www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5 may, 2014 Page No. 6158-6164

Trust-based security for Ad-Hoc network

Prof. (Ms) A. A. Patil[1], Prof. T. I. Bagban[2], Prof. S. J. Patil[3]

[1]Department of Information Technology,
Dr. J. J. Magdum College of Engineering, Jaysingpur, India.
ashwinipatil_123@yahoo.co.in

[2] Department of Information Technology,
DKTE'S Textile & Engg. Institute, Ichalkaranji, India
bagban@yahoo.com

[3] Department of Electronics Engineering,
DKTE'S Textile & Engg. Institute, Ichalkaranji, India
p.sandeep2020@gmail.com,

Abstract: A mobile Ad-hoc network (MANET**)** is decentralized type, infrastructure less wireless network of mobile nodes. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves. i.e., routing functionality will be incorporated into mobile nodes. Due to multi-hop routing and absence of centralized administration in open environment, MANETs are vulnerable to attacks by malicious nodes. In order to decrease the hazards from malicious nodes, a simple trust model is built to evaluate neighbors' behaviors using forwarding packets. Extended from the Ad-hoc on demand distance vector (AODV) routing protocol , a trust-based reactive multipath routing protocol, Ad-hoc on-demand trusted-path distance vector (AOTDV), is proposed for MANETs. This protocol is able to discover multiple loop-free paths as candidates in one route discovery. These paths are evaluated by two aspects: hop counts and trust values. From these paths shortest path is chosen that meet the requirements of data packets for dependability or trust. Several experiments have been conducted to compare AODV and AOTDV protocols and the results show that AOTDV improves packet delivery ratio and reduce the impairment from black hole.

Keywords: AODV, AOTDV, MANETs**.**

1. Introduction

A mobile Ad-hoc network (MANET) is a self organized multi-hop system comprised of mobile wireless nodes. Two nodes out of direct communication range need intermediate nodes to forward their messages. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. To find the path which is malicious node free is solution for MANET attacks. For this selection of path should be dependable. Designing a dependable routing protocol is a significant problem for a MANET.

Using authentication and encryption mechanism, secure routing protocols [10, 11] have been developed to ensure properties such as confidentiality, integrity etc. However, those protocols require a centralized trusted third party, which is impractical for MANETs [3].

As in social society, one will trust another person to carry out an action, but the former cannot guarantee the latter's behaviour [2]. Thus the concept of trust is introduced into computing network to measure an expectation or uncertainty that an entity has about another's future behaviour for a certain action. Trust can be derived from direct interactions or from recommendations.

There are two primary motivations associated with trust management in MANETs. At first, trust evaluation helps distinguish between good and malicious entities. Creating trust history, one entity can remember others' behaviours. This memory provides a method for good entities to avoid working with ‘ex-convict’ or suspect ones. Secondly, trust management offers a prediction of one’s future behaviour and improves network performance. The results of evaluation can be directly applied to an incentive for good or honest behaviours while a penalty for selfish or malicious behaviours in the network. The feedback reminds network participants to act more responsibly. These motivations have interested researchers from the areas of information security and computer network in trust management of MANETs.

We introduce a trust model to evaluate neighbours’ behaviours. For evaluating the neighbours’ behaviours packet forwarding ratio is used. In this trust model, a node trust is represented as a weighted sum of forwarding ratio of packets and a continued product of node trusts is computed as path trust. Then one novel reactive type routing protocol is proposed for MANETs, termed as ad hoc on-demand trusted-path distance vector (AOTDV). In this protocol, a source can establish multiple loop-free paths to a destination in one route discovery process. Each path has an evaluation vector composed of a hop count and a trust value. A destination will respond with at most k shortest paths as candidates that satisfy the trust requirements of data packets. The shortest one will be selected as the forwarding route using hop count. We have performed some experiments for comparing AODV and AOTDV. The experiment results show that AOTDV improves packet delivery ratio and throughput. As a trusted multipath routing protocol, AOTDV also isolate the malicious node from the network.

2. Present Theory & Practices:

Trust-based routing protocols is combination of two research fields – trust models in trust management and routing protocols for MANETs.

