Preventing Black hole Attack from Routing Path in MANETs by Secret Key and Hashing

Abdulssalam A.Alafi
M.Tech, Dept of ECE, SIET, SHUATS, India.

Aditi Agrawal
Assistant Prof, Dept Of ECE, SIET, SHUATS, India.

A.K Jaiswal
Prof & Head Dept. of ECE, SIET, SHUATS, India.

Rajeev Paulus
Assistant Prof, Dept Of ECE, SIET, SHUATS, India.

Abstract – MANETs system is made out of remote portable device that communicates by transferring on wireless medium. This system is portrayed by absence of infrastructure, without facilitator and central assets. Communication is conceivable by devices in a system that are helpful; however it is not generally valid in disseminated compelled asset condition. Hacker can play out the malicious exercises by not following directing convention of network layer protocols, one such attack is black hole attack. In black hole attack device control the routing messages and pull in the correspondence data towards it and after that drop the data. Earlier works identifies and prevent black hole attack by observing the nodes in a network, which is not practical arrangement in hostile environment. The proposed technique mitigates Black hole Attack from routing path in MANETs by Secret Key and Hashing. Analysis of our results demonstrates that our proposed technique precisely remove the black hole attack and extend the performance of network.

Index Terms – MANETs, NS-2 routing, black hole attack, secret key, hashing.

1. INTRODUCTION

Ad-hoc wireless networks are comparatively new paradigm in multi-hop wireless networking that is increasingly becoming popular and will become an essential part of the computing environment, consisted of infrastructure-less mobile networks.(MANET) is an infrastructure-less varied-hop network where each node communicates with other nodes directly or in directly through intermediate nodes [2]. The reason for growth of ad-hoc network goes to its self-organizing and self-configuring properties [6]. All nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes [3].

MANETs are infrastructure-less, self-arranging, rapidly changing wireless networks, they are extremely equal for applications involving particular outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations, mine site operations, urgent business meetings and robot data acquisition. In general, routes in the amidst nodes in an ad hoc network may include multiple hops and, hence, it is appropriate for such networks are called "multi-hop wireless ad hoc networks. Figure 1 shows an example mobile ad hoc network and its communication topology.

Ad hoc wireless networks inherit the imitative problems of wireless communications such as bandwidth configure, power control, and transmission quality reinforcement, while, in addendum their mobility, multi-hop nature, and there is no fixed infrastructure make a number of complexities and design constraints that are new to mobile ad hoc networks[1,5].

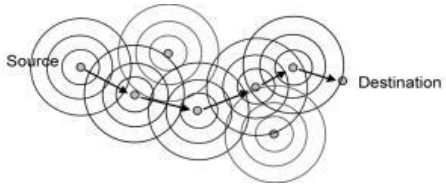

Figure 1.1. Mobile Ad Hoc Networks

The different paradigms of concern for such network are Broadcast nature of the wireless medium, Hidden terminal problem, Packet losses due to transmission errors, Mobility-induced route changes, Mobility-induced packet losses, Battery constraints, potentially frequent network partitions, Ease of snooping on wireless transmissions (security hazard), Quality of Service.

Mobile wireless networks are more accessible to physical and information security threats than fixed-wired networks. The using of open, share broadcasting wireless channels means

nodes with inadequate physical preservation are vulnerable to security menace in addendum because a mobile ad hoc network is a assigned infrastructure-less network, it mainly count on demarcation security solution of every mobile node, as security centralize control is hard to implement[9].

The objective of paper is to provide security to MANETs environment by mitigating attacks on AODV (ad hoc on distance demand vector) routing protocol of MANETs, and to present its design and enforcements in wireless ad hoc networks. Through real simulation in network simulative-2 ns2, we identify important design issues and propose an approach, to reduce the loss of information and to avoid declarmining trust nodes by eliminating the black hole nodes by the PKI. The paper is formulated as follows. Section II gives a background of AODV and black hole attack. In section III we have discussed some other works related to this work. Section IV gives the review stage and section V discuses our proposed (PKI) based technique for black hole detection.

