DESIGN AND DEVELOPMENT OF A NEW ALGORITHM FOR DETECTING AND LOCALIZATION OF MULTIPLE ATTACKS IN WIRELESS SENSOR NETWORK

Dr. M. Mohammadha Hussaini[1], Dr. A. Rajalakshmi[2]

[1]Associate Professor, Department of EEE, Institute of Road and Transport Technology, Erode.
[2]Associate Professor, Department of Computer Applications, Dhanalakshmi College of Engineering, Chennai.
Email:rajalakshmianbhu@gmail.com

Abstract

In Wireless Sensor Network (WSN) is a standalone network capable of autonomous operation where nodes communicate with each other without the need of any existing infrastructure. They are self configuring, autonomous, quickly deployable and operate without infrastructure. Mobile ad hoc networks consist of nodes that cooperate to provide connectivity and are free to move and organize randomly. These nodes are often vulnerable to failure thus making wireless network open to threats and attacks. Communication in WSN relies on mutual trust between the participating nodes but the features of Wireless Sensor Network (WSN) make this hard. Nodes sometimes fail to transmit and start dropping packets during the transmission. Such nodes are responsible for untrustworthy routing. A trust based scheme can be used to track these untrustworthy nodes and isolate them from routing, thus provide trustworthiness. The proposed system is very simple toimplement and manipulates future behaviour via dynamic computation of previous data forwards and has records of historical behaviours. Unlike other systems' default trust assumptions, our system initialises trust with forwarding ratios. We proposed a trust based malicious detection algorithm to efficiently measure the performance of networks and handle those attacks accurately and separately. Local monitoring algorithm was used to detect the multiple attacks. After detecting these attacks and attacker nodes are eliminated. The simulation results show that our proposed methods can achieve over 98 percent throughput and accuracy when determining worm hole attack, black hole attack, ip address spoofing attack and mac address spoofing attack.

1. INTRODUCTION

Security in WSN might be as important in military and security applications (e.g. intruder detection). Attackers may attempt to block traffic in networks (i.e. perform a denial of service attack) or compromise data by adding some spoofed sensed data to network (i.e. aggregating attack). Attackers from the inside (corrupted node is placed into WSN) can commit routing attacks by leading data flow to spoofed sinkholes. Defenses against attacks depend on the particular attack type. For example, to suppress denial of service attacks, rerouting technique may be used (avoiding affected region). Another prevention technique lies in usage of error-detection codes which produce redundant information about message to assure the integrity of message. Network encryption and sensor node authentication are great approaches to secure WSN. However, sensor nodes need to be equipped with physical resources in order to compute cryptographic algorithms which may lead to more expensive sensor nodes. Moreover, computation of such algorithms negatively influences network's energy consumption. The base station also needs to be aware of security arrangement of WSN in order to be able to communicate with protected WSN and therefore a base station software developer must understand such arrangements of the related WSN.

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deals with data transmission. This scenario decreases the memory overhead, minimize the use of network resources, and run well in high mobility situation. In AODV, the communication involves main three procedures, i.e. path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. When the source node wants to establish the communication with the destination node, it will issue the route discovery procedure. The source node broadcasts route request packets (RREQ) to its entire accessible neighbor's. The intermediate node that receive request (RREQ) will check the request. If the intermediate node is the destination, it will reply with a route reply message

BUPT

(RREP). If it is not the destination node, the request from the source will be forwarded to other neighbour nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from. The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes. The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts. When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

TRUST

Trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities". Trust has also been defined as the degree of belief about the behavior of other entities. Establishing trust relationships among participating nodes is vital to facilitate collaborative optimization of system metrics. Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the party". Trust is based upon the information that one node can gather about the other nodes in passive mode i.e., without requiring any special interrogation packets. Vital information regarding other nodes can be gathered by analyzing the received, forwarded and overheard packets.

Characteristics of trust

1. The existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed. Therefore, a decision method to determine trust against an entity should be wholly distributed.
2. Trust should be gauged without too much computation and communication load in a very customizable manner, while also capturing the complexities of the trust relationship.
3. A trust decision framework should not work under the assumption that all nodes are cooperative for WSN. The selfishness is prone to be rampant over collaboration. For example, to save battery life or computational power.