2.1 Trust Model

Several trust models have been developed for trust management. These models can be classified into two groups: centralised models and decentralised models.

In centralized models, trust values are maintained in a common central node or through an authorized third party. The requirement of a trusted third party goes against the nature of MANETs.

In decentralized models, a node assigns a trust/trustworthiness value for every communicated node. Most researchers [12, 13, 14, 15] are advocating the use of ratings and prefer to complex rating aggregation algorithms to evaluate trust from several aspects and filter out the bad ratings. However, these sophisticated models are not appropriate for MANETs where resources are limited and network topology is dynamic. Several trust models [16, 17] have been developed for peer-to-peer systems based on sharing recommendation information to establish reputation. Although in principle, these models could be applied to routing in MANETs, additional recommendation information exchanging incurs significant network overhead. In particular, Pirzada and McDonald [4] proposed aggregation mechanism, where nodes calculate trust according to multiple observed events including acknowledgements, packet precision, gratuitous route replies, and blacklists. They have obtained promising simulation results, but it is possible to obtain similar promising effects with a simplified trust model.

2.2 Routing Protocols

Routing protocols in Ad-hoc network can be categorized into two types: proactive and reactive. Pro-active routing protocols establish and maintain routes at all instants of time in order to avoid the latency during new route discoveries. Reactive routing protocols do discovery route only when one node tries to transmit packets to another unknown-route node so as to save resources. The nodes in an Ad-hoc network generally have limited resources, such as bandwidth and power energy; therefore reactive routing protocols attract more interests. AODV [6] combines the use of destination sequence numbers in DSDV [8] with the on-demand route discovery technique in DSR [9] to formulate a loop-free and single path routing protocol. Unlike DSR which use source routing, AODV is based on a hop-by-hop routing mechanism. Extended from AODV, AOMDV [7] is proposed to discover multiple loop-free and link-disjoint paths. Experiments show that AOMDV is able to achieve a remarkable improvement in the end-to-end delay.

Several secure routing protocols with cryptography have been proposed to protect the Ad-hoc networks, such as SAODV [10], Ariadne [11], but most of these protocols required centralized units or trusted third-parties to issue digital certificates or monitor network traffics. The requirement for a common trusted authority actually restricts the self organization nature. Therefore, these protocols are less practical for MANET.

Recently a new class of routing protocol in MANET has been proposed, termed trusted routing protocol, which consists of two parts: a routing part and a trust model [3]. Routing decisions are made according to the trust model. Pirzada et al. [5] evaluated the performance of three trust-based reactive routing protocols (trusted AODV, DSR and TORA) using trust model by varying number of malicious nodes. The results indicate that each trust-based routing protocol has its own peculiar advantage that makes it suitable for application in a particular extemporized environment. Especially AODV routing maintains a stable throughput and surpasses TORA and DSR at higher traffic loads [5]. Therefore, trust model is introduced in AODV and designed a trust-based multipath routing protocol (AOTDV).

3 Trust Model

A node can calculate the trust of neighbours by monitoring their behaviour. A node can monitor its neighbours behaviours by placing itself in a promiscuous mode. Promiscuous mode allows a node to view all packets on a network that are associated with it.

We assume that one node broadcasts a packet and all neighbours will receive the packet correctly. However, if the distance between source and destination is beyond one hop, packets might be dropped by intermediate nodes because of unexpected causes (such as heavy traffic) or malicious attacks (such as black-hole or grey-hole attacks). Trust evaluation in a routing procedure is an assessment of forwarding behaviours of neighbours by a sender. More specifically, a node A will give its neighbor B a trust score after the node B transmits a packet sent by node A. Thus, we use packet forwarding ratio to evaluate the quality of forwarding.

In this model trust is depends on forwarding ratio. Node A will calculate trust of node B after B forwards packet which is sent by A. If node B forwards it correctly trust will increase otherwise decrease. 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 neighbour node forwards a data packet after tampering with data, it is not considered as correct forwarding. If the sender monitors this illegal modification, the forwarding ratio of the neighbour will decrease.

Definition 1 (Forwarding ratio): Forwarding ratio is the proportion of the number of packets forwarded correctly to the number of packets supposed to be forwarded.

