International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

TASM: Trust Aware Scheme for Secure and Reliable Data Transmission in MANETS

Lata B T, Venugopal K R

Abstract*: Wireless sensor nodes are tiny and have limited battery and memory. These sensor nodes are distributed and self organizing networks. Mobile Ad Hoc network (MANETs) has wide range of applications areas. Growing usage of MANETs in various applications makes a paramount issue in providing QoS. MANETs are vulnerable to different kinds of malicious attacks due to its dynamic nature, which affects nodes connectivity, increase in energy consumption and functionality. Centralized and cryptographic security approaches requires more computational functions which increases overhead. Traditional approaches have more overhead. Most existing trust-based security schemes for mobile ad-hoc networks (MANETs) consider packet loss an indicator of possible attacks by malicious nodes. Thus to achieve secure and reliable data transfer a trust aware scheme is required to evaluate trust level among honest and malicious nodes. In this paper we propose Trust Aware Scheme for Moving nodes (TASM) which discovers efficient node by computing each node's trust value. In this scheme moving nodes exchange their trust information and analyses the received trust value and makes judgement. This scheme modifies the existing AODV routing protocol and determines malicious nodes based on trust value and log information. Received Signal Strength Indicator (RSSI) determines efficient and trusted neighbour node selection while routing. Proposed scheme is compared with the existing trust based scheme and network parameters like throughput, packet delivery ratio and end to end delay is evaluated. Trusted routing can efficiently deliver data for different routing applications used in military, Fanets and mobile IoT.

***Keywords* : Malicious, MANETs, Secure, QoS, RSSI, Trust based routing,**

I. INTRODUCTION

With wide and rapid development of smart computing applications of wireless technology, researchers are more emphasizing on wireless sensor network (WSN) for industrial, agriculture, military and environment monitoring [1-5]. Mobile Ad-hoc network (MANET) has led to the growth of mobile devices. These networks consist of mobile nodes that communicates through wireless channel without any infrastructure. Dynamic and self organizing characteristic enables MANETs to move from one network to another. MANET's nodes are responsible to transfer data and can join or leave the network without any constrain. However due to its dynamic nature, MANET's causes frequent changes in topology in an unpredictable way [6-8]. Mobile nodes are limited to power and transmission range hence each node has to seek assistance of its neighbour nodes and transfer data in multihop transmission. Due to absence of centralized administration, MANET's require secure data transmission through authentic cooperation nodes to achieve reliable routing. Most of the researches have been conducted on efficient MANET's routing by assuming node's cooperation and trustworthiness [9]. However most of the schemes are vulnerable to attacks which disrupt the network when a malicious node tries to misbehave while forwarding data. Due to lack of secure information sharing between trusted and non-trusted nodes leads to attacks.

Motivation of this work is based on analysis of node behavior by computing trust value which reflects honest or malicious while data transmission through multihop. Consider an example of node being abnormal which injects corrupted data and degrades the network performance. By designing trust aware scheme framework for any application scenario will improve network performance and mitigates attacks.

Hence to evaluate trustworthiness and secure information sharing among nodes needs to be formalised. Trust management scheme provides secure MANET's environment and creates trust level among nodes for decision making [10-16]. In order to secure nodes from attacks in this paper we propose trust aware scheme for secure data transmission in MANET's. In this scheme every node computes the trust level degree of other nodes independently and maintains log of stable route maintenance information. On other hand nodes share their trust results with neighbours to perform effective cooperation to get information about trusted and non-trusted nodes. Major contributions of this paper are:

- Modification to existing AODV routing protocol, since this protocol updates neighbour log information sequentially but fails to update location information during connect establishment of moving nodes.
- RSSI estimates distance and selects efficient trusted neighbour selection within the transmission range.
- Develop generic trust scheme which can be easily integrated to routing protocol, this scheme prevent attacks by periodically updating the trust values of neighbour nodes through location information.

Manuscript received on April 02, 2020.
Revised Manuscript received on April 20, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Dr. Lata B T*, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India.. Email: lata_bt@yahoo.co.in
Dr. Venugopal K R, The Vice Chancellor, Bangalore University, Bengaluru. India

The rest of this paper is structured as follows. Section 2 describes the related works carried on various security threats, mechanisms and their disadvantages. Network model is discussed in the Section 3. Proposed trust scheme is explained in the section 4.

The performance analysis and relative simulations are depicted in the section 5. Finally, we draw the conclusion on the proposed scheme in section 6.

