Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks

Latha Tamilselvan[↑] **and** **Dr. V. Sankaranarayanan**[↑↑]

BSA Crescent Engineering College, Vandalur, Chennai, Tamilnadu, India

Abstract:
An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are capable of communicating with each other without the use of a network infrastructure or any centralized administration. Due to Open medium, dynamic topology, Distributed Cooperation, Constrained Capabilities ad hoc networks are vulnerable to many types of security attacks. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render the traditional solutions inapplicable. In particular, in mobile ad hoc network (MANET), any node may compromise the routing protocol functionality by disrupting the route discovery process. The solution proposed Secure Ad hoc On-Demand Distance Vector (SAODV) is an extension of the AODV routing protocol that can be used to prevent Impersonation attack. In this attack, the attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. The methodologies used to achieve these requirements are Hash chains and Digital Signatures.

Keywords:
Security, Ad hoc Networks, Routing Protocols, Hash Chains, Secure AODV, Digital Signature.

1. Introduction

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantage of this is their limited bandwidth, memory, processing capabilities, open medium and less secure compared to wired devices[2]. Two basic system models are Fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET).An ad hoc network is a collection of nodes that do not need rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [2]. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology [3].

Proactive routing protocols: In proactive protocols, the routes are discovered before usage avoiding the latency incurred in finding the route. These protocols require the nodes to maintain routing and network topology information through one or more tables. Any change in the network needs to be reflected in these tables by propagating the changes throughout the network. Examples of this class include DSDV, WRP.

Reactive routing protocols: Reactive protocols try to conserve the precious battery power of the nodes by discovering routes only when it is required. Only when there is a packet to be transferred, the route discovery protocol is initiated by the source and the route is found. Because of this nature, this class of routing protocols is also called as "Dynamic routing protocols". Examples of this class include DSR, AODV and ABR.

Hybrid protocols make use of both reactive and proactive approaches. They typically offer means to switch dynamically between the reactive and proactive parts of the protocol. Examples of this class include TORA and ZRP.

Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their Limited Bandwidth, Dynamic Topology, No Centralized Control, Limited Battery Power [1][4]. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. The different attacks can be classified based on their nature as either passive or active attacks [5]. A passive attack attempts to illegitimately acquire valuable information by listening to the traffic without disrupting the operation of the routing protocol. Hence detection of passive attacks is highly difficult. On the other hand, active attacks alter the flow of data either by inserting false packets or by modifying the packet contents. Active attacks can further be classified into Internal and External attacks. Internal attacks are caused by a node that belongs to the same network as the victim, whereas external attacks are caused by nodes that do not belong to that network.

1.1. The AODV protocol:

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [6][12][13]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination.

Manuscript received March 5, 2007
Manuscript revised March 25, 2007

Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes.

Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Impersonation attack'.

2. Impersonation Attack

Impersonation attacks [7] are also called *spoofing* attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion. A compromised node may also have access to encryption keys and authentification information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information.

3. Solution: Secure AODV (SAODV)

Two mechanisms are used to secure the AODV messages:[8] [9][14]

i. Hash chains to secure mutable fields of the messages (hop count information is the only mutable field).

ii. Digital signatures to authenticate the non-mutable fields of the messages.

For the non-mutable information, authentication is performing in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information.

3.1. Working of SAODV hash chains

SAODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every node that receives the message (either an intermediate node or the final destination) to verify that the hop count has not been decremented by an attacker. This prevents any Hop Count Field change. That is when forwarding a RREQ generated by *S* to discover a route to *D*, reduce the hop count field to increase the chances of being in the route path between *S* and *D* so it can analyze the communication between them. A variant of this is to increment the destination sequence number to make the other nodes believe that this is a 'fresher' route.

Applying a one-way hash function repeatedly to a seed forms a hash chain. Every time a node originates a RREQ or a RREP message, it performs the following operations:

Generates a random number (Seed). Sets the Max Hop Count field to the Time-To-Live value (from the IP header).

Max Hop Count = Time-To-Live

Sets the Hash field to the seed value.

Hash = Seed

Sets the Hash Function field to the identifier of the hash function that it is going to use.

Hash Function = h

The details of the hash function are given in the table 1. As for the simulation purpose the following two hash algorithm are implemented.

