A System of Umpires for Security of Wireless Mobile Ad Hoc Network

Ayyaswamy Kathirvel, Rengaramanujam Srinivasan
Faculty of Computer Science and Engineering, B.S.Abdur Rahman University, India.

Abstract*:* *A mobile ad hoc network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Protecting the network layer from malicious attacks is an important and challenging issue in both wired and wireless networks and the issue becomes even more challenging in the case of MANET. In this paper we propose a solution of umpiring system (US) that provides security for routing and data forwarding operations. Umpiring system consist of three models, are single umpiring system (SUS), double umpiring system (DUS), and triple umpiring system (TUS). In our system each node in the path from source to destination has dual roles to perform: packet forwarding and umpiring.US does not apply any cryptographic techniques on the routing and packet forwarding message. In the umpiring role, each node in the path closely monitors the behavior of its succeeding node and if any misbehavior is noticed immediately flags off the guilty node. For demonstration, we have implemented the umpiring system by modifying the popular AODV protocol.*

Keywords: *single umpiring system, double umpiring system, triple umpiring system, Malicious nodes.*

Received September17, 2009; Accepted December 23, 2009

1. Introduction

A mobile ad hoc network (MANET) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Each node moves and operates in a distributed peer-to-peer mode, generating independent data and acting as a router to provide multi-hop communication. MANET is ideally suited for potential applications in civil and military environments, such as responses to hurricane, earthquake, tsunami, terrorism and battlefield conditions. Security is an important aspect in such mission critical applications.

In this paper we tackle the problem of securing the network layer operations from malicious nodes. Malicious nodes may disrupt routing algorithms by transmitting a false hop count; they may drop packets, route the packets through unintended routes and so on. Our work rests on the foundations of two excellent systems already proposed: the twin systems of watchdog and pathrater [21] and SCAN [3]. A brief look at each one of them is in order.

Marti et al. [21] introduced two extensions to the Dynamic Source Routing Protocol DSR to mitigate the effect of routing misbehaviors – watchdog and pathrater. The watchdog identifies misbehaving nodes while the pathrater avoids routing packets through these nodes. When a node forwards packets the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next hop transmissions. If the next node doesn't forward the packet then it is misbehaving. The watchdog detects the misbehavior and sends a message to the source, notifying it of the misbehaving node.

In SCAN [3] two ideas are exploited to protect the mobile ad hoc network: (i) local collaboration where the neighboring nodes collectively monitor each other and (ii) information cross-validation by which each node monitors neighbors by cross-checking the overheard transmissions.

In SCAN, each node monitors the routing and packet-forwarding behavior of its neighbors and independently detects the existence of malicious nodes in its neighborhood. This is made possible because of wireless nature of the medium and all the involved nodes are within each other's transmission. In order to enable cross-checking they have modified AODV protocol and added a new field *next_ hop* in the routing messages so that each node can correlate the overheard packets accordingly.

While each node monitors it neighbors independently all the nodes in the neighborhood collaborate to convict a malicious node. An agreement between a minimum of k neighboring nodes is required for convicting a malicious node. Once its neighbors convict a malicious node the network reacts by depriving it of its right to access the network. In SCAN each node must possess a valid token in order to interact with other nodes. They have used asymmetric key cryptography to prevent forgeries of tokens. A group of nodes (minimum-k) can collaboratively sign a token, while no single node can do so. Further each node has to get its token renewed periodically by its neighbors. A node which behaves continuously in a good manner can get its token renewed at less frequent intervals as compared to a fresh entrant node.

Our umpiring system has been strongly influenced by the above two schemes. In our system all the active nodes have dual roles just as in watchdog; we also exploit promiscuous hearing functionality as done by both SCAN and watchdog. We have adopted the token concept from SCAN. We achieve the avoidance of malicious nodes by a system of tokens, which is similar to the ones used in SCAN. Token is a pass or validity certificate enabling a node to participate in the network. It contains two fields: nodeID and status bit; nodeID is considered to be immutable. Initially the status bit of all participating nodes is set as 0 indicating “green flag” with freedom to participate in all network operations. It is assumed that a node cannot change its own status bit. When an umpiring node finds its succeeding node misbehaving it sends a M-Error message to the source and malicious node’s status bit is changed using M-Flag message (set to 1 indicating “red flag”). With “red flag” on the culprit node is prevented from participating in the network.