Definition 2 (Window forwarding ratio): The window forwarding ratio FR(t) is the packet forwarding ratio in a recent window. FR(t) is computed as follows

$$FR(t)=\begin{cases}\dfrac{N_C(t)-N_C(t-W)}{N_A(t)-N_A(t-W)} & ,t>W \\ \\ \dfrac{N_C(t)}{N_A(t)} & ,t\leq W\end{cases} \qquad (1)$$

Where $N_C(t)$ represents the cumulative count of correct forwarding and $N_A(t)$ signifies the total count of all requesting before time t. The count of correct forwarding in a time window (from time t-W to t) is equal to $N_C(t)-N_C(t-W)$, where W represents the width of the time window. We compute FR(t) only using the forwarding count and requesting count in the recent W time units. The history records out of the recent window are discarded.

3.1 Node Trust

In MANETs, there is two types packets: control packets and data packets. Control packets are used for route request, route reply, route update and route error. The accuracy of control packets plays a vital role in establishment of accurate routes in network. So FR(t) is divided into two parts: control packet forwarding ratio, denoted by CFR(t), and data packet forwarding ratio, denoted by DFR(t). They are computed using forwarding count of control packets and data packets according to formula (1) respectively.

Two trust factors [CFR(t) and DFR(t)] are assigned weights in order to determine the overall trust value of a node. The direct trust in node B by node A is represented as T_{AB} and is given by the following formula

$$T_{AB}(t)=w1\times CFR_{AB}(t)+w2\times DFR_{AB}(t) \qquad (2)$$

where $CFR_{AB}(t)$ and $DFR_{AB}(t)$ represent control packet forwarding ratio and data packet forwarding ratio observed by node A for forwarding node B at time t, respectively. The weights w1 and w2 ($w1, w2 \geq 0$ and $w1+w2=1$) are assigned to CFR and DFR, respectively.

After each interaction, node A checks whether the neighbor B forwards the packet correctly. If so, the trust value T_{AB} increases. Otherwise, T_{AB} decreases. In our trust model, trust values are limited in a continuous range from 0 to 1 (i.e. $0 \leq T_{AB} \leq 1$). The trust value of 0 signifies complete distrust whereas the value of 1 implies absolute trust. An example of trust levels of nodes are listed in Table 1. If there is no interaction between two nodes, the initial trust value is set to 0.75 (less trustworthy node). That is, we adopt a limited optimistic view on unknown nodes. A threshold h, termed as the black-list trust threshold, is used to detect malicious nodes. In other words, if the trust value of a node is smaller than h, it will be regarded as a malicious node.

Table 1: Trust levels of nodes.

Level	**Trust Value**	**Meaning**
1	[0, 0.5]	Malicious node
2	(0.5, 0.75]	Suspect node
3	(0.75, 0.9]	Less trustworthy node
4	(0.9, 1]	Trusted node

3.2 Path Trust

In our model the trust of a path P (denoted by $T_P(t)$) is equal to the continued product of the trust values of nodes along the path P, i.e.

$$T_p(t)=\prod(\{T_{AB}(t) \mid n_A,n_B \in P \text{ and } n_A\rightarrow n_B \text{ and } n_B \neq n_D\}) \quad (3)$$

in which, n_A and n_B are any two adjacent nodes among the path P and $n_A\rightarrow n_B$ means that n_B is the next-hop node of n_B and n_D is the destination node in the path P

4 Trust-based on-demand routing protocol

4.1 Routing table

The Use of a routing table is to store the routes to other nodes. In an Ad-hoc network each node maintains a routing table composed of multiple routing entries. AOTDV adopts a hop-by-hop routing mechanism, in which the source is not expected to know all nodes in the path to a destination; it is sufficient for the source to know which neighbor is the next hop. When a data packet is going to a destination, it refers to local routing table to find the next hop (node A). Once it reaches node A, it refers to node A's routing table for the next hop to the destination. This process will continue until it reaches the destination.

Any node only stores routes to nodes that have interacted with it recently, not all routes in history because network topology of a MANET changes dynamically.