Value	Hash Function
0	Reserved
1	RIPEMD-5
2	SHA

Table 1: Hash Functions

Calculates Top Hash by hashing seed Max Hop Count times.

$$\text{Top Hash} = h^{(\text{Max Hop Count} - \text{Hop Count})}(\text{Hash})$$

Where
– h is a hash function.
– $h^i(x)$ is the result of applying the function h to x i times.

In addition, every time a node receives a RREQ or a RREP message, it performs the following operations in order to verify the hop count:

Applies the hash function h Maximum Hop Count minus Hop Count times to the value in the Hash field, and verifies that the resultant value is equal to the value contained in the Top Hash field.

$$\text{Top Hash} = h^{(\text{Max Hop Count} - \text{Hop Count})}(\text{Hash})$$

Before re-broadcasting a RREQ or forwarding a RREP, a node applies the hash function to the Hash value in the Signature Extension to account for the new hop.

$$\text{Hash} = h(\text{Hash})$$

The Hash Function field indicates which hash function has to be used to compute the hash. Trying to use a different hash function will just create a wrong hash without giving any advantage to a malicious node. Hash Function, Max Hop Count, Top Hash, and Hash fields are transmitted with the AODV message, in the Extension. All of them except the Hash fields are signed to protect its integrity.

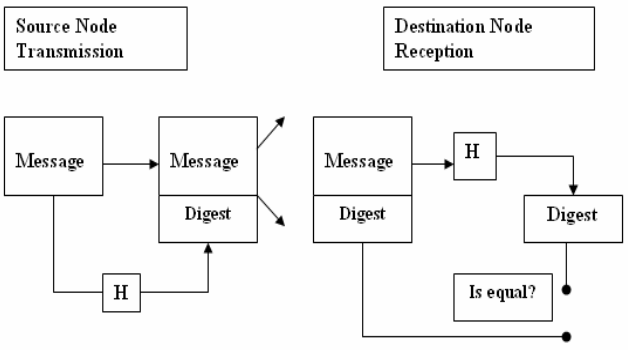

Figure 1: Hash Chain Creation

The functionality of the hash chain between source and destination node is illustrated in figure 1, where H is the hash function used.

3.2. Working of SAODV digital signatures

Digital signatures are used to protect the integrity of the non-mutable data in RREQ and RREP messages. That means that they sign everything but the Hop Count of the AODV message and the Hash from the SAODV extension. The main problem in applying digital signatures is that AODV allows intermediate nodes to reply RREQ messages if they have a 'fresh enough' route to the destination. While this makes the protocol more efficient it also makes it more complicated to secure. The problem is that a RREP message generated by an intermediate node should be able to sign it on behalf of the final destination. And in addition, it is possible that the route stored in the intermediate node would be created as a reverse route after receiving a RREQ message (i.e. it does not have the signature for the RREP).

The solution used here is an intermediate node cannot reply to a RREQ message because it cannot properly sign its RREP message, it just behaves as if it didn't have the route and forwards the RREQ message.

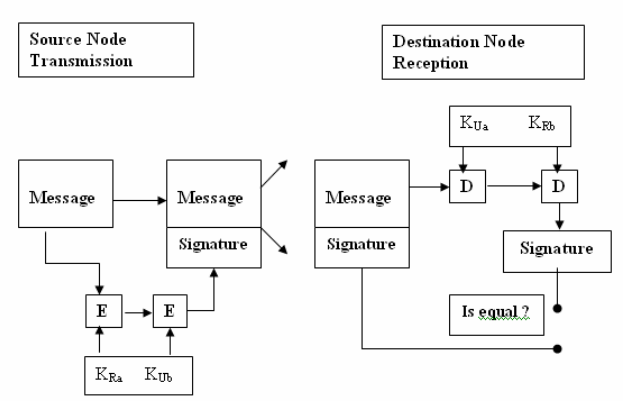

Figure 2: Digital Signature Creation

K_{Ra} -Sender's Private Key K_{Ua} -Sender's Public Key
K_{Ub} - Receivers Public Key K_{Rb}- Receiver's Private Key
E -Encryption D-Decryption

When a node receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. Only if the signature is verified, it will store the route. When a RREQ is received by the destination itself, it will reply with a RREP only if it fulfills the AODV's requirements to do so. This RREP will be sent with a RREP Signature Extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will

store the route with the signature of the RREP. Using digital signatures we can prevent attacks like,

i. Impersonate a Source node *S* by forging a RREQ with its address as the originator address.
ii. Impersonate a Destination node *D* by forging a RREP with its address as a destination address.