2. BACK GROUND

A. Ad hoc on demand distance vector routing protocol(AODV) [1,5] is a well-known and most widely used protocol in MANETs It is reaction(on demand) , where routing information is traded only when elucidation need to take place between nodes and only as long as the communication occurs this information is updated. AODV it uses three main messages they are RREQ (Route Request), and RERR (Route Error). RREQ packet is broadcasted via exporter in order to find the path, nodes in the network, each node which receive RREQ pack keep the transmitter up to finds a new route to the destination. On receiving RREQ, if the node is destination or if the node has fresh route to destination, it sends RREP packet. Hop the number of any node increases by- 1 on delivery. The RREQ message and route entree is updated with new information by middle nodes upon receipt of RREP message. The sequence number for nodes will be increases each time, new RREQ, RREP, RERR messages have sent. The detection process for route is begin whenever a node need to communicate with others [4].

AODV Route Discovery

To establish a route from source S to D, RREQ packet is broadcasted from S. On receiving RREQ packet intermediate node.

(i) RREP packet is sent back, when the destination node or when has a fresh enough node to destination.

(ii) Routing table is updated and RREQ is again broadcasted.

RREP is sent back to the source when RREQ is taken via the destination. The nodes in the source receives RREP (route reply) message during the middle nodes that was update routing tables. RREP is acceptable by source if:

(i) The destination sequence number of this node is bigger than the one in the table routing.

(ii) Destination sequence numbers are equalized and the hop count is lesser with the one in routing table.

B. Black Hole Attack is a sort of negation of service attack. When a malicious node can attract all packets by false pretences a fresh route until destination, then soak up them without for-warding them to the destination and seggast to as a node dropping every packet and sending counterfeit routing packets to route packets over itself. The sink node (the destination) to attract additional traffic to the malicious node and then drops them [1]. Also implemented on the AODV protocol. Also find the malicious node. Based on the trust value of node& define which path is most suitable for routing the packet and untrusted node can easily remove or ignored [3]. Provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem and the more detection method should be initiated to solve the black hole attack. [6] The traffic involving in a destination node, its Dst Seq may change. As the last in the black holeat-tack, the Specifically investigate the effects of the attack when the number of connections to the number of connection from the destination are changed. [8]

3. RELATED WORK

Surana k.a, et. al [1] proposed a watch mechanism which first performs detection and them gives a new route to the node. Therefore elimination of route though malicious node is done in the route – determination phase of AODV. Lathatamilselvan& Dr. v sankaranarayanan [2] presented a feasible solution for mitigating, making use of fidelity tables and assigning fidelity levels to the participating nodes. Simulation was perfumed using global mobile simulator & Results showed that percentage of packets & received it through the designed system is better than that in AODV in presence & they suggested future works may be concentrated on ways to reduce the delay in the network. Nirali modi & Vinit Kumar gupta [3] proposed a feasible solution for Black hole attack that can be implemented on the AODV protocol. The proposed method is that node defines which path is most suitable for routing the packet and Entrusted node can easily remove or ignored. Future work, is intended & to develop simulation to analyze the Performance of proposed solution based on the security parameters like packet overhead, memory usage, and mobility. Ei ei khin and Thandar Phyu[4] implemented black hole attack based on AODV protocol and analyzed the effect of malicious nodes on performance of AODV using NS-2.34 simulator. The result are based on evaluating the degradation in AODV performance based on metrics like average end to end delay, routing overhead. The result were analyzed with variable node mobility pause time and number of transaction. Authors' suggested future work as simulating and analyzing black hole attach in other routing