2. LITERATURE SURVEY

Edwin H.M. Sha, Hui Xia, Lei Ju, Xin Li, Zhiping Jia, [1] have proposed a model where each node derives neighbours' historical trusts based on their own packet correct forwarding ratios and uses packets correct forwarding ratios to recognize an evaluated (or monitored) node's historical behaviours. Taking an evaluated node's historical trust and its capability to deliver a mutually agreed service as the inputs, fuzzy logic rules prediction method is employed to calculate this evaluated node's current trust on the point view of the monitor. The obtained value not only offers a prediction of one's future behaviours, but also provides a relative identification of node's properties (i.e., normal or malicious nodes).

Asad Amir Pirzada and Chris McDonald [2] have proposed a model that computes situational trust in agents based upon the general trust in the trust or and in the importance and utility of the situation in which an agent finds itself, also where utility is considered similar to knowledge so that an agent can weigh up the costs and benefits that a particular situation holds. The number of variables in their model has been reduced by merging the utility and importance of a situation into a single variable called weight, which in turn increases or decreases with time. Also their model makes use of trust agents that reside on network nodes and each agent operates independently and maintains its individual perspective of the trust hierarchy and hence gathers data from events in all states, filters it, assigns weights to each event and computes different trust levels based upon them.

T.Beth, M.Borcherding, and B. Klein [3] have proposed a system in which trust among nodes is represented by opinion, a term derived from the subjective logic and the values of opinions are updated during a routing information exchange process. The credibility of a node is based on its healthy behaviour.

Fan Ye, Hao Yang, Haiyun Luo, Lixia Zhang and Song Wulu [4] have proposed solutions that are designed

explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in in-depth protection.

Jaisanka.N and Saravanan.R [5] have proposed a multipath routing scheme called Multipath On-demand Routing (MORT), in order to minimize the route break recovery overhead. This scheme provides multiple routes on the intermediate nodes on the primary path to destination along with source node. The primary path is the first path received by the source node after initiating the route discovery, which is usually the shortest path. Having multiple routes at the intermediate nodes of the primary path, avoid overhead of additional route discovery attempts, and reduce the route error transmitted during route break recovery.

Kamal Deep, Meka Mohit and Virendra Shambhu Upadhyaya [6] have proposed a Trust-basedframework which uses Route Trustas a metric for the source node to make such informed route selection decisions and focuses on improving the performance of AODV including multi-path variants of the protocol which are equally susceptible to malicious node behaviour. Also the schemes to make the protocol secure rely on heavy encryption techniques or on continuous promiscuous monitoring of the neighbours both of which are restrictive in the resource constrained wireless domain and would are susceptible to scalability concerns.

T. M. Navamani, S. Priyadsrini, and Venkatesh Mahadevan [7] have proposed a system that promotes enhanced AODV with route lifetime prediction algorithms with traditional AODV in terms of network packet delivery ratio, routing failures, and control packet overhead. The added route lifetime prediction algorithm implemented in AODV performs better than the original AODV protocol in varying node velocity environments. Their proposed algorithm selects the path with longest route lifetime. As the route with lowest lifetime is eliminated and only the route with Routing overhead is defined as the amount of routing control packets, including RREQ and RREP. Thus in this system, route discovery process considers the lifetime of the route as the metric while selecting the route, the routing failure is minimized. This reduces the number of route discovery process and also the computation overhead of every node involved in route discovery process which affects the overall performance of routing protocol.

Chung-wei Lee and Rajiv K. Nekka [8] have proposed a routing protocol that is based on securing the routing information from unauthorized users. Even though routing protocols of this category are already proposed, they are not efficient, in the sense that, they use the same kind of encryption algorithms (mostly high level) for every bit of routing information they pass from one intermediate node to another in the routing path. This consumes lot of energy/power as well as time. This routing algorithm basically behaves depending upon the trust one node has on its neighbour.