The mechanism of creating the signature and verifying it is illustrated in the figure 2.

4. Simulation and Analysis

In this section, the simulation study and analysis of SAODV protocol is discussed. The simulation is done using GloMoSim [10][15] to analysis the performance of the networks by varying the nodes mobility in the networks. The metrics used to evaluate the performance is given below.

Packet Delivery Fraction: This is the fraction of the data packets generated by the CBR sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes.

Throughput: This is the ratio of total number of bytes transferred per second

Average Path Length: This is the average length of the paths discovered by the protocol. It was calculated by averaging the number of hops taken by each data packet to reach the destination.

Average End-to-End Delay of Data Packets: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

4.1. Simulation Profile

The simulation profile is illustrated in the table 2

Property	Value
Nodes	20
Adversaries	10%,20%
Measurements	10 random runs in begin setting 10 random runs in malicious setting
Security Binding	Single destination per source
Simulation time	120 Sec
Mobility	Random way point speed 2, 10, 20, 30, 50 m/s
Load	5,10,20 CBR Sources, Data pay load 512 B 5 CBR Sources in Malicious settings
Coverage Area	670m by 670m

Table 2: Simulation Profile

4.2. Simulation Results

Figure 3 to 6 shows the observed results for 20 node network without any malicious behavior. As shown in Figure 3. the packet delivery fraction obtained using SAODV is above 95% in all scenarios and almost identical to that when using a pure AODV. This suggests that SAODV is highly effective in discovering and maintaining routes for delivery of data packets, even with relatively high node mobility.

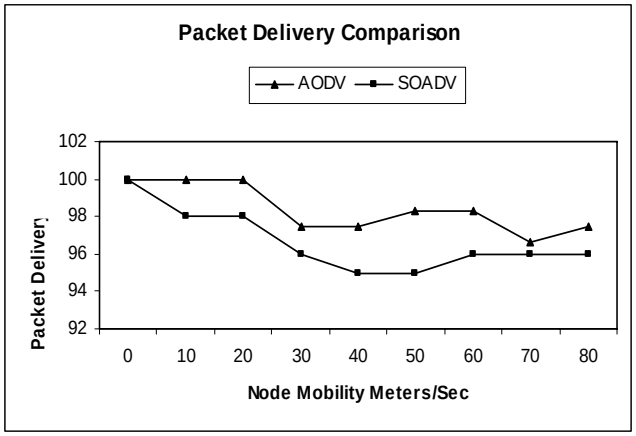

Figure 3: Packet Delivery

Figure 4 shows the throughput of the simulation. It's based on number of bytes received in the destination. As the mobility of the node increases, in SAODV the throughput slightly degrades but after that it gets stabilized and compared to AODV throughput is increased.

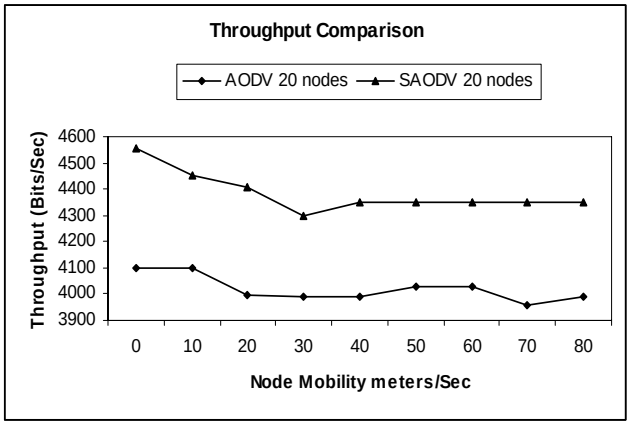

Figure 4: Throughput

Figure 5 shows the results of the average path length. Traditionally, the shortest path to a destination (in terms of number of hops) is considered to be the best routing path. AODV explicitly seeks shortest path using the hop count field in the route request/reply packets. SAODV, on the

other hand, assumes that the first route discovery packet to reach the destination does not traveled via malicious nodes; it chooses the safest path than shortest. Due to this elimination of malicious nodes in the way, the average path length is bit higher than the pure AODV.