Fig. 1 shows the structure of routing table entries for AOTDV. A routing entry in AOTDV consists of the following fields:

1. Destination: the identifier of destination node.

2. Destination sequence number: the greatest known sequence number for destination denotes freshness of the route. It is used to avoid routing loop

3. Next hop: A neighbour node, to which a packet is sent.

4. Hop count and path trust: the two metrics compose an evaluation vector of a path. The selected path is the shortest one in the paths which satisfy the packet trust requirement.

5. Expiration timeout (ET): the time after which the route is considered to be invalid. Each time a route is used to transmit data, the timeout for the route is reset to the current time plus a constant (active route timeout).

Destination
Destination Sequence Number
{(NextHop1,HopCount1,PathTrust1, ExpirationTimeout1), (NextHop2,HopCount2,PathTrust2, ExpirationTimeout2), … }

Figure 1 Structure of routing table entries for AOTDV

Multiple routes leading to the same destination are arranged in ascending order of HopCount, that isHopCount1 ≤ HopCount2 ≤ · · · ≤ HopCountn. If two paths have the same

HopCount, the one with greater PathTrust precedes, that is ∀ $HopCount_i=HopCount_{i+1}$, PathTrusti ≥ $PathTrust_{i+1}$.

4.2 Trust record list

To store the trust information trust record list is introduced. Each node will maintain a trust record for every neighbour to which packets have been sent for forwarding. A trust record listed in Table 2 contains a node ID, node trust, two integer counters of NC and NA for control packets, two integer counters of NC and NA for data packets and a packet buffer. The packet buffer is used to record all packets sent recently. It is a circular buffer, which means that the buffer will cycle and overwrite the oldest packet If it is not removed in time.

Table 2: Structure of a trust record

node ID
node Trust
NC and NA for control packets
NC and NA for data packets
packet buffer

5. Performance Evaluation

5.1 Simulation model & parameters

Our simulations are implemented in Network Simulator (NS-2) from Lawrence Berkeley National Laboratory (LBNL) with extensions for wireless links form the Monarch project at Carnegie Mellon University. The simulation parameters are summarized as follows:

Table 3: Simulation parameters

Network Simulator	NS-2
Network area	1000 X 1000
Number of nodes	100, 125, 175, 200.
Speed of the nodes	10 m/s.
Traffic load	CBR
MAC protocol	IEEE802.11b
Simulation time	200s. and repeated for various number of nodes.

5.2 Performance metrics

5.2.1 Packet delivery ratio

The fraction of the data packets delivered to the destination nodes to those sent by the source nodes.

5.2.2 Throughput

It is the average rate of successful message delivery over a communication channel.

5.2.3 Routing packet overhead

The number of routing packets transmitted per data packet delivered at the destination. Each hop - wise transmission of a routing packet is counted as one transmission. The routing load metric evaluates the efficiency of the routing protocol.

5.2.4 Average End-to-End Delay

Average end to end delay includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets.

6. Result and discussion

When we designed the security routing protocol, we found that it had increase in packet delivery ratio as compared with AODV as shown in Figure 2

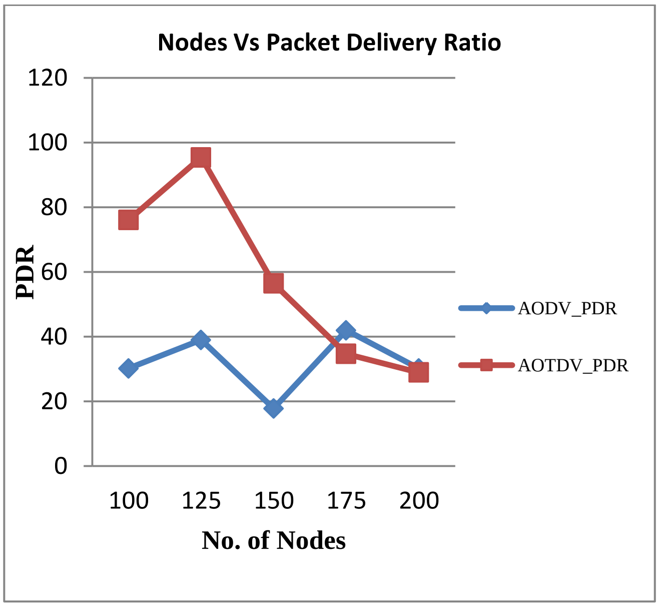

Figure 2 Comparison of packet delivery ratio

Fig. 3 shows AOTDV has higher throughput than AODV for less number of nodes. In AOTDV, lesser number of routes reply messages are generated which will result in lower MAC layer load. Hence throughput for AOTDV increases at a less number of nodes than that of AODV, resulting in higher throughput than AODV with less number of nodes.