Our objective is designing the security system is to keep the overhead as minimum as possible while optimizing the throughput. We do not use encryption or key algorithms as done by SCAN. We find that token issuing and token renewals and broadcasts to announce convictions create very large communication overheads and also degrade energy performance, which SCAN has completely over looked. There is no token renewal feature in our system. In our system all the nodes are pre issued with green tokens. They continue to enjoy the status until any immediate ancestor node, in its umpiring mode finds its next node misbehaving, sends the M-Error and M-Flag messages and red flag is set.

Just like SCAN in order to facilitate cogent promiscuous hearing we have used “next_hop” field with our AODV implementation. Our umpiring system can detect any false reporting of hop count during the route reply process RREP. In watchdog detection of malicious action is by a single node while in SCAN it is done by a set of neighbors. In our system the designated predecessor node in its umpiring role carries out both detection and conviction.

The rest of the paper is organized as follows: section 2 provides a models and assumptions; section 3 discusses umpire system security models. Section 4 presents simulation results; section 5 discusses the related work and section 6 gives the conclusions.

2. Models and Assumptions

Assumptions made in the design of Umpiring system are as follows:

1.A wireless ad hoc network where nodes are free to move about or remain at stand still, at their will is assumed.

2.Nodes may fail at any time.

3.There exists a bi-directional communication link between any pair of nodes, which is a requirement for most wireless MAC layer protocols including IEEE 802.11 for reliable transmission.

4.Wireless interfaces support promiscuous mode of operation.

Promiscuous hearing means, over hearing by a node say A, messages not addressed to it, transmitted by a second node B, situated in the communication range of A, to a third node C. Most of the existing IEEE 802.11 based wireless cards support such promiscuous mode of operations, to improve routing protocol performance.

3. Umpiring System Security Model

In the umpiring system each node is issued with a token at the inception. The token consists of two fields: NodeID and status. NodeID is assumed to be unique and deemed to be beyond manipulation; status is a single bit flag. Initially the status bit is preset to zero indicating a green flag. The token with green flag is a permit issued to each node, which confers it the freedom to participate in all network activities[8-11].

Each node in order to participate in any network activity, say Route Request RREQ, has to announce it’s token. If status bit is “1” indicating “red flag” protocol does not allow the node to participate in any network activity.

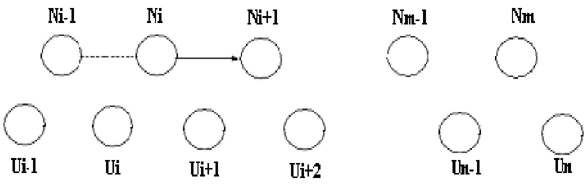
We investigate an umpiring system for securing the mobile ad hoc networks from attacks from malicious nodes. We consider following systems:

- Single Umpiring System (SUS)
- Double Umpiring System (DUS)
- Triple Umpiring System (TUS)

It is assumed that the source and the destination node are not malicious. A brief look at each one of them is in order.

3.1.Single Umpiring System

In the single umpiring system an additional node is appointed as designated umpires is illustrated in Fig. 1. In the figure Ui-1, Ui, Ui+1, Ui+2 . . Un-1, Un are designated umpires and Ni-1, Ni, Ni+1 . . Nm-1, Nm is nodes. Assume that Ni-1 as a source node and Nm is designated node. The role of the designated umpires is overhearing both routing message and packet forwarding message in the promiscuous mode. When a designated umpire node is found to be misbehaving – say dropping forwarded packets or changing Hop_count and sequence number, the corresponding umpire immediately sends a M-ERROR message to the source and the status bit of guilty node is set to “1” – red flag using M-Flag message[12].



During data forwarding and route RREP, Ui-1 and Ui is the umpire for Ni-1, Ui and Ui+1 is the umpire for Ni. . . ..Un-1 and Un is the umpire for Nm

Ni-1, Ni, Ni+1 . . . Nm-1 and Nm are Nodes
Ui-1, Ui, Ui+1, Ui+2 . . . Un-1 and Un are designated Umpires

Figure 1. Umpiring System Model for Security.