3. PROPOSED SYSTEM

3.1 DESIGN DIAGRAM

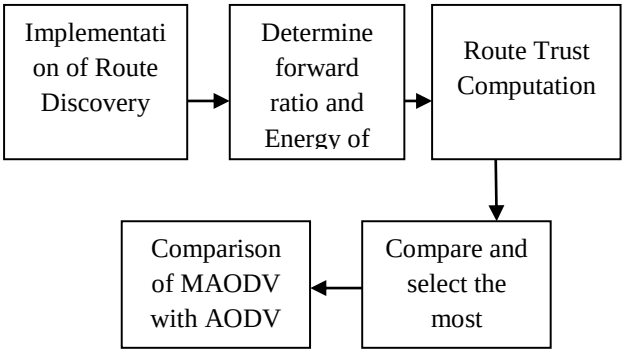


Figure 3.1 System Design

Figure 3.1 shows the architecture diagram of the system design. There are 5 major sections in system design. Each section deals with a vital functionality of the proposed system.

During route discovery, the RREP from shortest path is recorded for transmission in traditional AODV. However, the proposed system includes a multipath discovery approach by recording more than one route information. This is achieved by letting the source wait for more than one RREP.

Initially, packets are left to flow in the network to analyse the forwarding capability of every node. This is measured by a trust factor known as Forwarding Ratio (FR). These FR values become the trust values of every node.

The proposed system aims in establishing a trust factor for every recorded route. This factor is known as Route Trust. Route Trust is calculated using the trust values assigned for every node. Thus for transmission, the Route Trust of every route is compared and the route with the highest Route Trust is used as primary transmission route**.**

BUPT

Lastly, the modified protocol is compared with the traditional AODV in terms of delivery rate and packet loss**.**

4. PROPOSED METHODOLOGY

4.1 ROUTE DISCOVERY

In our proposed system, more than one route is recorded during route discovery process. When a node wants to send a packet to some destination node and does not locate a valid route in its routing table for that destination, it initiates a route discovery process. Source node broadcasts a route request (RREQ) packet to its neighbors, which then forwards the request to their neighbors and so on. To control network-wide broadcasts of RREQ packets, the source node use an expanding ring search technique. In this technique, source node starts searching the destination using some initial time to live (TTL) value. If no reply is received within the discovery period, TTL value incremented by an increment value. This process will continue until the threshold value is reached. When an intermediate node forwards the RREQ, it records the address of the neighbor from which first packet of the broadcast is received, thereby establishing a reverse path. When the RREQ is received by a node that is either the destination node or an intermediate node with a fresh enough route to the destination, it replies by unicasting the route reply (RREP) towards the source node. As the RREP is routed back along the reverse path, intermediate nodes along this path set up forward path entries to the destination in its route table and when the RREP reaches the source node, a route from source to the destination established. Now the first route has been established between the source and destination. However, in our system, we make the source wait for one more RREP. Therefore, there is more than one path available. Various calculations are performed on these paths to find the trustable path.

4.2 TRUST COMPUTATION

In our model, there are three types of trust, which are historical trust, current trust and route trust,

- Node's historical trust: it is estimated by the node's physical neighbors based on historical interaction information. In this project, the packet forwarding ratio is used as the single observable factor for assessing this trust. Two trust factors, which are control packet forwarding ratio CFR and data packet forwarding ratio DFR, are assigned weights in order to determine the overall historical trust of a node.
- Node's current trust: a node's current (or prediction) trust predicts this evaluated node's future behaviours for the next time moment. In our model, it is computed from the node's historical trust. At time t, we use the term 'trust value' TV (t) for a node's current trust value, for simplicity of representation.
- Route trust: it can be used to anticipate the quality of providing services (e.g., forwarding packets) along a routing route P, which is denoted by RouteTVp. When a source prepares to discover a routing route for transmitting message to any destination, it needs to assess the credibility of this route. Route trust value is computed according to the intermediate nodes' trust values along this route, which can be defined as a constraint in the trusted routing decision.