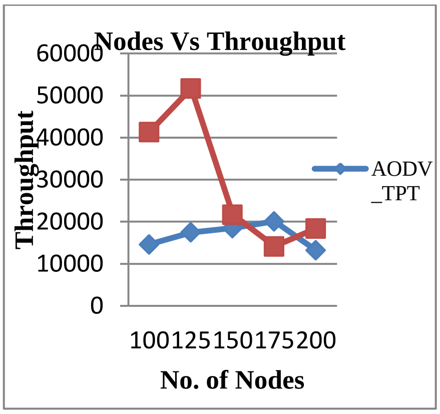

Figure 3 Comparison of throughput

Fig. 4 show routing packet overhead of AODV and AOTDV by varying number of nodes. The overhead in AOTDV is higher than that in AODV. There are two reasons for the higher overhead: (i) more RREQ and RREP packets need to be sent for qualified routes to meet trust requirement in AOTDV, and meanwhile, trust requirement is not considered in AODV; and (ii) the additional route update packets increase the amount of control packets and the routing packet overhead in AOTDV.

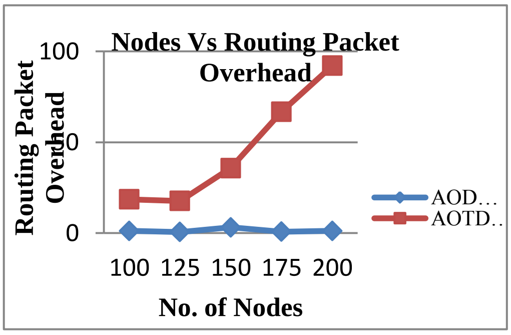

Figure 4 Comparison of routing packet overhead

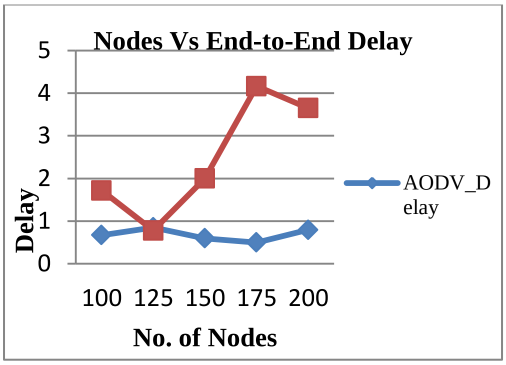

Figure 5 Comparison of End-to-end delay

Fig. 5 compares the average end-to-end delay for AOTDV and AODV. There is a random variation in delay, as quite naturally expected because of the Ad-hoc nature of the network.

7. Conclusion

The proposed trust based on demand routing protocol finds multiple trusted path to destination from which shortest path is selected for communication. Trust is depends upon packet forwarding ratio so we can easily isolate malicious node which are caused for black hole and gray hole attack in network. Throughput and packet delivery ratio of AOTDV are better than AODV.

References

[1] X. Li Z. Jia P. Zhang R. Zhang H. Wang.:' Trust-based on-demand multipath routing in mobile Ad-hoc networks' , in IET Information Security, 2010, Vol. 4, Iss. 4, pp. 212–232.