In the figure1 node Ui is the designated umpire for node Ni. Similarly node Ui+1 are the designated umpire for node Ni+1. Designated umpire node Ui+1, can tell correctly whether node Ni is forwarding the packet sent by it, by promiscuously hearing Ni+1's transmissions. During reply process RREP, umpire node Ui+1 can verify whether Ni+1 is unicasting the route reply RREP and whether the hop count given by Ni+1 is correct. Thus during forward path and reverse path node Ui+1 act as umpire.

3.2. Double Umpiring System

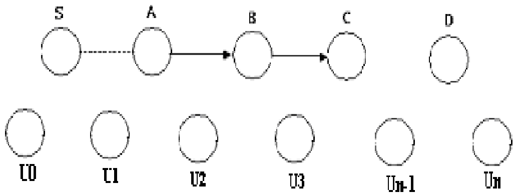
The working of the double umpiring system is explained with reference to Fig. 1. There are two umpires which monitor the behavior of an intermediate node. The role of the double umpiring system, the designated umpires is overhearing both routing message and packet forwarding message in the promiscuous mode.

In the figure 1 node Ni is monitored by umpire Ui and umpire Ui+1. If both umpires ague the node is misbehaving then Ni can be quarantined.

Assume that node B is culprit in the figure 2. It is dropping the forwarded data packets given by node A. Now designate umpire node U2 and U3 can overheard B‘s transmission, the designated umpire immediately sends a M-ERROR message to the source and the status bit of culprit node is set to "1" – red flag using M-Flag message.

3.3. Triple Umpiring System

The working of the Triple umpiring system is explained with reference to Fig. 1. In Triple umpiring system, three umpires are used to identify and convict the guilty node. Three umpires in TUS are a node (next/previous immediate node) and two additional nodes is appointed as designated umpires i.e., Ui and Ui+1 are designated umpires for node Ni. Umpire Ui and Ui+1 are located so that they can overhear communication to Ni. Similarly Ni-1 and Ni+1 monitor the performance of Ni in the forward and reverse paths respectively [13, 16].



During data forwarding and route RREP, U0 and U1 is the umpire for S, U1 and U2 is the umpire for A, Un-1 and Un is the umpire for D

S: Source; D: Destination; A, B, C intermediate nodes
U1, U2, U3 .. Un, Un-1 : Designated Umpires

Figure 2. Triple umpiring system model.

The decision can be made by all the 3 nodes involved: Ni-1 in its umpiring node in the forward path (Ni+1 in the reverse path) and Ui and Ui+1. The decision can be bound up an all of them auguring or any two of them auguring about the misbehavior of the node Ni.

In the figure 2, umpire node U2 and U3 are designated umpires for node B. similarly node Un-1 and Un are designated umpires for the destination node D. Assume that node B is culprit in the Fig. 2. It is dropping the forwarded data packets given by node A. Now designate umpire node U2, U3 and node A can overheard B‘s transmission, the designated umpire immediately sends a M-ERROR message to the source and the status bit of culprit node is set to "1" – red flag using M-Flag message.

In our system there is no change in the token – it can be used for the full lifetime of the node, if the node continuously behaves correctly. At the instance of the first offence the status of the guilty node is set to 1 preventing its further participation in the network.

We assume that no node can alter its own status bit. Only the designated umpire corresponding to the forward or reverse path under consideration can change the status bit. For example the status bit of B in Fig.2 can be changed only by A in the forward path and only by C in the reverse path. It is also assumed that a node cannot announce wrongly its token particulars – NodeID and status bit.

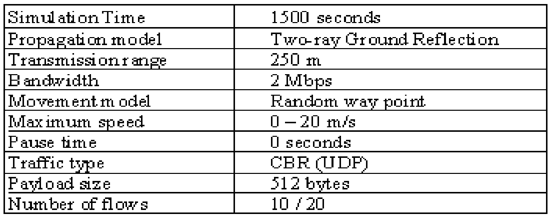
4. Simulations and Results

We use a simulation model based on QualNet 4.5 in our evaluation [1,14, 22]. Our performance evaluations are based on the simulations of 100 wireless mobile nodes that form a wireless ad hoc network over a rectangular (1500 X 600 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11 [7]. The performance setting parameters are given in Table 1 [7-17].