protocols. Madhuri Gupta, Krishna Kumar Joshi[5] proposed on algorithm to identify gray hole attacker node & simulation on NS2.In the proposed solution the some compares the (DSN) of the first entry from routing table with the threshold value(average of DSN of all replying nodes)this node is identified as attacker it the DSN is much greater than threshold value. Heta Changela, Amit Lathigara[6] studied effect of black hole attack on AODV and proposed scheme for finding single malicious node the source node after receiving RREQ-ASK compares destination sequence number (DSN) with (SSN). If the DSN is greater than SSN then the node is discarded. Lalita Prajapati, Anurag Singh Tomar [7] Presented a new technique to detect black hol attack by detection in three steps. The first is cheling in the packet delivery ration at the distention. And if it is found to be cars than the threshold value a check is perfumed. The second stab is that source node checks forward packets ration of every node that gives a rout reply and detects malicious node it does not send forward message. The third step is identifying suspect by sending a dummy packet for new session creation with prime products of two node and dividing prime number suspect node to find whether genuine or n Satoshi Kurosawa, et.al [8]proposed a dynamic training method to detect black hole ack in AODV and simulation are performed in NS2 the DSN tend to rise when number of connections increases otherwise when there are few connections it rises monotonically but when attack takes place the sequence number is increased largely without conceding the environment .Neeraj Saini, Lalit Garg[10] Packet Delivery ratio is more in the modified AODV than the AODV with Black hole .End to End delay is more in the modified AODV than the AODV with blackhole. Also the effect on modified AODV by the malicious node is less as compare to AODV. But still the detection of Black hole in ad hoc is considered as a challenging task. Ankita Joshi et al. [15] proposed a three dimensional check algorithm which performs security checks on the basis of three parameters that are acknowledgement received before time out for packets send, checking residual energy of nodes and finally verifying with digital signature. The proposed approach is tested for multi hope hybrid Ad-hoc networks.

4. REVIEW STAGE

Existing work secure knowledge algorithm SKA [13] is designed to mitigate the black hole attack from routing path. This algorithm is based on monitoring approach. Any node in a network promiscuously monitors the neighbor node and maintains the table known as knowledge table. This algorithm maintains the threshold value for packet dropping operation. If node drops more than threshold value, then algorithm checks the packet dropping reasons based on node resources such as energy, buffer and TTL value of packet. If the packet is not dropped by constraint resources than algorithm confirm the detected node as black hole node and prevent from future communication. It is rely on intermediate nodes knowledge table. However intermediate node not always sends the true replay to source. Another limitation is extra over head of control packets. This algorithm prevent not in initial part. Moreover that algorithm is AODV and maintains the knowledge table, monitor by promiscuous mode and if any node drops the packets more than threshold value, then it checks the packet drop reason and if packet drop only due to malicious activities then only it conforms as malicious node,[13]

Trust value calculation Every node in a network keeps a trust value that represents the trustiness of each of its neighboring nodes. This trust value gets updated based on the ongoing data transmission with its neighboring nodes. Trust value: Trust value of a neighbor is calculated as a ratio of number of packets dropped to the number of packets to be forwarded by that neighboring node. Trust value is calculated using a simple formula.

$T = 1-D/F$

Where

T = Trust value

D = packets dropped by a node, which are actually to be forwarded.

F = Number of Packets forwarded to that node, which are actually to be further forwarded.

Trust value will be on a range of 0 to 1.

Distinguishing nodes based on trust value. Higher the range value, more trust worthy the node is. Based on this, all nodes below the range value of 0.3 are considered to be malicious the experience a node having with the other one. **Routing Mechanism,** When any node send messages to last node, it sends the RREQ to all the neighboring nodes. The ROUTE REPLY obtained from its neighbor is sorted by trust ratings. RREP (route reply) messages from non-trusted nodes are omitted and thus the routing path avoids the malicious nodes and establishes a secure channel of trustworthy nodes.

Black hole avoidance. Once a node has been identified as malicious, all RREP (route reply) packets from non trusted nodes are omitted and thus route will be selected only through trusted nodes and data packets will be transmitted only to these nodes. At the same time, it removes all the routing paths containing the malicious nodes from the route table of that particular node and its precursors. Thus black hole nodes are completely removed from existing routes and prevented from establishing route in future.

Reception of confirmation packet. The packet contains malicious node id, a node checks whether the packet is from a trusted source. If the packet is from a trusted source, then the node updates the range value of node id mentioned in that

packet to 0.0 so that it will not establish route through that malicious node in future by dropping the RREP packets from the malicious node. And it also removes all the routing paths that contain the malicious node from the route table.

Problems in existing work. The existing system relies on trust values. Packet drop can be due to many reasons i.e, packet properties such as destination address, time to live (TTL) etc, and node properties such as energy of the node. Since this system does not consider the other packet drop reasons, it may happen that packets are dropped because of above mentioned reasons which in turn affect the trust value calculated on a node. Due to which the trust vale of a node may be lowered and thus it results in trusted node being taken as a malicious or black hole node that causes avoiding a trustable node in the data transmission route. We can summaries the limitations of existing work as follows.