[2] Gambetta, D.:'Can we trust trust?', in Gambetta, D. (Ed.):'Trust: Making and Breaking Cooperative Relations'(Oxford Press, 2000, 1st edn.), pp. 213–237

[3] Griffiths, N., Jhumka, A., Dawson, A., and Myers, R.:'A Simple Trust Model for On-Demand Routing in Mobile Ad-hoc Networks', Proc. Int. Symp. onIntelligent Distributed Computing (IDC 2008), 2008, pp. 105-114

[4] Pirzada, A.A., and McDonald, C.:'Trust establishment in pure ad-hoc networks', Wireless Personal Communications, 2006,37,(1),pp39–168

[5] Pirzada, A.A., McDonald, and C., Datta, A.:'Performance comparison of trust-based reactive routing protocols', IEEE Trans. on Mobile Computing, 2006, 5, (6), 695–710

[6] Perkins, CE., Royer, EM., and Das, SR.:'Ad-hoc On-demand Distance Vector Routing', Proc. Int. Workshop on Mobile Computing Systems and Applications (WMCSA),1999, pp.90-100

[7] Marina, MK., and Das, S R. 'On-demand Multipath Distance Vector Routing for Ad-hoc Networks', Proc. Int. Conf. on Network Protocols. Nov. 2001, pp.11-14

[8] Perkins, C.E., and Bhagwat, P. 'Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for mobile Computers', Proc. Int. Conf. ACM SIGCOMM, 1994, pp234-244

[9] Johnson, D., and Maltz, D. ’Dynamic Source Routing in Ad-hoc Wireless Networks’, in Tomasz, I., and Hank, K. (Ed.):’Mobile Computing’ (Kluwer Academic Press, 1996, 1st edn.), pp. 153-181

[10] Zapata, M.G., and Asokan, N.:’Secure Ad-hoc On-Demand Distance Vector Routing’, ACM Mobile Computing and Communications Review, July 2002, 3, (6), pp. 106-107

[11] Hu, Y.C., Perrig, A., and Johnson, D.B.:’Ariadne: A Secure On-Demand Routing Protocol for Ad-hoc Networks’, Proc. Int. Conf. Mobile Computing and Networking (Mobicom’02), Atlanta, Georgia, September 2002, pp.12-23.

[12] Buchegger, S., and Boudec J.L.:’A robust reputation system for p2p and mobile ad-hoc networks’, Proc. Int. Workshop on the Economics of Peer-to-Peer Systems, Cambridge MA, U.S.A., June 2004.

[13] Jøsang, A., and Ismail, R.:’The beta reputation system’, Proc.of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002. pp. 1-14.

[14] Sabater, J., and Sierra, C.:’Regret: Reputation in gregarious societies’, Proc. Int. Conf. Autonomous Agents, Montreal, Canada 2002, pp. 194-195

[15] Srivatsa, M., and Liu, L.:’Securing decentralized reputation management using trustguard’, Journal of Parallel and Dis-tributed Computing, 2006, 66, (9), pp. 1217–1232

[16] Selçuk, A.A., Uzun, E., and Pariente, M.R.:’A reputation-based trust management system for P2P networks’, Proc. Int. Symposium on Cluster Computing and the Grid, 2004, pp. 251–258

[17] Xiong, L., and Liu, L.:’PeerTrust: Supporting reputation-based trust in peer-to-peer communities’. IEEE Trans. on Knowledge and Data Engineering, 2004,16,(7), pp. 843–857

Author Profile

Prof. (Ms.) A. A. Patil – Received the BE degree in Information Technology from DKTE’s TEI, Ichalkaranji, Shivaji University, Kolhapur, and pursuing ME degree from same University, Currently working as an Assistant Professor in the Department of Information Technology, Dr. JJMCOE, Jaysingpur, Shivaji University, Kolhapur. Research interests are in the field of Ad-hoc Network and Mobile Computing.

Prof. Mr. T. I. Bagban – Received the BE degree in Computer Science & Engg. from WCE, Sangli, Shivaji University, Kolhapur, and M.Tech. degree from WCE, Sangli, Shivaji University, Kolhapur, and Pusuing PhD from Shivaji University. Currently working as an Associate Professor in the Department of Information Technology, DKTE’s TEI, Ichalkaranji, Shivaji University, Kolhapur. Research interests are in the field of Program analysis, Computer Networks, and Web mining.

Prof. Mr. S. J. Patil– Received the BE degree in Electronics from DKTE’s TEI, Ichalkaranji, Shivaji University, Kolhapur, and ME degree from same University, Currently working as an Assistant Professor in the Department of Electronics, DKTE’s TEI, Ichalkaranji, Shivaji University, Kolhapur. Research interests are in the field of Ad-hoc Network and Wireless Sensor Network.