4.2.1 Computation of Forwarding Ratio

Forwarding Ratio (FR): It is the proportion of the number of packets forwarded correctly to the number of those supposed to be forwarded. Correct forwarding means a forwarding node not only transmits a packet to its next hop node but also forwards devotedly (correct modification if required). For instance, when a malicious neighbor node forwards a data packet after tampering with data, it is not considered as correct forwarding. If the node does not forward properly, the forwarding ratio of this neighbor will decrease. At time t, FR (t) is computed as follows:

$$FR(t) = \frac{\text{No. of packets forwarded}}{\text{No. of packets supposed to be forwarded}}$$

In mobile ad hoc networks, all packets can be classified into two types: control packets and data packets. The accuracy of control packets plays a vital role in establishment of accurate routes in the network. So FR is divided into two parts: Control packet Forwarding Ratio, denoted by CFR, and Data packet Forwarding Ratio, denoted by DFR. They are computed using forwarding count of control packets and data packets according to formula respectively. However for simplicity, our proposed system uses DFR alone.

4.2.2 Assigning Trust Values

The values obtained from calculating Forwarding Ratio is directly used by the proposed system to initialise the Trust values of the nodes. In existing system, a default value, say 0.5 is used. However, it is believed that it is necessary to filter nodes even at the initial stage. The Trust value of each node is updated in a special column "Trust Value" as shown in Table 4.2.2.

Trust Value	Destination ID	Next Hop	Sequence no	Hop Count
….	….	….	….	….
….	….	….	….	….
….	….	….	….	….
….	….	….	….	….

Table 4.2.2 Routing Table

4.3 ROUTE TRUST COMPUTATION

As already mentioned, this system focuses on trust-based route selection. At anytime, a route's trust is calculated by making use of the previously assigned trust values of nodes. So, at time t, the trust of a route P (denoted by RouteTVp(t)) is equal to the summation of node trust values in the route.

$$\text{RouteTVp (t)} = \sum_{k=0}^{n} \text{TVi}$$

In which, RouteTVp (t) is the route trust of path P at time t. TVi denotes the trust value of all intermediate nodes referred by i, in that path.

As shown in Figure 4.3, at the time t, the Trust value of nodes B, D, C, E are 0.9, 1, 0.81, 0.7 respectively. The trust value of route P(A,B,D,F) equals 1.9. The trust value of route P(A,C,E,F) equals 1.51.

The computation of route trust takes into account trust values of all intermediate nodes. Route trust denotes a joint probability at which packets will be forwarded if they are sent along the routing path.

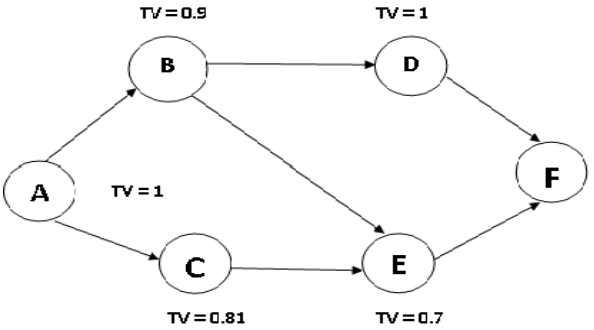


Figure 4.3 Route trust computation

4.4 SELECTION OF TRUSTABLE ROUTE

In the previous section, the methodology of Route trust calculation is elaborated. After the calculation, we have a set of path with their respective Route trust values. The route with the highest RouteTV is selected as the primary trustable path. Only in case of inevitable route failure, other alternative paths are considered during route rediscovery. In other words, the selection of trustable path is based on comparison of available paths based on their RouteTV.

5. RESULTS AND DISCUSSION

The simulation results obtained from executing the classical AODV protocol and the proposed protocol in ns-2 simulator, for various scenarios. Table 6.1 lists the general simulation parameters. Some of these parameters are varied to compare the performance of AODV and the proposed modified AODV protocol**.**

The radio propagation models implemented in ns-2 are used to predict the received signal power of each packet. There are three propagation models in ns-2, which are the free space model, two-ray ground reflection model and the shadowing model.