Before the simulation we randomly selected a certain fraction, ranging from 0 % to 40 % of the network population as malicious nodes. We considered only two attacks – modifying the hop count and dropping packets. Each flow did not change its source and destination for the lifetime of a simulation run.

We have done four sets of studies corresponds to 10 flows with flows between 10 different source-destination pairs. Set I corresponds to SUS, Set II, and Set III are corresponds to DUS, and TUS respectively.

Table 1. Parameter settings.



Simulation Time	1500 seconds
Propagation model	Two-ray Ground Reflection
Transmission range	250 m
Bandwidth	2 Mbps
Movement model	Random way point
Maximum speed	0 – 20 m/s
Pause time	0 seconds
Traffic type	CBR (UDP)
Payload size	512 bytes
Number of flows	10 / 20

There are some critical issues to be discussed:
What happens when the umpires themselves are malicious?

We have investigated two types of malicious behavior of umpires (i) Umpires who after accepting umpireship are not acting as umpires; possibly, they are selfish they are conserving their own energy. These umpires, if they detect any misbehaving node they simply ignore them. We call them '*sleeping umpires*'. The second category of umpires is strongly malicious in that, they totally behave in a malicious way. If they detect malicious behavior of a node they ignore; but they go to book innocent nodes.

Our experiments are based on four important parameters:

4.1. Throughput

In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources. We present in Tables 2 the packet delivery ratios of Set I - III for 30 percentage of malicious node, with node mobility varying between 0 to 20 M/s.

Table 2. Packet delivery ratios of Set I to III for 30 % malicious nodes.

Mobility (M/s)	30 Percentage of Malicious nodes		
	SUS	DUS	TUS
0	71.23	67.94	65.25
5	68.86	64.18	61.51
10	65.41	61.11	58.42
15	64.38	60.88	58.26
20	63.52	59.18	56.29

From Table 2 the following conclusions can be drawn:

- In general packet delivery ratio decreases as mobility and percentage of malicious nodes increase.
- In the case of Set-I, with 30% malicious nodes, packet delivery ratio drops from 71.23% (65.25% for set-III), when the nodes are stationary to 63.52% (56.29% for set-III), when the nodes are moving at 20 m/s.
- SUS have high throughput but very low security whereas TUS have low throughput but very high security.
- In general packet delivery ratio decreases as Set-I to Set-III and security increase.

From the above results we conclude that SUS leads to a substantial improvement over DUS and TUS, from the point of view of throughput.

From throughput and energy point of view SUS has got the benefit. But DUS and TUS we can use the umpire to def the umpire role and take over alternative route if the route fails. Assume that node Ni is culprit in the Fig. 1. If Ni fails, the umpire node Ui and Ui+1 take up the linkage and pass on the message to destination.

4.2. Failure to deduct (False Negatives) Probability

False Negatives Probability can be defined as:
False Negatives Probability = number of malicious nodes left undetected/total number of malicious nodes

Table 3. False negatives of Set I to III for 30 % malicious nodes.

Mobility (M/s)	30 Percentage of Malicious nodes		
	SUS	DUS	TUS
0	0.1974	0.1852	0.1731
5	0.1594	0.1513	0.1471
10	0.0916	0.0749	0.0618
15	0.1091	0.0988	0.0871
20	0.1007	0.0918	0.0873

From Table 3 the following conclusions can be drawn:

- In general false negative probability decreases as the results from Set-I to Set-III.
- In the case of Set-I have high failure to deduct probability.

From the above results we conclude that SUS have high false negatives when compared with DUS and TUS.

4.3. False Accusation (False Positives) Probability

We find false positive probability increases with increased mobility speed. The values vary from 0 to 0.0924 and are similar to the patterns obtained for SCAN [2].

Table 4 False positives of Set I to III for 30 % malicious nodes.

Mobility (M/s)	30 Percentage of Malicious nodes		
	SUS	DUS	TUS
0	0	0	0
5	0.0136	0.0116	0.0091
10	0.0592	0.0471	0.0354
15	0.0764	0.0692	0.0511
20	0.0816	0.0748	0.0612

We present a comparison of False Positive Probability values from set-I to set-III in Table 4. It is seen that with set-I False Positive Probabilities slightly increase.