II. RELATED WORKS

Secure routing is a vital role in achieving network performance. Most of conventional secure scheme consists of cryptographic tools [17-20] to mitigate intruder from launching attacks. These schemes are mostly controlled by centralized or third party network. However, it is invalid for MANET's. These secure routing has disadvantage in identifying passive attacks such as blackhole and greyhole. Hence trust based routing approaches have become popular to ensure secure routing in MANET's. Reputation based schemes are designed for cooperative routing to distinguish between malicious and honest nodes, these scheme involves trust computation to evaluate relation between two nodes. In [21] author proposed secure AODV routing to detect malicious node through local observations and statistic report generated for each peer nodes behavior. In [22] author proposed architecture for trust based management for MANET's. This scheme considers trust level computed physically and logically for each node. In [23] author proposed trust value evaluation through random graph theory and dynamic cooperative game. In [24] proposed misbehaving node detection scheme using trust authority (TA) which detects malicious nodes through probabilistic and judges the nodes through evidence probability check and predicts the authentic and malicious nodes.

In [25] proposed secure trust based routing through Advance encryption standard (AES), this scheme is modelled using dolphin cat optimizer for improving network lifetime. The optimal route selection is done on basis of trust factors like direct trust, delay, distance and link estimation. However, this scheme consumes more communication overhead while computing encryption functions. In [26] author proposed trust evidence scheme using game theory in WSN. This scheme achieved network security and energy saving through clustering based routing.

III. NETWORK MODEL

We consider a set of mobile nodes which can freely move in a certain range within the network. AODV routing protocol is adopted for discovering the route and maintenance. The source node having data to be sent to the destination will initiate Route Request Message (RREQ) and keeps broadcasting to neighbour nodes for shortest path. Neighbour nodes replies to source with Route Reply (RREP) message for data transmission. If any link failure is detected by the node it triggers route maintenance by generating route error (RERR) to source node. Malicious nodes are induced into network, which does misbehaving and drops the packets. Trust model evaluates the trust level of nodes while communicating and detects honest and malicious nodes in network.

IV. PROPOSED TRUST SCHEME (TASM)

Packet drop in MANET's can be due to congestion, link failure or due to low energy and by malicious node. When the node is malicious, it deliberately drops the packet without forwarding to its neighbour and we define it as attacker node. Efficient neighbours are selected using below algorithm

A. Neighbour Selection Algorithm

Input: Network graph of node (N) of $G = (V, E)$

Output: Trust value $(TV)_i$

1. Generate neighbour node list using distance equation given below
   $\boldsymbol{Distance}_{a,b} = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$.
2. Get log info of specific node $log_{(N_i)}$
3. Check the sequence ID from log info of nodes.
4. $for\ i = 0 \ldots . n$ then, where n is number of nodes
5. Calculate signal strength of source node to the current node i by $S_i = RSSI(N, G_i)$ [27] where G_i is ith node in graph .
6. $if\ (S_i < Range)$ then.
7. $P_{ID_{N_i}}$ = Packet ID from log info $log_{(N_i)}$.
8. $if\ P_{ID_{N_i}} == P_{ID_{N_{i+1}}}$
9. Compute trust value $(TV)_i$
10. Else
11. Return to 1
12. end if.

B. Trust Evaluation

To evaluate trust operation, each node broadcast Hello packets within its transmission range frequently for neighbour discovery. This packet contains sender's information and ID, with exchanging of Hello packets each node can get to know ID's of its neighbour within range in timely manner. Each node maintains following information log:

- Sending packet information log, which contains number of packets generated or sent through specific path.
- Receiving packet information log, which contains number of packets received at destination through specific path.
- Cooperative information log, this file contains the cooperative and uncooperative nodes information through trust computation.
- Neighbour list information log, which contains list of neighbour nodes and their ID's
- Trust information log, which contains trust values of nodes.

C. Direct trust

In direct trust calculation distribution probability ^{b} density function is used. The ^{b} represents probability of good and bad events. The beta (a, b) is a continuous probability distribution on interval $(0,1)$ $0 < p < 1$. The probability density is given as:

$\frac{p^{(\alpha-1)}(1-p)^{(\beta-1)}}{B(\alpha,\beta)}$ Where α and β are positive parameters. (1)

For random variable p and $B(\alpha,\beta)$ can be given as:

$$B(\alpha,\beta) = \frac{\Gamma(\alpha)+\Gamma(\beta)}{\Gamma(\alpha+\beta)} \quad (2)$$

The expected value for random variable p for beta distribution can be computed as :

$$E(p) = \frac{\alpha}{(\alpha+\beta)} \quad (3)$$

Variance of random variable p for beta distribution can be computed as:

$$V(p) = \frac{\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2} \quad (4)$$

