# Evaluating MANET Uncertainty Analysis Framework

Samradnyee S Pawar, Sandeep A Thorat, Durgesh P Kshirsagar

# Evaluating MANET Uncertainty Analysis Framework

Samradnyee S. Pawar
Computer Science and Engineering,
Rajarambapu Institute of Technology,
Islampur, INDIA
pawarsamradnyee@gmail.com

Sandeep A. Thorat
Computer Science and Engineering,
Rajarambapu Institute of Technology,
Islampur, INDIA
sandeep.thorat@ritindia.edu

Durgesh P. Kshirsagar
Computer Science and Engineering,
Rajarambapu Institute of Technology,
Islampur, INDIA
durgesh.kshirsagar@ritindia.edu

***Abstract*—Using trust relationships between nodes, decision making in a peer-to-peer distributed network like MANET possible to improve. Uncertainty plays an important role in such decision making process. Our earlier research work viz. Sandeep et al. [1] proposed Uncertainty Analysis Framework (UAF) for MANET and integrated it with different trust variants representing direct trust, indirect trust and global trust. The research work explored relationship between uncertainty and trust. The UAF is found useful to quantify Belief, Disbelief, and Uncertainty (BDU) of a network. The earlier research work measured impact of direct, indirect and global trust on the performance of the routing protocols. The proposed work is useful to get more insights about - MANET working, effectiveness of trust based algorithms and impact of uncertainty on the behavior of MANET. This research work analyses UAF behavior and performance of indirect and global trust-based routing protocols using different test conditions. The proposed research work observed that, uncertainty reduces drastically when trust is used for decision making in routing protocols. It is also observed approximately 140 seconds are required to identify good and misbehaving nodes in the network. Belief, Disbelief and Uncertainty values are fairly stable after 140 seconds from network bootstrap. Indirect trust model is found more useful for open and distributed peer-to-peer networks.**

***Index Terms*—MANET; Routing Protocols; Packet Delivery Ratio (PDR); Average End to End delay (AE2E); Normalizing Routing Load (NRL); Belief; Dis-belief; Uncertainty**

## I. INTRODUCTION

Uncertainty is a state of limited knowledge where it is difficult to exactly describe existing state and future outcome. Uncertainty leads to incorrect decisions or more than one possible outcome. Uncertainty is seen in different fields including physics, engineering, economics, information science, statistics etc.[1].

A Mobile Ad-hoc Network (MANET) is continuously self-configuring network of mobile nodes connected by wireless links without any centralized control. As MANET is characterized by dynamic topology, absence of infrastructure, lack of centralized control and uncertainty of mobile nodes, analyzing behavior and working of MANETs is much more challenging than analysis of infrastructure-based network.

In MANET, each node relies other to forward packet to next available hop. Thus, each node acts as a router. Therefore, nodes should co-operate each other by forwarding packets to one another. S. A. Hosseini et al. [2] discussed packet dropping can be nullified by trust mechanism of node. Trust can be defined as reliance on and confidence in honesty, faith and integrity. In MANETs, Trust is a degree to which one node can depend upon another in order to forward packets. It is important to quantify trust and recognize uncertainty to reduce it in order to simulate collaboration between the nodes.

For aimed functionalities of MANET, establishing and quantifying trust of node is essential during routing [3]. It is important to quantify trust and recognize uncertainty in order to simulate collaboration between the nodes. Uncertainty shows significant impact on performance of network. While measuring trust in MANET, it is necessary to address present uncertainty. Author Y. Li et al. [4] modeled trust as Belief, Disbelief and Uncertainty (BDU). Belief is the probability of node to forward packet. Disbelief is probability that node will drop the packet and Uncertainty is probability of difficulty in predicting the behavior of node to forward or drop packet.

In our earlier publication Sandeep et al. [1], proposed Uncertainty Analysis Framework (UAF) to quantify Belief, Disbelief and Uncertainty (BDU) of a MANET. In the research work, the protocol AODV is integrated into different trust variants representing global trust, direct and indirect trust. It is observed that trust-based protocols show positive impact on performance of network. AODVIT (which represents indirect trust) and AODVCN (which represents global trust) found more effective. The work used different mobility models to assess performance of the AODVCN and AODVIT.

Further, this research work does extensive analysis of Uncertainty Analysis Framework (UAF) and its impact on MANET and trust-based routing protocols. Collaborative nature of mobile nodes show positive impact on performance of MANET. MANET is highly dynamic network, its performance is affected by many parameters like density of nodes, node speed, pause time etc. There is need to observe performance of proposed UAF using these parameters. In earlier work, BDU values calculated at the end of simulation. It is important to observe how their values change over time under different conditions. This research work addresses above mentioned issues.

Here, Uncertainty Analysis Framework (UAF) impacts on MANET is analyzed by varying network parameters like network size, number of malicious nodes, pause time and

ISBN 978-3-903176-03-4

speed of mobile nodes. The Belief, Disbelief and Uncertainty (BDU) values of individual nodes and entire network observed over the time period. The paper proposes evaluation of MANET using Uncertainty Analysis Framework (UAF). The paper is organized as follows; Section II presents existing literature review. Section III gives notion of test conditions for analysis of UAF. The experimental observations are described in section IV with definitions and test conditions. Section IV.(1) to IV.(5) describe detailed analysis of each test condition. The important discussions and conclusion is given in section V and VI respectively.