1. Based on distance vector :- packet may drop due to congestion
2. Relay on intermediate node :- one cannot trust on intermediate node in distributed environment
3. Extra overhed :- by maintain table, reasons for checking packet dropping
4. Malicious node not detected in initial stage
5. Could not mitigate false misbehaving node

5. PROPOSED WORK

Every node in a network receives a PKI from trusted third party by securely using RSA algorithm. (Rivets-Shamir-Adleman) which is a cryptosystem for public key encryption, using for securing sensitive data & Black hole attack initiates the malicious activity by giving false route reply message. In order to get integrity of route reply message, destination node needs to reply the route reply by using proposed algorithm.

Algorithm

1. Destination get the RREQ packets from different node
2. Node selects a best route based on metric less hop count, and prepare the route reply packet
3. Node adds the route reply packet with its secret key got from the PKI(public key infrastructure)
   (RREP) XOR (Secrete Key)
4. Node calculate the message digest using the digest algorithm according to PKI instruction (In our method it is MD5) (message digest 5)
   H(RREP XOR Secrete Key)
5. Node append the calculated digest information with original route replay packet
6. RREP unicast towards the source node

Source node remove the H(RREP XOR Secrete Key) from the RREP packet and adds the secrete key got from the PKI and perform the following task (RREP) XOR (Secrete Key) H(RREP XOR Secrete Key)

Destination ID
Destination Sequence Number
Origination ID
Destination Sequence Number
Hop count
H(RREP XOR Secrete Key)

Figure1.2. RREP Packet format of proposed protocol

And compare the calculated information with obtained information if both matches, then source node conclude that the information did not tamper during the communication. Table 1 shows the comparison between the proposed scheme and SKA.

Table 1: Comparison between proposed &existing scheme

Existing System	Proposed System
Secure Knowledge Algorithm(SKA)	Proposed Algorithm
Based on monitoring.	Based on message digest.
Remove the black hole attack in dropping information phase, which is the second phase of black hole attack.	Removes the black hole attack in attracting information phase, which is the initial phase of black hole attack.
Overhead is more.	Less overhead when compared to existing system.
Need to maintain knowledge table.	No need to maintain knowledge table.
Packet dropping nodes are not always black hole nodes.	Here, black holes are removed at initial phase so, no packet loss or packet drop will occur.

6. RESULT AND DISCUSSION

For comparing the results the simulations are performed in Network Simulator -2.Refer to Table 2 which shows the simulation parameters taken.

Table 2: Simulation parameters

PARAMETERS	VALUES
Nodes	10-40
Channel	Wireless channel
MAC	802.11
Routing	AODV, Proposed(SAODV)
Querying	Priority queue

Simulation time	0.9 sec
Network area	1000x1000 meters
Packet size	512 kb
Traffic	CBR(constant bit rate)

Results are observed by varying no. of nodes i.e 10, 20, 30 nodes with the presence of malacious nodes .The x-axis represents the simulation time and the y-axis represents the throughput measured in terms of Mbps.

Figure 1.3, figure 1.4 and figure 1.5 shows the graphical performance of proposed approach for varying nodes. Figure 2.1 shows the comparison of proposed work with SKA AODV. The throughput of the proposed PKI AODV is more when compared to the Black hole AODV and SKA AODV, referring to figure 2.4 ,the packet delivery ratio of the proposed PKI AODV is more when compared to the SKA AODV, with more overhead..