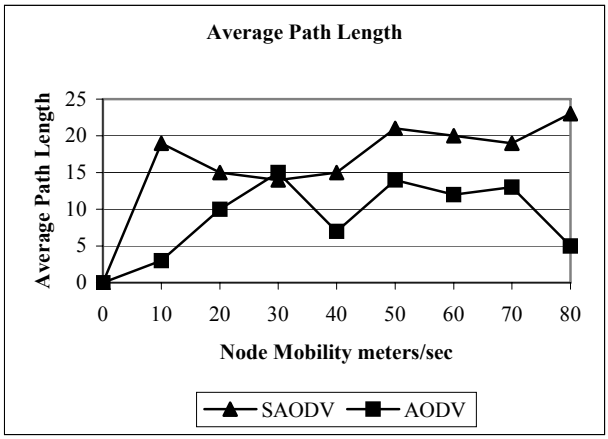

Figure 5: Average Path Length

Figure 6 shows the average end-to-end delay. This is more compared to AODV. While processing SAODV routing control packets, each node has to verity the hop count and check weather it is correct else report it to the black list, if the nodes is the destination then it has to get the public key of the source node and create the signature and compare it with the packet.

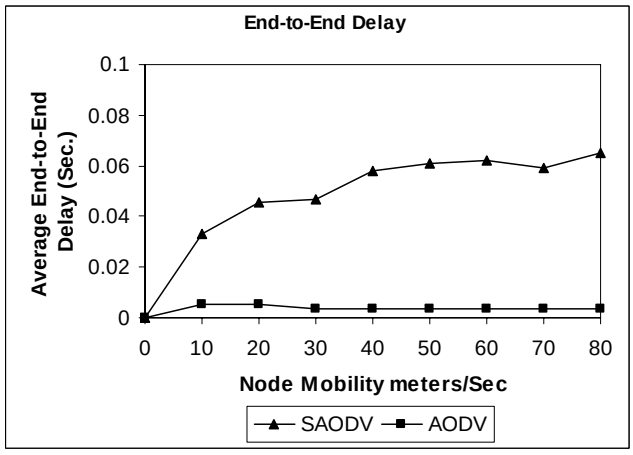

Figure 6: End-to-End Delay

So this hash and signature mechanism adds some delay in the network, so the average end to end delay is also slightly increased.

4.3. Effect of Malicious Node Behavior

The experiments described in the previous section done without any malicious node in the network and the performance is evaluated. Additional experiments to determine the effect of malicious node behavior on the protocol are done. The same simulation setup is used but with the effect of 10%, 20% of malicious node behavior. The malicious nodes are chosen in random among the number of nodes and the behavior is also chosen in random, where the node can increment the hop-count or decrement hop-count. In addition to that a masquerading node can modify the source or destination address. This kind of malicious behavior can be detected using the hash function and the signature comes with the routing packets. When a node detects the above kind of behavior it adds the last address where it receives the packets in to the black list and drop the packet. The source node after waiting a period of request timeout and start re-transmitting the packets. This action tries to avoid the data packet to be transferred throw the malicious nodes. The figure 7 shows the average end-to-end delay of networks after inserting 10% and 20% of malicious nodes in the networks respectively.