## II. LITERATURE REVIEW

Uncertainty modeling is important to measure performance of different systems which give output values. Research work is carried to model uncertainty using different methods. Vikas Kumar *et al.* [5] stated approaches like fuzzy modelling, Monte Carlo method to quantify uncertainty. Modelling uncertainty during risk assessment plays vital role for effective decision making. Arunraj *et al.* [6] used fuzzy set theory and Monte Carlo simulation for uncertainty analysis. The proposed method provides good measure of uncertainty than existing methods.

Previous research is carried to define trustworthiness of the node based upon three observations. First method is direct observations in which each node has trust value for each neighbor node based on packet forwarding behavior [7]. Second method is global trust to drop malicious peers from the network to quantify packet forwarding [8]. Third one is Trusted Third Party (TTP) called central authority but it is violating characteristics of MANET hence inappropriate in MANETs [9].

Research done to propose reputation systems which divided trust value as right or wrong. Thus, ignored many significant factors which affect the performance of MANET. Feng Li *et al.* [9] proposed new reputation system which includes uncertainty model to reflect node's confidence based on past experiences and analyzed how uncertainty affected by collection of trust value. Based on analytical and simulation results, it is also found that uncertainty reduces with mobility in MANET [9]. Feng Li *et al.* [10] presented a certainty oriented to reputation system which described relationship among uncertainty, recommendation and observation. Yirui Cong *et al.* [11] investigated interference prediction problem in MANET and analyzed that communication in MANET can be made superior with effective prediction of time varying interferences. In wireless ad-hoc network, node reliability is an important factor for secure communication. Research has been done to evaluate reliability of MANET under scenario of node failure [12]. Authors observed that increase in node failure decreases throughput hence reliability decreases gradually with increase in node failure. Z. Wei *et al.* [13] done research to enhance security of MANET using direct trust and indirect trust. The trust value of node is derived using Bayesian inference and Dempster-Shafer-Theory (DST). Nodes with lower trust excluded to provide secure path over wireless medium. Research contributions [14] and [15] found Bayesian inference and Dempster-Shafer theory (DST) as superior mechanism to evaluate trust value of node. Beyond the Bayesian inference and Dempster-Shafer-Theory, Yiping Li *et al.* [4] reviewed information-gap theory to model uncertainty. R. Venkataraman *et al.* [16] proposed Regression based trust model to compute trust and it is observed that nodes in network are able to observe malicious activities of their neighbor hence trustworthy paths can be taken in order to avoid data loss in the network. Kannan Govindan *et al.* [3] discussed different perspectives to design MENET. Reviewed properties which should be considered while developing trust matrix of MANET. Based on AHP and logic rules H. Xia *et al.* [17] presented new trust evaluation model. Fuzzy Trusted Dynamic Source Routing (FTDSR) protocol is proposed on the basis of fuzzy logic prediction method to obtain reliable route [17]. Number of experimentations have been done to check efficiency of protocol in identification of malicious nodes and attack resistance. T. Eissa *et al.* [18] proposed trust-based scheme for securing AODV routing protocol using friendship mechanism. Nodes itself can evaluate routing path based on parameters like node reputation and identity information to forward data through secure paths.

Performance of MANET is affected by several parameters like node mobility, node density, mobility model etc. Banoj Kumar *et al.* [19] discussed AODV and DSR routing protocols and impact of node mobility on MANET based on these protocols. Performance of MANET is sensitive to node density and node mobility[20]. It is observed that performance of MANET degrades with decrease in node density. Two protocols AODV and DSR are compared using node density and node mobility parameter under random waypoint model and random waypoint with attractions. Sandeep *et al.* [21] proposed opportunistic routing protocol to maintain smooth network performance in presence of selfish nodes. It is observed that opportunistic routing protocol helps to improve PDR in presence of selfish nodes. M. Virendra *et al.* [22] proposed trust-based security architecture for mobile ad-hoc networks. The impact of node mobility is considered during trust establishment.

Research contributions [20] [19] and [23] done to evaluate performance of network under different test conditions. Test conditions include parameters like node density, transmission packet size, mobility of node, pause time and speed of mobile nodes etc. It is done to evaluate performance of MANET without considering uncertainty of network. The efficiency of MANET is computed in terms of throughput, end to end delay, packet delivery ratio, normalizing routing load. In this work, to quantify trust and analyze uncertainty with respect to network parameters like network dimension, number of malicious nodes, speed and pause time of mobile nodes number of experiments performed.

## III. EVALUATING MANET UAF

This research work is done to analyze performance of MANET and trust-based routing By varying network dimen-

sions, number of malicious nodes, node speed of nodes, pause time of nodes.

To analyze performance of network by varying network dimensions, it is obvious that network dimensions and node density are inversely proportional. Therefore, it is interesting to analyze network uncertainty under diverse node densities. Performance of the network can be analyzed by varying malicious nodes. Malicious nodes show tendency to drop packets. However, uncertainty and packet dropping are closely related to each other [1]. Therefore, numbers of malicious nodes in the network have significant impact on BDU values.

Third test condition performed by varying node speed from minimum to maximum. As dynamic topology is characteristic of MANET, with varying speed of mobile nodes MANET topology becomes more uncertain. Uncertainty of MANET also analyzed by varying pause time of mobile node. If pause time is less many number of nodes come in contact with one another, hence it is necessary to evaluate and compare different protocol performance.