4.4. Communication Overhead

Communication overhead can be evaluated based on the number of transmissions of control messages like RREQ, RREP, RERR, M_ERROR, and M-Flag messages in the umpiring system. We present the communication overhead details in Table 5.

Table 5 Communication overhead of Set I to III for 30 % malicious nodes.

Mobility (M/s)	30 Percentage of Malicious nodes		
	SUS	DUS	TUS
0	0.0791	0.0827	0.0887
5	0.1032	0.1066	0.1098
10	0.1225	0.1302	0.1372
15	0.1456	0.1512	0.1569
20	0.1518	0.1592	0.1636

For Set-III, we find that the largest increase in communication overhead is 7 % corresponding to 30% malicious nodes and mobility 20m/s. The corresponding figure for Set-I is 0.1518.

5. Related Works

The Key Distribution Center (KDC) architecture is the main stream in wired network because KDC has so many merits: efficient key management, including key generation, storage, distribution and updating. The lack of Trusted Third Party (TTPs) key management scheme is a big problem in ad hoc network [2, 4, 6,18-21, 23].

Yong et al. [23] propose a novel cryptography for ad hoc network security, where they present a new digital signature algorithm for identity authentication and key agreement scheme. Their scheme has no central administrator. They have shown that their scheme can withstand man-in-middle and Byzantine mode conspiracy attacks.

Hubaux et al. [4] make a survey of threats and possible solutions for one security of ad hoc network. They extend the idea of public key infrastructure. Their system is similar to Pretty Good Policy (PGP) in the sense public key certificates are issued by the users. However they do not rely on certificate directories for the distribution of certificates. They present two algorithms in this connection.

All the above schemes only try to protect the system from the attacker, but not bother about quarantining attackers. The twin systems of *watchdog* and *pathrater* [21] not only detect the mischievous nodes but also prevent their further participation in the network. SCAN [3] also has similar action, but is more comprehensive, in the sense not only packet dropping but also other misbehaviors like giving wrong hop count are covered. Our self-USS is an extension of the above two works.

6. Conclusions

An umpiring system for security for mobile ad hoc network has been proposed. We have presented experimental results for all the 3 systems. We find that: Throughput with single umpire system is greater than DUS and TUS. From throughput and energy point of view SUS has got the benefit. But DUS and TUS we can use the umpire to def the umpire role and take over alternative route if the route fails. We envisage that our system can profitably be used in civilian situations where invariably nodes are lean and energy starved. Research work is in progress.

7. Acknowledgements

We express our thanks to Dr. P. Kanniappan, the Vice Chancellor, Prof. V. M. Periasamy, the Register and Prof. K.M.Mehata, the Head, Department of CSE & Dean, School of Computer and Information Science B.S.A.Crescent Engineering College Chennai, Tamilnadu, India for the encouraging environment provided.

References

[1] Bajaj L., Takai M., Ahuja R, Bagrodia R, and Gerla M., "Glomosim : A scalable network simulation environment. Technical Report 990027, pp. 1 – 12, 1999.

[2] Capkun S, Buttyan L and Hubaux J., "Self-organized public-key management for mobile ad hoc networks", IEEE Trans. Mobile Computing, vol. 2, No. 1, pp. 52-64, 2003.

[3] Hao Yang, James Shu, Xiaoqiao Meng and Songwu Lu, "SCAN: Self-Organized Network-Layer Security in Mobile ad hoc networks", IEEE Journals on selected areas in communications, vol. 24, No. 2, pp. 261 – 273, 2006.

[4] Hubaux J., Buttyan L, and Capkun S., "The quest for security in Mobile ad hoc networks", in Proc. ACM MobiHoc, pp. 146-155, 2001.

[5] IEEE 802.11. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, August, 1999.

[6] Kong J., Zerfos P, Luo H, Lu S, and Zhang L, "Providing robust and ubiquitous security support for MANET", Proc. IEEE ICNP, pp. 251-260, 2001.

[7] Kathirvel A. and Srinivasan R., "Performance Enhancement on demand routing protocol in mobile ad hoc networks", Proc. Second National Conference, PSG tech, pp. 169 – 174, 2006.