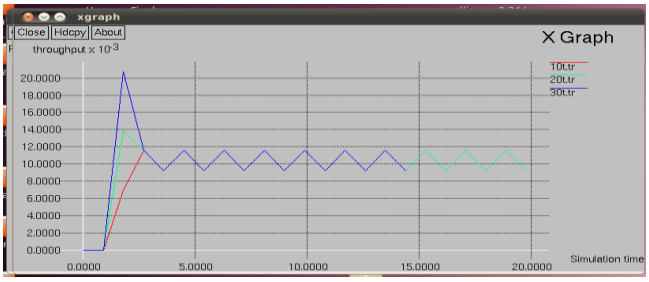

Figure 1.3. Throughput comparison of number of node with malicious node

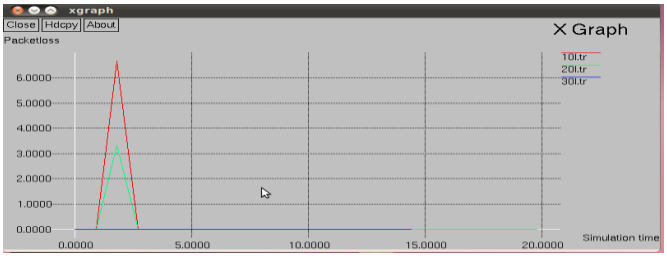

Figure 1.4. Pack loss comparison of number of node with malicious node

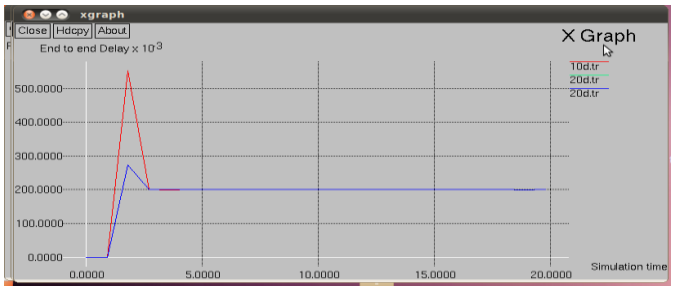

Figure 1.5. End to End Delay comparison of number of node with malicious node

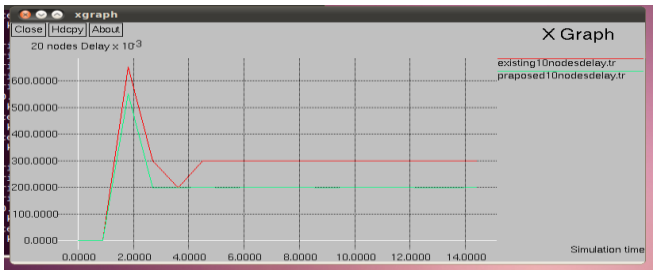

Figure 2.2. Comparison of delay of number of node (20) with malicious node proposed protocol

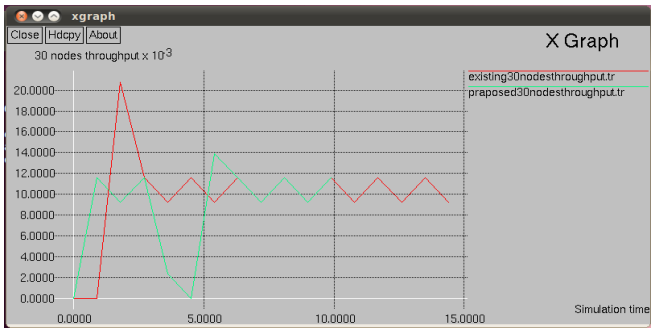

Figure 2.3. Comparison of throughput of number of node (30) with malicious node proposed protocol

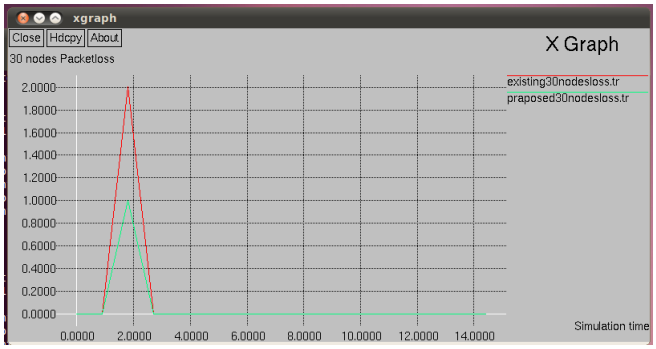

Figure 2.4. Comparison of packetloss of number of node (30) with malicious node proposed protocol

However results clearly indicate that our proposed work performed well in comparison with existing work. Thus we compare the proposed work and existing work. Further we can observe that the throughput of proposed work is more in initial stage of simulation time as it removes the malicious node in initial stage, where existing work removes the node after detecting and conforming mode. Both protocols performed identical afterwards as both will detect and remove the black hole node. Delay of proposed work is less as it contain less overhead, where as existing work delay is high as it contain extra overhead of control packets, maintain the table and conforming mode. In Packet loss comparison there is not much difference as both protocol is based on distance vector routing algorithms.