We are analyzing performance using five metrics. Packet Delivery Ratio (PDR), Average End to End delay (AE2E) and Normalizing Routing Load (NRL) measures routing protocol performance under different test conditions. Simulation parameters are given in Table I. Simulation results and analysis is discussed in next section. We have measured belief of the network at the end of simulation and over the time period for each test condition, Belief is the degree to which one node can depend on another to forward packet in the network. Disbelief is the inability of a node to forward packet. Uncertainty is the state of limited knowledge where it is not possible to predict the reliability of the MANET.

| **Parameter** | **Value** |
|---|---|
| Simulation Time | 500 sec |
| Grid Size | 1000 $m^2$ |
| Number of Nodes | 50 |
| Maximum Node Speed | 10 m/s |
| Number of connections | 20 |
| Mobility Model | Random waypoint mobility model |

TABLE I: Simulation Parameters

## IV. EXPERIMENTAL RESULTS

This section discusses experimental results in detail. Sub section IV.A describes experimental setup. Sub section IV.B describes observations and analysis under four different test conditions.

### *A. EXPERIMENTAL SETUP*

The NS-2.35 simulator is used to analyze performance of AODV, AODVCN, AODVIT. All experiments conducted on a computer having Ubuntu 12.04 operating system with 4 GB RAM and Intel Core i5 processor (3.2GHz). For wireless networks, IEEE 802.11g extension distributed coordination function is used in MAC layer of every node. Two ray ground propagation model was used with UDP at transport layer. All test conditions use Constant Bit Rate (CBR) traffic with number of connections equal to 20. Number of participating nodes are 50 having packet size 512 bytes.

### *B. OBSERVATIONS AND ANALYSIS*

#### *1) **Test Condition 1: Varying Dimensions of the Network**:*

Three protocols AODV, AODVCN, and AODVIT are used in the investigation of the performance of network by varying network dimensions. The network sizes used are 500, 700, 900, 1100, 1300 $m^2$. Fig. 1(a) shows Average End to End delay (AE2E) performance. AODVCN has delay approximately 1450 ms and AODV and AODVIT has approximately 810 ms and 1200 ms respectively. AE2E increases in proportion of the network size. A reason behind this behavior is that, as the network size increases, nodes get dispersed into a wider area and node density in network decreases. Therefore, time required to receive a packet at destination increases.

The performance is shown in Fig. 1(b) with increasing network size from 500 $m^2$ to 1300 $m^2$, the number of packets delivered using all three protocols decreases from approximately 70 to less up to 30. With increase in network size, packet forwarding behavior of node negatively gets affected. In this case, the performance of three protocols AODV, AODVCN, and AODVIT is constantly decreasing; AODVIT is performing best in large network sizes.

PDR of AODV is only approximately 25, which is not good. NRL for all the three protocols is directly proportional to network size. In higher dimensioned networks, nodes are following highest distances among them. As PDR decreases with increase in network size, this shows chances of packet loss with increase in network dimension. Therefore routing load increases because of retransmission of lost packets.

NRL of AODV is 7 routing packets per data packets and this requirement is greater than NRL of AODVCN and AODVIT because PDR of AODV is less and approximately 27. This suggests AODV has more packet drop. Therefore, more overhead generated to resend the packets which are dropped. After AODV, NRL of AODVCN is approximately 5 routing packets per data packet. The cause of higher NRL of AODVIT is due to flooding. To send recommendation packets to participating nodes, central node uses flooding. Large number of flooded packets increases control overhead. AODVIT has higher PDR hence very fewer packets are retransmitted. AODVIT uses indirect recommendations only from neighbor nodes; therefore, fewer packets are used. Considering PDR and indirect recommendation factors, from Fig. 1(c), NRL of AODVIT is always low.

The network belief (B) and disbelief (D) are inversely proportional to each other. The belief (B) values are recorded at the end of the simulation. At that point, uncertainty (U) is almost zero. Hence, we have not shown corresponding disbelief (D) and uncertainty (U) graphs. It is observed that BDU values are sensitive to the size of the network. From

