors for this request, it deletes the routing info that it has recorded.
- Simple: It is simple with each node behaving as a router, maintaining a simple routing table, and the source node initiating path discovery request, making the network self-starting.
- Most effective routing info: After propagating an RREP, if a node finds receives an RREP with smaller hop-count, it updates its routing info with this better path and propagates it.
- Most current routing info: The route info is obtained on demand. Also, after propagating an RREP, if a node finds receives an RREP with greater destination sequence number, it updates its routing info with this latest path and propagates it.
- Highly Scalable: The algorithm is highly scalable because of the minimum space complexity and broadcasts avoided when it compared with DSDV

V. RESULTS AND DISCUSSION

5.1 END TO END DELAY

It is the average time taken by a data packet to arrive in the destination. With an increase in the number of nodes, the delay increases. The number of packets used to discover the route increases with increase in the number of nodes. But when compared with the existing methodology, the proposed system decreases the delay and increase the throughput by about 25%.

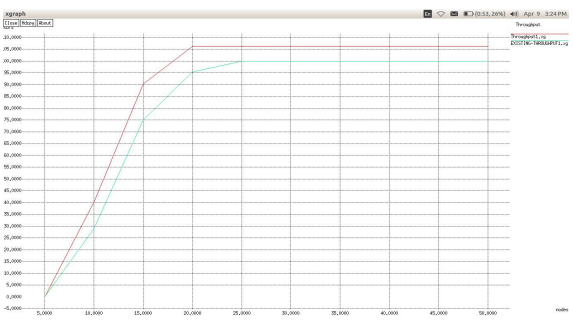

Fig 5.1 End to End Delay

5.2 PACKET LOSS

The routing overhead indicates the number of packets dropped in between while sending from the source to the destination. It increases with an increase in the number of nodes. When compared with existing methodology, the proposed approach decreases packet loss by about 45.9%.

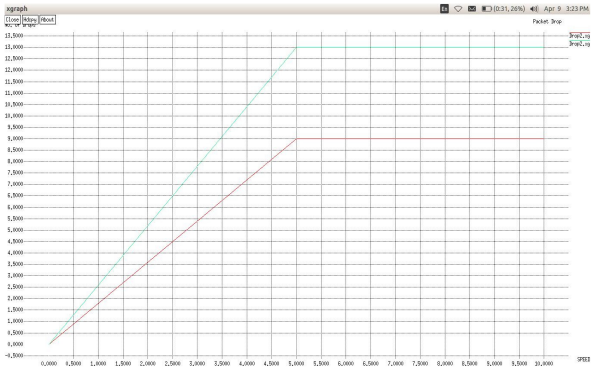

Fig 5.2 Packet Loss

VI. CONCLUSION AND FUTUREWORK

CONCLUSION

The RSS-based detection mechanism, detect the Sybil attacker in the network. The demonstration is given through the simulation by using the application of distance with the RSS value and also with the help of the neighbour joining behaviour. The simulation also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. The simulation results showed that our mechanism works better even in mobile environments and detect both join-and-leave and simultaneous Sybil attackers with a high degree of accuracy.

FUTURE WORK

In future, it is planned to generalize the proposed method by improving the result to 100% true positives even in the mobile environment with the help of test bed experiment

REFERENCES

[1]. Douceur J R (2002), 'The Sybil attack', Revised Papers from the First International Workshop on Peer-to-Peer Systems, Vol.6, No.9, pp.251 -260.

[2]. Capkun S, Hubaux J P and Buttyan L (2006), 'Mobility helps peer-to-peer security', IEEE Trans. Mobile Comput., Vol. 5, No. 1, pp.43 -51.

[3]. Piro C, Shields C and Levine B N (2006), 'Detecting the Sybil attack in mobile ad hoc Networks',Proceeding. Securecomm Workshops, pp.1 -11.

[4]. Chen Y, Yang J, Trappe W and Martin R P (2010), 'Detecting and localizing identity- based attacks in wireless and sensor networks', IEEE Trans. Veh. Technol., Vol. 59, pp.2418 -2434.