7. CONCLUSION

In this paper „PKI based algorithm" for mitigating black hole attack in AODV protocol has been proposed, which is used to provide security to the MANETs. This algorithm prevents the black hole attack at initial stage. The main goal of PKI is not only to mitigate black hole attack but also to increase the throughput thereby reducing the packet loss due to black hole node.

REFERENCES

[1] Surana K.A., rathi s.b., thosar t.p. and snehal mehatre, Securing black hole attack in routing protocol aodv in manet withwatchdog mechanisms, world research journal of computer architecture (2012)
[2] Dr. V Sankaranarayanan, prevention of co-operative black holeattackinmanet,journal of networks, 2008.
[3] Nirali Modi, Vinit Kumar Gupta, prevention of blackholeattackusingaodvroutingprotocol in manet, (ijcsit) international journal of computer science and information technologies, 2014.
[4] Piyush Khemariya, Upendra kumar Purohit** & Umeshbarahdiya,performance study of improved aodv against black hole attack in wireless environment, international journal of engineering research and modern education (ijerme)(2016)
[5] Madhuri Gupta, Krishna Kumar Joshi, an innovative approach to detect the gray-hole attack in aodv based manet, international journal of computer applications ,2013.
[6] Heta Changela, Amit Lathigara, algorithm to detect and overcome the black hole attack in manets, international journal of computer applications ,2015.
[7] Lalita Prajapati, Anurag Singh Tomar, detection of black hole attack with improved aodv protocol in manet,(ijirset) 2015.
[8] Satoshi Kurosawa, Abbas Jamalipour, detecting blackhole attack on aodv-based Mobile ad hoc networks by dynamic learning Method, international journal of network security, 2007
[9] Neeraj Saini, Lalit Garg, enhanced aodv routing protocol against black hole attack, international journal of advanced,2014.
[10] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian journal of science and technology 9, no. 26 (2016).
[11] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "energy aware routing for manets based on current processing state of nodes." journal of theoretical & applied information technology 91, no. 2 (2016).
[12] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "analytical model for evaluating the bottleneck node in manets." indian journal of science and technology 9, no. 31 (2016).
[13] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "preventing black hole attacks in manets using secure knowledge algorithm." in signal processing and communication engineering systems (spaces), 2015 international conference on, pp. 421-425. Ieee, 2015.
[14] Mohammad, Arshad Ahmad Khan, and c. Atheeq. "mutual authenticated key agreement scheme for integrated internet manets." (2016)
[15] Ankita Joshi, Er. Aditi Agrawal, Prof A. K. Jaiswal, Dr. Rajeev Paulus, TD-DEEDV: A Technique to prevent collaborative attacks using Clustering and DigitalSignature in Multi Hop Hybrid Adhoc Networks, *International* Journal of Advanced Research in Computer Engineering & Technology (IJARCET)2016.

Authors

Abdulssalam Abdulwhab .A. Alafi

M.Tech student in the Electronics and Communication Engineering from Shepherd institute of Engineering and Technology, SHUATS. and he completed his Bachelor degree from the Higher Institute for comprehensive careers -Alshati of Libya in 2005.

Er . Aditi Agrawal she has been working in the Department of Electronic and Communication Engineering, as an Assistant Professor in Sam Higginbotom University of Agriculture, Technology and Sciences. She is member of IEEE.

Prof . A . .K . Jaiswal, he is presently working as professor and HOD of the department of electronics and communication in shepherd institute of engineering and technology of Sam Higginbottom University, Allahabad his area of work is optical fiber communication system and visited Germany Denmark and Finland for exploration of system designing under UND/Govt. of India sponsored POSAPP (fiber optics system application promotion programme). He has more than 35 years' experience in the related fields and has instrumented in fetching national award also for developing and commercializing a patented electronics process instrument.

Dr. Rajeev Paulus received his Doctorate degree in Electronic and Communication Engineering from SHUATS, Allahabad, and M.Tech. degree from the Department of Electronic Engineering, MNNIT, Allahabad. He received his Bachelor's degree in Electronic Engineering from the University of Pune. He has been working in the Department of Electronic and Communication Engineering, as an Assistant Professor in Sam Higginbotom University of Agriculture, Technology and Sciences. He is Life member of ISTE and member of IEEE.