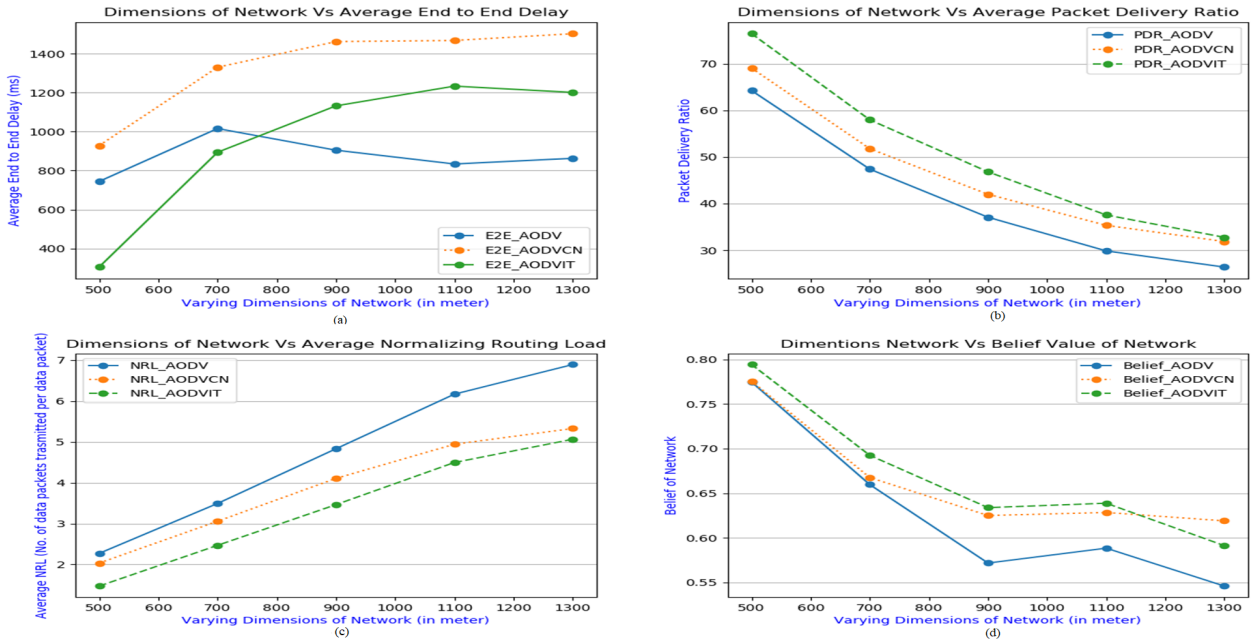


Fig. 1: Varying Dimensions of the Network

Fig.1(d), the Belief value of AODVIT is higher up to network dimension 1100 $m^2$. However, for network sizes up to 1100 $m^2$ AODVIT is performing best as it uses recommendations from the central node. After network size 1100 $m^2$ AODVCN is performing best with Belief approximately 0.63 than AODV having Belief approximately 0.54 and AODVIT having Belief 0.59. Because it uses recommendations from central node and in large-sized networks nodes are apart from one another. Hence Belief value of AODVIT decreased as the size of the network increased.

*2) **Test Condition 2: Varying Number of Malicious Nodes**:*

The network area of 1000 $m^2$ is simulated with 50 nodes. Nodes are free to move within the simulated area with a simulation time of 500 seconds. Initially, the number of malicious nodes was 0 and they are varied from 0 to 25. Malicious nodes behave as co-operative ones but actually, they drop packets intentionally in order to maximize their gain.

Fig. 2(a) shows an effect of varying number of malicious nodes on the AE2E performance of MANET. Initially, AE2E was less as there were only 50 nodes present. With an increase in malicious nodes from 0 to 50, node density increases. Therefore, the time required to deliver the packet from source to destination decreases. Hence AE2E decreased to approximately 110 ms for AODV and AODVIT. It is observed that AE2E of AODVCN is approximately 690 ms and observed higher than AODV (approximately 400 ms) and AODVIT (approximately 180 ms). Because AODVCN uses central node recommendation to forward packets to next available hop. Hence, packets are sent to only those nodes which are not malicious. Hence, the time required to send packets to destination increases.

PDR of AODVCN is approximately 31 which is better than AODV and AODVIT. AODVCN is using central recommendation to forward packets. Performance of AODVCN is better in the presence of malicious nodes. Due to more packet loss in AODV, PDR of AODV is very less and is observed approximately 25. Therefore, it is required to retransmit dropped packets in the network. Due to this reason, from Fig. 2(c), NRL of AODV is approximately 35 routing packets per data packets and this NRL is highest in all protocols. With the increase in malicious nodes, packet drop is more and flooding used in AODVCN has the drawback of packet duplication. Hence, when malicious nodes increased from 0 to 25, control overhead required for AODVCN is much higher (approximately 26 routing packets per data packets), results in increased NRL observed in Fig. 2(c). NRL of AODVIT is very less and equal to only 10 routing packets per data packets because it uses a recommendation from neighbor nodes and in case of AODVIT, packet drop is not greater than AODVCN hence overhead required to control traffic is less even in presence of 25 malicious nodes.

At the start of the simulation, the number of malicious nodes set to 0. Hence there is no packet drop hence the performance of all protocols is maximized. When malicious nodes are increased from 0, Belief values of every protocol gradually decreased from 0.74 to less than 0.5 Belief values of AODV decreases in proportion to the number of packets. Although the performance of AODVCN and AODVIT is fluctuating at alternative points of malicious nodes. By observing parameters such as high PDR, less AE2E and less NRL, when malicious nodes in the network are highest, the performance of AODVCN in terms of Belief is best with Belief value approximately 0.49. Malicious nodes drop packets which are supposed to forward hence network becomes defragmented