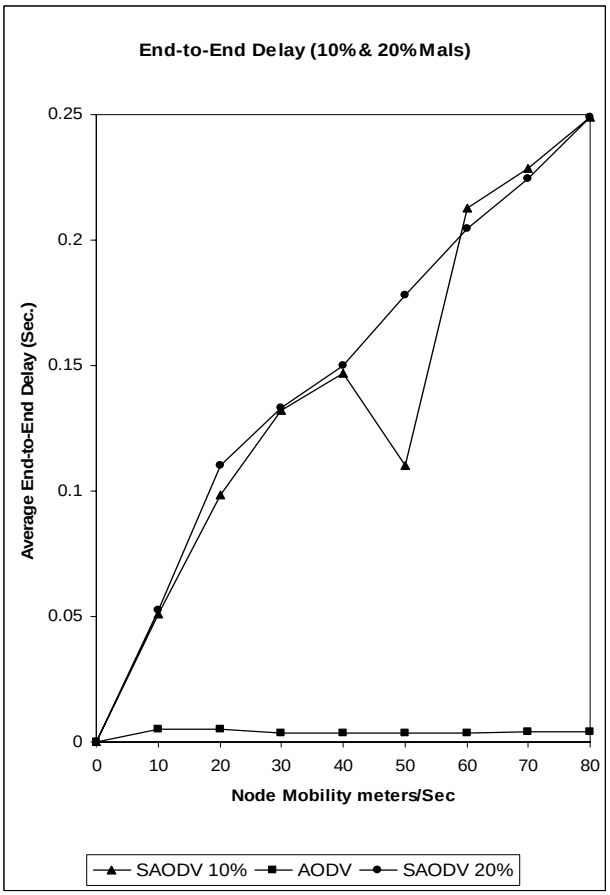

Figure 7: 10% & 20 % of Malicious node

The overhead is in terms of delay time of the order of 0.05 sec to 0.25 sec only compare to AODV. But this small overhead is definitely tolerable at cost of security. The increase in this delay with mobility is a visual phenomenon

in mobile network. The variation with 10% and 20% malicious is not much appreciable.

5. Conclusion and Future Work

In this paper we propose a strategy to counter the Impersonation attacks prevalent in Mobile Ad Hoc Networks. The solution is simulated using the Global Mobile Simulator and is found to achieve the required security with minimal additional delay and overhead. In addition to authenticate the non mutable fields using digital signature the eligibility of intermediate node is blocked. Our future work intends to be in the direction of simulating the protocol in a larger network and try to minimize the overhead and delay by using the Intermediate node eligibility.

References

[1] Yi-Chun Hu, Adrian Perrig, David B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe 2003, September 19, 2003, San Diego, California, USA.

[2] H. Deng, W. Li, and Dharma P. Agrawal, "Routing Security in Ad Hoc Networks, "IEEE Communications Magazine, Special Topics on Secuity in Telecommunication Networks, October 2002.

[3] V. Karpijoki, "Security in Ad Hoc Networks", http://www.hut.fi/~vkarpijo/netsec00/netsec00_manet_sec.ps

[4] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[6] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das, "Mobile Ad Hoc Networking Working Group", Internet Draft, 17 February 2003.

[7] Adam Burg, "Ad hoc network specific attacks ", Seminar on Ad hoc networking: concepts, applications, and Security, Technische Universität München, 2003.

[8] Manel Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", WiSe'02, September 28, 2002. See also http://doi.acm.org/10.1145/570681.570682.

[9] Manel Guerrero Zapata. (2001) 'Secure ad hoc on-demand distance vector routing (SAODV)' –IETF MANET List.

[10] R. Bagrodia, R. Meyerrl (1997), 'PARSEC: A Parallel Simulation Environment for Complex System', UCLA technical report.

[11] Panagiotis Papadimitratos and Zygmunt J. Haas (2002), 'Secure Routing for Mobile Ad hoc Networks', In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31.

[12] C. E. Perkins and E. M. Royer (1999), 'Ad-Hoc On-Demand Distance Vector Routing', in The Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA.

[13] E. M. Royer and C.-K. Toh (1999). 'A review of current routing protocols for ad hoc mobile wireless networks'. IEEE Personal Communications, pages 46-55.

[14] R L Rivest, A Shamir, L Adleman (1978), 'On Digital Signatures and Public Key Cryptosystems', Communications of the ACM, vol 21 no 2, pp120-126.

[15] Xiang Seng, Rajive Bagrodia (1997).'GloMoSim: A Library for Parallel Simulation of Large-scale Wireless Networks, Department of Computer Science.

Latha Tamilselvan received her B.E. in Electronics & Communication Engineering from Bharathidasan University in 1990, M.E. in Communication Systems from Regional Engineering College, Bharathidasan University, Trichy in 1995. She is doing Ph.D in Computer Science & Engineering in Anna University, Chennai. She has a total teaching experience of 12 years and 2 years industrial experience. She is currently working as an Assistant Professor in at B.S.A.Crescent Engineering College, Chennai, India.

Venkadachalam Sankaranarayanan was born in India in 1942. He received his B.E. in Electical Engineering from Annamalai University in 1966, M.Sc. (Engg) in High Voltage from college of Engineering, Guindy, Chennai and Ph.D. in computer applications from IIT(Madras) in 1979. He worked as professor in Anna University for about 3 decades. He was then deputed as Director Tamil Vitual University, from 2004 - 2006 Chennai. He is currently Director at B.S.A.Crescent Engineering College, Chennai, India.