[5]. Abbas S, Merabti M, Llewellyn-Jones D, Kifayat K (2013), 'Lightweight Sybil Attack Detection in MANETs', IEEE Systems Journal, Vol.7 , No.2 pp.236-248.

[6]. M. Bianchini, M. Gori, and F. Scarselli. Inside pagerank. ACM Trans. Inter. Tech. 5(1):92–128, 2005.
[7]. A. Bhargava, K. Kothapalli, C. Riley, C. Scheideler, and M. Thober. Pagoda: a dynamic overlay network for routing, data management, and multicasting. In Proc.ACM Symp on Parallel Algorithms, pages 170–179, 2004.
[8]. R. Bhattacharjee and A. Goel. Avoiding Ballot Stuffing in eBay-like Reputation Systems. In ACM SIGCOMM Workshop on the Economics of Peer-to-Peer Systems , August 2005.
[9]. M. Bianchini, M. Gori, and F. Scarselli. Inside pagerank. ACM Trans. Inter. Tech.5(1):92–128, 2005.
[10]. R. B¨ohme, G. Danezis, C. D´ıaz, S. K¨opsell, and A. Pfitzmann. Mix cascades vs. peer-to-peer: Is one concept superior? In Proc. Wkshp on Privacy Enhancing Technologies ,pages 243–255, 2004.
[11]. S. Buchegger and J.-Y. L. Boudec. A Robust Reputation System for P2P and Mobile Ad hoc Networks. In Proc. Wkshp on the Economics of Peer-to-Peer Systems , 2004.
[12]. J. Bulgatz. More Extraordinary Popular Delusions and the Madness of Crowds. Three Rivers Press, 1992.
[13]. S.Capkun and J.-P. Hubaux. BISS: building secure routing out of an incomplete set of secure associations. In Proc. ACM Wireless Security Conference , pages 21– 29, 2003
[14]. Sonam Gupta and Rekha Sharma," A QoS Based Simulation Approach of Zone Routing Protocol in Wireless Ad-hoc Networks ", International Journal of Computer Sciences and Engineering, Volume 2, issue 7, P.No 24-30, 2014

AUTHOR'S PROFILE

I, Muthukrishnan.H has completed my under graduation studies B.Tech(IT) from K.S.R College of technology affiliated to Anna University Chennai in the year 2006. Then I was employed as a software programmer in IT sector, then I have undertaken my post graduation M.E(CSE) in Mobile adhoc Network as my area specialization from Kongu Engineering College, affiliated to Anna Univeristy Chennai in the year 2010. As soon as I completed my course of education , I had been recruited as Assistant Professor in the same college. Since then I have started my career as Assitant Professor from 2010 June. My areas of interest covers Manet, Vanet, Database Technology, Datamining and its tools like Informatica, Datastage etc. And recently started working with MongoDb which is a NoSql database. And I have published a book in Cloud computing and E-learning module in the public and private cloud infrastructure. Have conducted many workshops on network simulators like GlomoSim and NS2.

Dr.S. ANANDAMURUGAN obtained his Bachelor's degree in Electrical and Electronics Engineering from "Maharaja Engineering College - Avinashi" under Bharathiyar University and Masters Degree in Computer Science and Engineering from "Arulmigu Kalasalingam College of Engineering – Krishnan Koil" under Madurai Kamaraj University. He completed his Ph.D in Wireless Sensor Networks from Anna University, Chennai. He has 13 years of teaching experience. Currently he is working as an Assistant Professor (Selection Grade) in the department of Information Technology in Kongu Engineering College, Perundurai. He is a life member of ISTE, CSI & ACEEE. He has received "**Best Staff"** award for the year 2007-08. He has authored more than 70 books. He has Published 20 papers in International and National Journals and 10 Papers in International and National Conferences. His area of interest includes Sensor Networks and Green Computing. He is an Editorial Board Member of the International Journal of Computing Academic Research (IJCAR). He has organized 1CSIR sponsored seminar for the benefit of faculty members and students. He has attended about 40 Seminars, FDP's, and Workshops organized by various Engineering colleges.