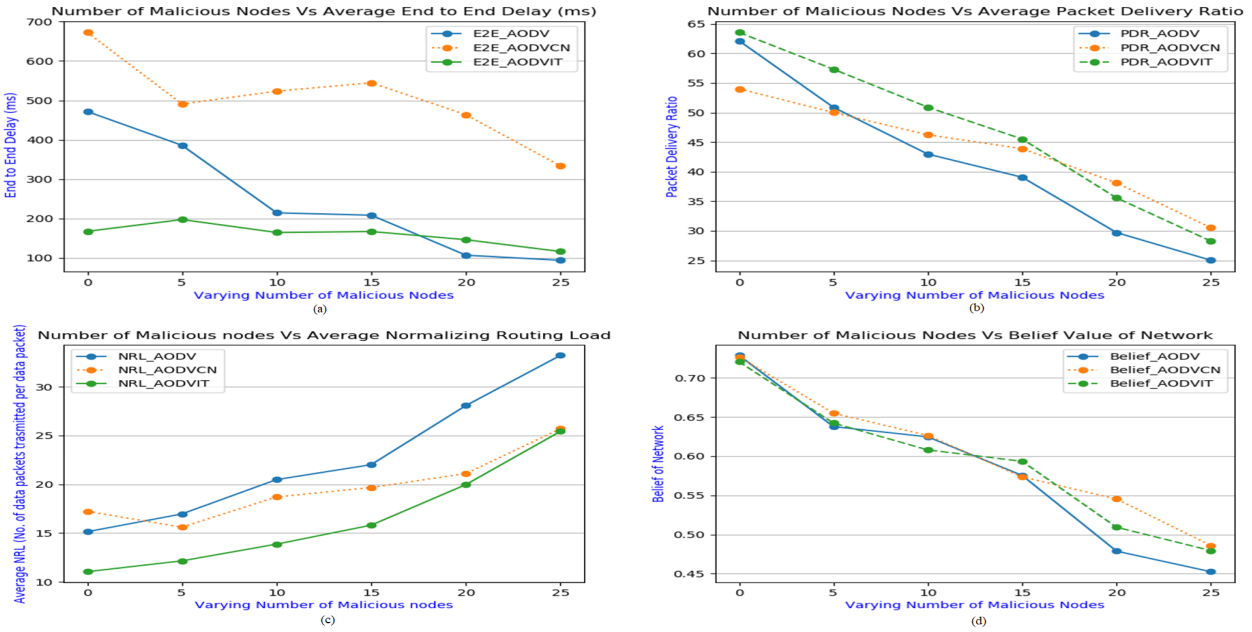


Fig. 2: Varying Number of Malicious Nodes

and Belief values decrease from approximately 0.75 to approximately 0.48 in presence of malicious nodes.

*3) **Test Condition 3: Varying Pause Time of Mobile Nodes**:*

In experimental methodology, the performance of the network can be measured with variation in pause time as 50, 100, 150, 200, 250 seconds while keeping rest of the parameters constant. As nodes in MANET are mobile, pause time is the short time period in which node is stationary in the network. Fig. 3(a) shows AE2E versus varying pause time of mobile nodes. Initially, the AE2E of AODVCN is highest (approximately 1450 ms) and behavior of AODVIT and AODV is similar when pause time is 250 seconds. When pause time is minimum, the topology of the network is very dynamic. Hence, nodes come in contact with each other for a very short period of time and route required to forward the packet for next hop changes continuously. Therefore, the value of AE2E increases. As the pause time increase from 50 ms to 250 ms, nodes become stable and route discovery becomes easy. Hence, as pause time of mobile node increases, in case of AODV and AODVIT, AE2E decreases to approximately 500 ms.

With the increase in pause time of mobile nodes, the network remains stable which leads to less packet loss. Therefore, pause time is directly proportional to packet delivery ratio. From Fig. 3(b), it is analyzed that performance of AODVIT is consistently better with PDR approximately 47. Because, when pause time increases, nodes become stable and AODVIT gets a recommendation from neighbor nodes which leads to less packet drop. Hence, at pause time 250 ms, the performance of AODVCN and AODVIT is almost same with PDR approximately 46. The performance of AODV is increasing from 33 to 39 with an increase in pause time but which is not good as compared to AODVCN (approximately 39 to 47) and AODVIT (approximately 42 to 47) because of packet loss. As AODVCN has a tendency of more packet loss, therefore retransmission of packet causes more NRL in AODV than AODVIT and AODVCN. Node stability decreases packet loss and increases PDR. Hence, NRL decreases approximately up to 3.0 gradually for all protocols.

From Fig. 3(d), Belief values of AODVCN and AODVIT are approximately 0.7 and 0.67 respectively which are highest. The performance of AODVIT is less than AODVCN because AODVIT depends more upon neighbor nodes to forward packets but when pause time is less, routes are continuously changing which causes network less stable. Initially, when pause time is 50, the network is very unstable. Therefore, Belief value of AODVIT is much smaller approximately 0.56 than AODVCN and AODV approximately 0.62. Belief value of AODV and AODVIT is continuously lower. Hence, it can be proved that AODVCN performs best even if the network is unstable and performance of trust-based routing protocols is positively affected by pause time of mobile nodes with Belief value approximately 0.61 to 0.68.

*4) **Test Condition 4: Varying Speed of Mobile Nodes**:*

While varying the speed of node, the most important two circumstances are route discovery and route maintenance. If the speed of node is too high, then it is difficult to maintain route between the nodes. Because of the instability of network, route discovery is significant. If the speed of node is less, there are chances of less route maintenance. With less route maintenance, the time required to send a packet to the destination is less hence AE2E is lower. As the speed