[8] Kathirvel A. and Srinivasan R., "A Study on Salvaging Route Reply for AODV Protocol in the Presence of Malicious Nodes", International Journal of Engineering and Technology, Volume 1, Number 2, pgno. 151 – 155, 2009. Singapore.

[9] Kathirvel A. and Srinivasan R., "Performance Analysis of Propagation Model using Wireless

Mobile Ad hoc Network Routing Protocols", International Journal of Wireless Communication, September 2009.

[10] Kathirvel A. and Srinivasan R., "Enhanced Self Umpiring System for Security using Salvaging Route Reply", International Journal of Computer Theory and Engineering, Volume 2, Number 1, 2010. Singapore.

[11] Kathirvel A. and Srinivasan R., "Self_USS: A Self Umpiring System for Security in Mobile Ad-Hoc Network", International Journal of Engineering and Technology. Singapore.

[12] Kathirvel A. and Srinivasan R.,"Single Umpiring System for Security of Mobile Ad Hoc Networks", Journal of Advances in Wireless Mobile Comminication, Volume 2 Number 2, pp 141-152, 2009.

[13] Kathirvel A. and Srinivasan R., "Triple Umpiring System for Security of Mobile Ad Hoc Networks", International Journal of Engineering and Information technology, Vol 1, No 2, pp 95 – 100, 2009.

[14] Kathirvel A. and Srinivasan R., "Global Mobile Information System Simulator in Fedora Linux", ACM Computer Commucation Review, 2009. ccr.sigcomm.org/online/files/new.pdf

[15] Kathirvel A. and Srinivasan R., "Reactive Route Recovery for Link Failure in MANET" , Proc. of the IEEE National Conference on Information and Communication Convergence (IEEE ICC – 2006), pp. 42 – 49, Chennai, India.

[16] Kathirvel A. and Srinivasan R., "Enhanced Triple Umpiring System for Security and Performance Improvement of Wireless MANETs", International Journal of Communication Networks and Information Security, Vol 2, No. 2.

[17] Kathirvel A. and Srinivasan R., "ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks", ACM Computer Communication Journal (Communicated)

[18] Lei Feng-Yu, Cui Guo-Hua, and Liao Xiao-Ding, "Ad hoc Networks security mechanism based on CPK", in proc. IEEE ICCISW, pp. 522 – 525, 2007.

[19] Marianne A. Azer, Sherif M. El-Kassas, and Magdy S. El-Soudani, "Certification and revocation schemes in ad hoc networks survey and challenges, Proc. IEEE ICSNC 2007.

[20] Michael Hauspie, and Isabelle Simplot-Ryl, "Enhancing nodes cooperation in ad hoc networks", Proc. IEEE , pp. 130 – 137, 2007.

[21] Sergio Marti, Giuli T.J., Kevin Lai and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Proc. ACM MobiCom, pp-255-265, 2000.

[22] Scalable Networks Technologies: QualNet simulator version 4.5. http://www.scalable-networks.com

[23] Pi Jian Yong, Liu Xin Song, Wu Ai, Liu Dan, "A Novel Cryptography for Ad Hoc Network Security", in Proc. IEEE, pp. 1448 -1451, 2006.

Ayyaswamy Kathirvel born in 1976 in Erode, Tamilnadu, India, received his B.E. degree from the University of Madras, Chennai, in 1998 and M.E. degree from the same University in 2002. He is currently with B.S.A. Crescent Engineering College in the Department of computer science and Engineering and pursing Ph.D. degree with the Anna University, Chennai, India. He is a member of the ISTE. His research interests are protocol development for wireless ad hoc networks, security in ad hoc networks.

Rengaramanujam Srinivasan born in 1940 in Alwartirunagari, Tamilnadu, India, received B.E. degree from the University of Madras, Chennai, India in 1962, M.E. degree from the Indian Institute of Science, Bangalore, India in 1964 and Ph.D. degree from the Indian Institute of Technology, Kharagpur, India in 1971. He is a member of the ISTE and a Fellow of Institution of Engineers, India. He has over 40 years of experience in teaching and research. He is presently working as a Professor of Computer Science and Engineering at BSA Crescent Engineering College, Chennai, India and is supervising doctoral projects in the areas of data mining, wireless networks, Grid Computing, Information Retrieval and Software Engineering.