The free space propagation model assumes the ideal propagation condition that there is only one clear line of-sight path between the transmitter and receiver.

The two ray ground reflection model considers both the direct path and a ground reflection path. Shadowing model simulates shadow effect of obstructions between the transmitter and receiver, and this model is mainly used to simulate wireless channel in in-door environment.

It is shown that two ray propagation model gives more accurate prediction at a long distance than the

BUPT

free space model. So, two ray propagation models are chosen for simulation.

Propagation Model	Two Ray Ground
Transmission Range	250 m
Simulation Area	1500 * 1500 m
Channel capacity	2 Mbps
Mac	802.11
Queue	Drop Tail Priority Queue
Queue Length	50
Antenna	Omni Antenna
Simulation Time	300 s
Packet size	64 bytes
Traffic type	CBR
Mobility model	Random Way Point
Number of nodes	100
Number of communication pairs	15
Packet sending rate	3 packets/s
Speed of node	0 – 20 m/s
Pause Time	0 s

Table 5.1 Simulation Parameters

5.1 EFFECT OF NODE MOBILITY

Basing on the Trust computation model, nodes carry a trust value. The trust values can also be shared among neighbors using a higher layer, such as Reputation Exchange Protocol. Along with the nodes moves, the interactions among nodes increases gradually, the 'Trust' is transferred to entire network. For the low credibility of the nodes, in Moreover, in this project, route trust is the trust experienced by the lastpacket which has arrived along the route. Since network load conditions will change from time to time during the connection, the trust will also change accordingly. By using the latest arrived data packet to calculate RouteTVp (t), the scheme is adaptive to changing network conditions.

5.1.1 Data Delivery Rate

The effect of mobility of nodes on Delivery rate is analyzed. The mobility of nodes is determined by the pause time parameter setting in ns-2 simulator. The other parameters setting are done as per Table 8. Pause time is varied as 0, 100, 200, 300, 400 and 500 seconds. For each pause time, the Delivery rate is calculated, and has been found that MAODV has better data delivery rate due to transmission along trustable routes.

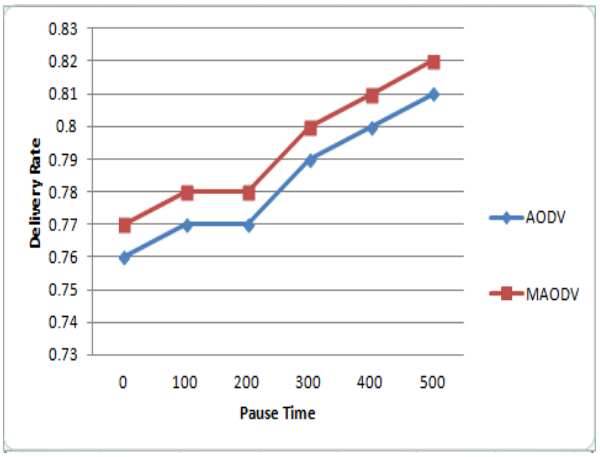


Figure 5.1 Effect of node mobility on data delivery rate

5.2 EFFECT OF NODE DENSITY

We evaluate the proposed protocols by varying number of nodes. When there are no inefficient nodes, the packet loss rate is very low. The reason is that, with the proportion of inefficient nodes increases, the probabilitypacket loss tends to increase on routing routes.

5.2.1 Packet Loss

The effect of load on packet loss rate is analyzed. The load in network is determined by the number of pairs of nodes in communication in ns-2 simulator. The other parameters setting are done as per Table 5.1.

In Figure 5.2, it is evident that the packet loss is more in AODV than the packet loss in MAODV.