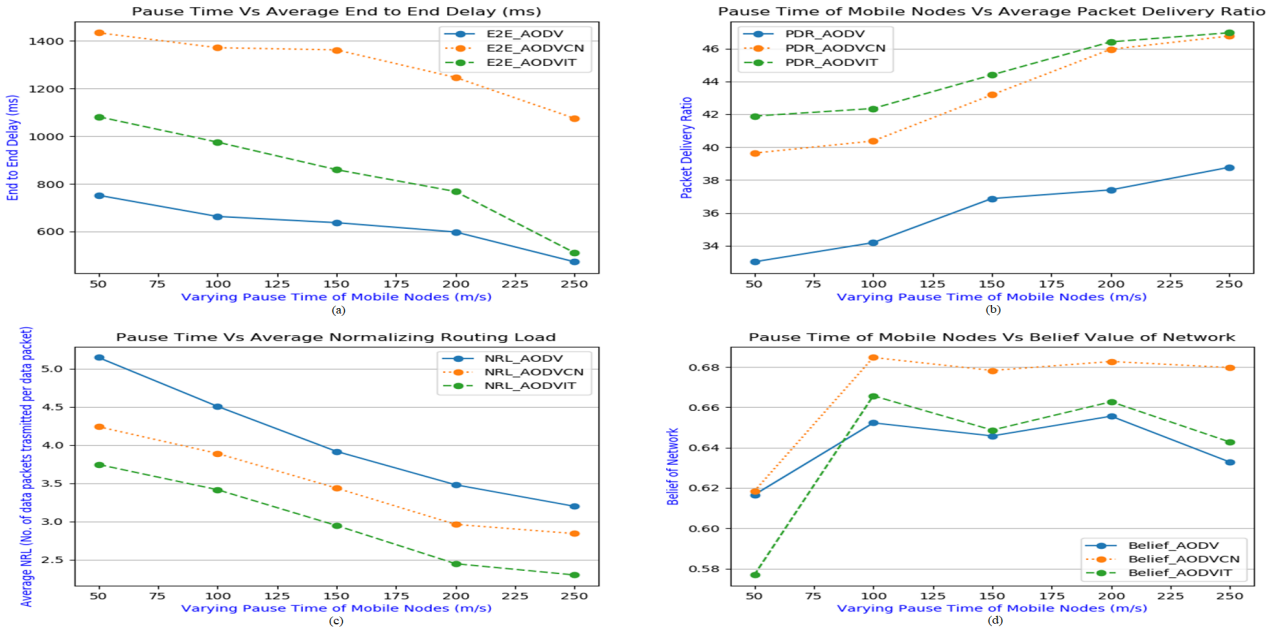


Fig. 3: Varying Pause Time of Mobile Nodes

of mobile node increases, routes are continuously changing. Therefore, AE2E increases.

From Fig. 4(a), it is observed that as initially nodes are stable because speed is almost zero. AE2E for all protocols is negligible. However, as speed increases, AE2E increases. When the speed of mobile nodes increases, AODVCN performs poor in terms of AE2E (approximately 900 ms) and AODVIT shows consistently best performance (AE2E approximately 10 ms). When the speed of node is less, routes are well maintained hence packet loss is rare. This behavior is observed in Fig.4(b). With an increase in speed (20 m/s), the degree of packet loss increases and PDR reaches to approximately 40. Up to the speed of mobile nodes 10 m/sec PDR of AODVCN is higher than AODVIT and performance of AODVIT yields better results after speed 15 m/sec. This is because as speed increases, number of nodes come in contact with each other and AODVIT uses neighbor node recommendations to forward packets. As PDR of AODV is less approximately 35, with an increase in speed of mobile node and retransmission of lost packets, NRL for AODV is increased up to approximately 27. However, protocol AODVIT shows the best performance in terms of PDR with initial speed 0.1 m/s, PDR value approximately 70.

Belief values of AODV, AODVCN and AODVIT are obviously affected by varying speed of nodes as it affects simulation parameters like PDR, AE2E, and NRL. As PDR of AODVCN is highest and there are fewer chances of packet loss, therefore AODVCN performs best when it is analyzed in terms of Belief value. Therefore, Belief value of AODVCN (approximately 0.54) is better than AODV and AODVIT (approximately 0.53).

*5) **BDU Analysis Over the Time Period**:*

The belief (B), disbelief (D) and Uncertainty (U) values are recorded over the simulation time period with network dimension network with size 900 $m^2$. BDU values are recorded after an interval of 70 seconds. Initially, the network is not matured but from simulation time 140 seconds, Belief and Disbelief values show significant impact on the performance of the network. From simulation time greater than 140 seconds, the network starts to exchange trust-based information among the nodes more certainly. Because at this point, the network becomes mature enough to calculate BDU values. Therefore, first two intervals are sufficient to monitor the behavior of the network. From Fig. 5(a), it is observed that, after network becomes mature, the performance of AODVCN and AODVIT is better with Belief approximately 0.63 than AODV. Conversely, Disbelief values Fig. 5(b) of AODV is higher than AODVCN and AODVIT. From Fig. 5(c), simulation time equal to approximately 140 seconds, Uncertainty values are consistently low and negligible. This is because after 140 seconds, as the network becomes mature its Belief and Disbelief values always grow opposite to each other and due to maturity of the network Uncertainty shows a sudden change in values from 0.25 to 0.01. Uncertainty value becomes almost zero for simulation time equal to 490 seconds. This indicates that Belief and Disbelief values become more certain with an increase in the time interval.

## V. DISCUSSION

### A. *Belief (B) analysis at the end of simulation*

The belief (B) values are measured using three trust variants. It is observed that BDU values affected by varying network dimensions. With the decrease in node density and increase in network dimension, nodes go far away from each other hence rather than neighbor recommendation (protocol AODVIT) global recommendation (protocol AODVCN)

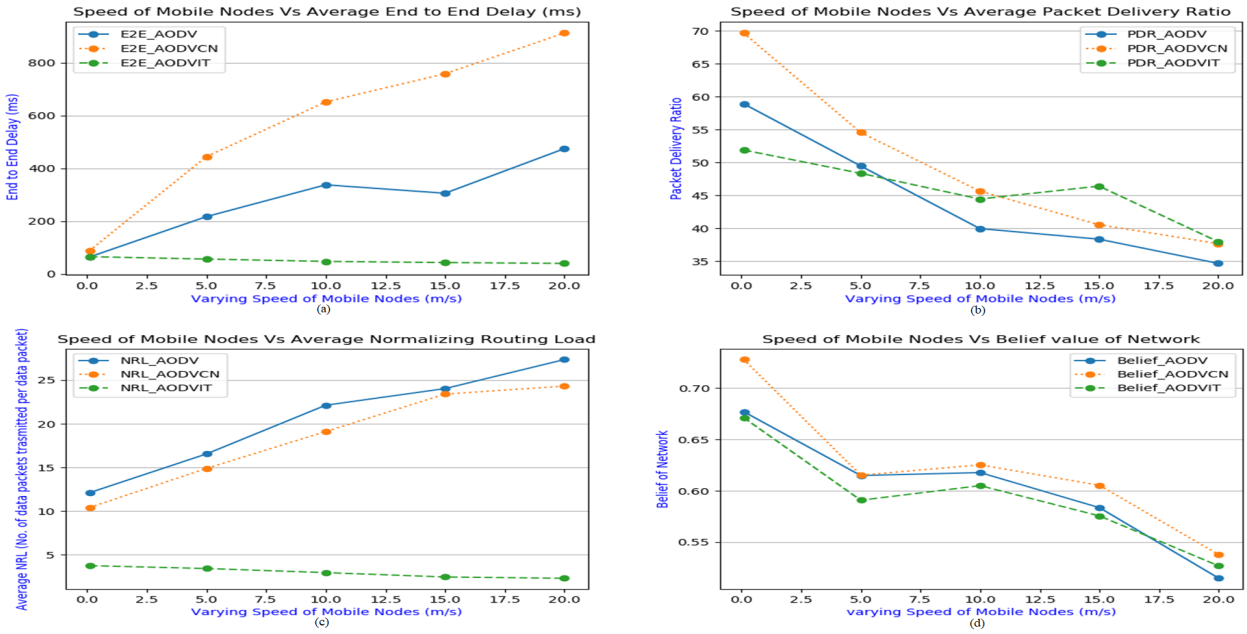


Fig. 4: Varying Speed of Mobile Nodes

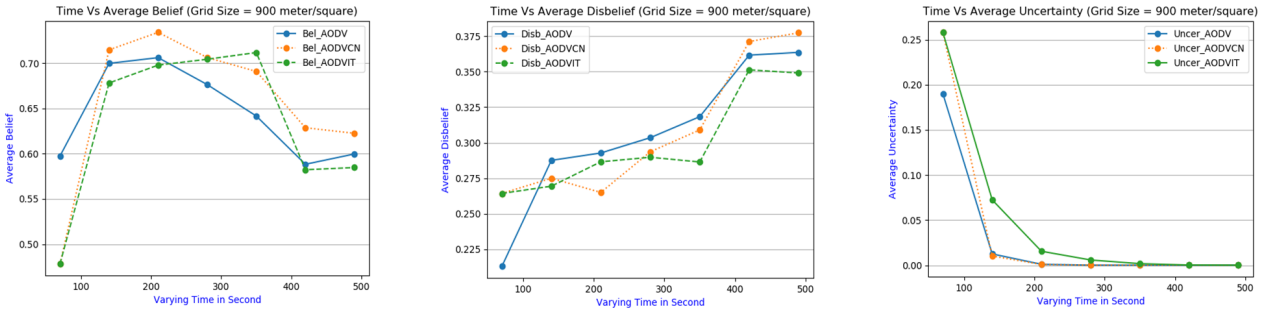


Fig. 5: BDU Analysis Over the Time Period

worked well in this scenario. Therefore, the network belief (B) of all protocols decreases from approximately 0.75 to approximately 0.55.

By varying number of malicious nodes, network belief (B) decreased because malicious nodes show the tendency to drop packets to maximize own gain. Central node gets evidence about all nodes from participating nodes, precisely, AODVCN is able to find malicious nodes more preciously than AODVIT. Hence the performance of AODVCN (Belief value approximately 0.49) is best in presence of malicious nodes.

AODVCN shows better performance with an increase in pause time with belief value approximately 0.68. AODVIT uses recommendations from neighbors and with an increase in pause time, less number of nodes come in contact with each other hence less recommendation received.

Although more nodes come in contact with each other by increasing speed of mobile nodes there is need of route discovery and route maintenance which is quite difficult in increased node speed. Therefore, AODVCN performs best (Belief value approximately 0.55) when node speed is 20 m/s.

### *B. BDU analysis at different time intervals*

Graph of Belief is always opposite to graph of Disbelief. It is observed that after the time period of 140 seconds effect of trust-based routing protocols can be seen in MANET. A period of 140 seconds is required for profiling of the network. After a time interval of 140 seconds, Uncertainty values show sudden degradation to reach value zero. From this point onwards, it is possible to define whether the network is co-operative or insecure.

### *C. Impact of trust-based routing protocols on MANET*

Performance of trust-based routing protocols shows 5% increase in the network belief than routing protocols. From simulation and analytical results, the performance of AOD-VCN observed best with 5% higher than the performance of AODV and AODVIT. The disadvantage of using central recommendation is single point failure.