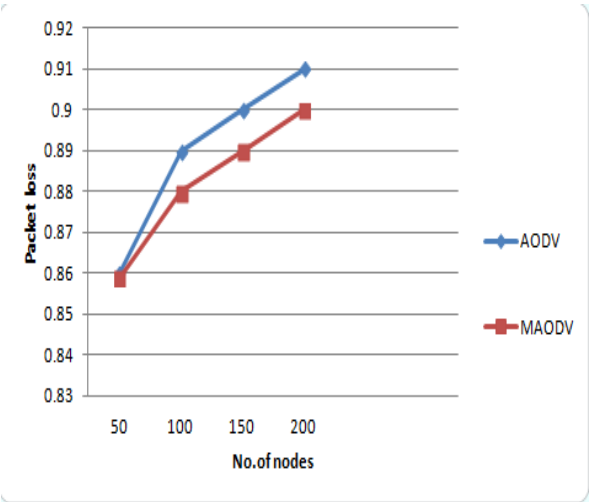


Figure 5.2 Effect of node density on packet loss

BUPT

6. CONCLUSION

We have proposed a trust-based malicious identification algorithm that enhances the security of network in the presence of malicious nodes. The proposed algorithm ensures the forwarding of packets through the trusted and least link delay routes only by monitoring the behavior of each other. Local monitoring algorithm is proposed to detect the various attacks like warm hole, black hole, ip address and mac address attacks. After detecting these attacks and attacker nodes are eliminated. The proposed algorithm that identifies the most trustworthy routes among a set of routes. Trust value for each node is calculated using behavior of the nodes. In an ad-hoc network where doubt and uncertainty are inherent, the proposed trust model creates and maintains trust levels based on PRR and energy computation mechanism. The routes selected using the proposedmodel may not be cryptographically secure but they do establish relative levels of trustworthiness with them. The model will be most suited to wireless sensor networks where there is no trust infrastructure and the trust relationships are less formal, temporary or short-term.

REFERENCES

[1] Edwin H.M. Sha, Hui Xia, Lei Ju, Xin Li, Zhiping Jia, (2012) ELSEVIER, journal homepage: www.elsevier.com/locate/adhoc. "Trust prediction and trust-based source routing in mobile ad hoc networks".

[2] Asad Amir Pirzada and Chris McDonald, (2009) "Establishing Trust in Pure Ad hoc Networks".

[3]T.Beth, M.Borcherding, and B. Klein, (2006) "A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks". In Proceedings of the European Symposium on Research in Computer Security.

[4] Fan Ye, Hao Yang, Haiyun Luo, Lixia Zhang and Song Wulu, IEEE (2010). "Security in Mobile Ad Hoc Networks: Challenges and solutions", UCLA Computer Science Department.

[5] Jaisanka.N and Saravanan.R, (2010) IACSIT International Journal of Engineering and Technology, "An Extended AODV Protocol for Multipath Routing in MANETs".

[6] Kamal Deep, Meka Mohit ,Virendra Shambhu Upadhyaya, (2009) "Trust Based Routing Decisions in Mobile Ad-hoc Networks", Department of Computer Science and EngineeringState University of New York at Buffalo, New York.

[7] T. M. Navamani, S. Priyadsrini, and Venkatesh Mahadevan, July 2012International Journal of Information and Electronics Engineering, "An Efficient Route Discovery in Manets with Improved Route Lifetime".

[8] Chung-wei Lee , Rajiv K. Nekka Computer Science Dept, Auburn University (2010) "Trust Based Adaptive On Demand Ad Hoc Routing Protocol".

AUTHOR PROFILE



Dr. M. Mohammadha Hussaini received BE.Degree during the year 1991 and M.E Degree during the year 1993 from Madurai Kamaraj University with distinctions in both. She received her Ph.D in faculty of electrical Engineering from Anna University in the year 2012.She has also published more than seven International Journals and more than 15 papers in national conferences.She is working as Associate Professor in Institute of Road and Transport Technology,Erode.



Dr. A.Rajalakshmi received the Master of Computer Applications and M.Phil from Anna University in 2008 and St.Peter University in 2010. She is working in Dhanalakshmi College of Engineering as Assistant professor. She is pursuing Ph.d in Bharathiar University. She is having 5 years of teaching experience in respective field. She published journal in advanced science letters, Vol. 20, 1813-1816, 2014.

BUPT