## VI. CONCLUSION

The research work explored impact of Belief, Disbelief, and Uncertainty on MANET using trust based routing protocols. The research work does extensive evaluation of existing Uncertainty Analysis Framework (UAF) [1] using various test conditions. The AODV protocol integrated into trust variants viz. global trust (AODVCN) and indirect trust (AODVIT) to analyze the impact on the MANET.

It is observed that, performance of MANET is affected by varying network dimensions, number of malicious nodes, pause time of nodes and speed of nodes. It is found that, a time period of approximately 140 seconds is required to have mature values of Belief, Disbelief, and Uncertainty in a network. Trust based protocols show better performance after this time period; these protocols can clearly distinguish between good behaving and malicious nodes after the time period. UAF is able to categorize given network as cooperative or malicious after this time period.

The performance of AODVCN and AODVIT is analyzed under various test conditions. The simulation results show that belief (B) value of the network is 5% greater in AODVCN if compared with AODVIT. This emphasizes, global trust is effective than indirect trust. However, global trust mechanisms suffer with disadvantages like single point of failure, Bottleneck at the central node, and practical difficulty in deploying central node in distributed network like MANET. Hence, choice between global trust and indirect trust should be made after considering above factors. When pause time of mobile nodes is high and speed of nodes is less, then network is fairly stable. In such a network it is observed that, Belief of AODVCN and AODVIT yields approximately similar results.

## REFERENCES


[1] S. A. Thorat and P. J. Kulkarni, "Uncertainty analysis framework for trust based routing in manet," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1101–1111, 2017.

[2] S. A. Hosseini and H. Farrokhi, "The impacts of network size on the performance of routing protocols in mobile ad-hoc networks," in *Circuits, Communications and System (PACCS), 2010 Second Pacific-Asia Conference on*, vol. 1. IEEE, 2010, pp. 18–22.

[3] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[4] Y. Li, J. Chen, and L. Feng, "Dealing with uncertainty: A survey of theories and practices," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 11, pp. 2463–2482, 2013.

[5] V. Kumar and M. Schuhmacher, "Fuzzy uncertainty analysis in system modelling," in *Computer Aided Chemical Engineering*. Elsevier, 2005, vol. 20, pp. 391–396.

[6] N. Arunraj, S. Mandal, and J. Maiti, "Modeling uncertainty in risk assessment: an integrated approach with fuzzy set theory and monte carlo simulation," *Accident Analysis & Prevention*, vol. 55, pp. 242–255, 2013.

[7] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Hermes: A quantitative trust establishment framework for reliable data packet delivery in manets," *Journal of Computer Security*, vol. 15, no. 1, pp. 3–38, 2007.

[8] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 640–651.

[9] F. Li and J. Wu, "Mobility reduces uncertainty in manets," in *INFOCOM 2007. 26th IEEE International conference on computer communications. IEEE*. IEEE, 2007, pp. 1946–1954.

[10] ——, "Uncertainty modeling and reduction in manets," *IEEE transactions on mobile computing*, vol. 9, no. 7, pp. 1035–1048, 2010.

[11] Y. Cong, X. Zhou, and R. A. Kennedy, "Interference prediction in mobile ad hoc networks with a general mobility model," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4277–4290, 2015.

[12] A. Choudhary, O. Roy, and T. Tuithung, "Node failure effect on reliability of mobile ad-hoc networks," in *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*. IEEE, 2014, pp. 207–211.

[13] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4647–4658, 2014.

[14] J. Pearl, "Bayesian and belief-functions formalisms for evidential reasoning: a conceptual analysis," in *Readings in uncertain reasoning*. Morgan Kaufmann Publishers Inc., 1990, pp. 540–574.

[15] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1*. ACM, 2002, pp. 294–301.

[16] R. Venkataraman, M. Pushpalatha, and T. R. Rao, "Regression-based trust model for mobile ad hoc networks," *IET Information Security*, vol. 6, no. 3, pp. 131–140, 2012.

[17] H. Xia, Z. Jia, L. Ju, X. Li, and E. H.-M. Sha, "Impact of trust model on on-demand multi-path routing in mobile ad hoc networks," *Computer Communications*, vol. 36, no. 9, pp. 1078–1093, 2013.

[18] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in manet: Design and implementation," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 666–677, 2013.

[19] B. K. Panda, B. Dash, R. Das, and A. Sarangi, "Mobility and its impact on performance of aodv and dsr in mobile ad hoc network," in *Internet (AH-ICI), 2012 Third Asian Himalayas International Conference on*. IEEE, 2012, pp. 1–5.

[20] K. Amjad and A. J. Stocker, "Impact of node density and mobility on the performance of aodv and dsr in manets," in *Communication Systems Networks and Digital Signal Processing (CSNDSP), 2010 7th International Symposium on*. Ieee, 2010, pp. 61–65.

[21] S. A. Thorat and P. J. Kulkarni, "Opportunistic routing in presence of selfish nodes for manet," *Wireless Personal Communications*, vol. 82, no. 2, pp. 689–708, 2015.

[22] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying trust in mobile ad-hoc networks," in *Integration of Knowledge Intensive Multi-Agent Systems, 2005. International Conference on*. IEEE, 2005, pp. 65–70.

[23] N.-U. Park, J.-C. Nam, and Y.-Z. Cho, "Impact of node speed and transmission range on the hello interval of manet routing protocols," in *Information and Communication Technology Convergence (ICTC), 2016 International Conference on*. IEEE, 2016, pp. 634–636.