The b distribution probability is simple to use, this distribution has two parameters (a,b) for random variable p which has a value between 0 and 1 and can be used as Bayesian statistics modelling to evaluate network related events like trust value, number of packets delivered and nodes mobility. If the node A has log information about honest node and malicious node behaviour of B. The honest behaviour and malicious behaviour is represented as α and β. The trust value using b distribution probability can be given as :

$$f(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)} p^{(\alpha-1)}(1-p)^{(\beta-1)} \quad (5)$$

Where $0 \le p \le 1, \alpha,\beta > 0$ with variance probability $p \neq 0$ if $\alpha < 1$ and $p \neq 1$ if $\beta < 1$

The direct trust can be given as:

$$E(p) = \alpha/(\alpha+\beta) \quad (6)$$

Each node computes trust values of its neighbour node and stores into information log files. α and β represents honest and malicious node behaviour. Each node is set a trust value of 0.5 under direct trust.

D. Indirect Trust

Indirect trust can be computed using Dempster shaft theory [28,29] which computes three indirect observations is given as :

$n = (trust), \bar{n} = (untrust), U = (trust\ or\ untrust)$

If node N_a observe node N_b as trusted node is given as:

$T(n) = E(p)$

$T(\bar{n}) = 0$

$T(U) = 1 - E(p)$

If node N_a observe node N_b as untrusted node is given as:

$T(n) = 0$

$T(\bar{n}) = 1$

$T(U) = 1 - E(p)$

V. SIMULATION AND PERFORMANCE ANALYSIS

Performance analysis of our proposed TASM scheme is compared with existing trust based routing protocol like TSRF [23] and reputation based trust scheme RBT [24] using event driven simulation tool NS2. The trust value is calculated based on the behaviour of the node and the information log. Each node collects node information log periodically and computes the direct trust using b distribution probability and predicts honest and malicious nodes efficiently. The parameters used for simulation are depicted in the Table 1.

Table- I: Simulation parameters

Simulation Parameters	Value
Network area	600x600
Node Deployment	Random
No of nodes	50
No of Malicious node	5
Mac layer	802.11
Transmission range	250mts
Traffic	CBR
Simulation time	100 sec
Initial energy	100J
Packet size	512bytes
Mobility speed	10m/s

A. Throughput

It is the percentage of packets accepted by the destination node to the packets delivered by the source node for every second. Throughput can be given as:

$$Throughput = \frac{m_1}{m_2} * 100\%$$

where m_1 packet received at destination and m_2 is packet sent from source, throughput is measured in kbps. The Figure 1 shows the comparison of our scheme TASM with TSRF and TSR. When the network is free from malicious, all the schemes achieves good throughput, when the malicious nodes are introduced it can be seen the throughput of TSRF and RBT decreases gradually with increase in malicious node. Our scheme outperforms TSRF and RBT in presence of malicious node and detects malicious behaviour and tries to route it through trusted neighbour thus delivering more packets to destination.

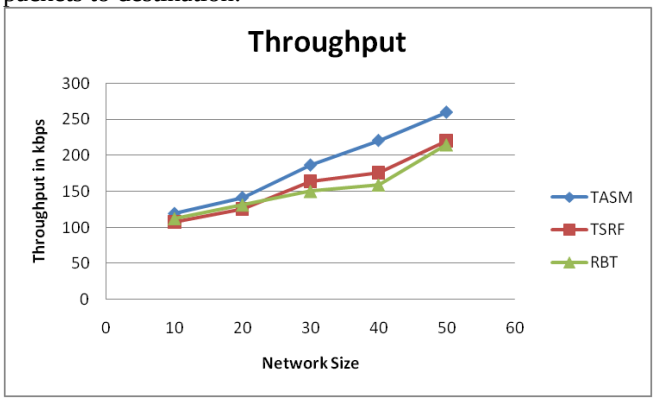

Fig. 1. Throughput graph

B. Packet Delivery Ratio (PDR)

PDR is the percentage of summation of data packets generated by summation of packets received.

$$PDR = \frac{Number\ of\ data\ packets\ received}{Number\ of\ data\ packets\ sent} * 100\%$$

Since trusted nodes process the packets, the node's buffer will not be occupied with more packets such that the packet gets processed faster with less time interval. Malicious nodes intentionally drop the packet and decreases PDR, our scheme TASM detects malicious nodes by computing trust value and routes the data packet reliably compared to TSRF and RBT. Figure 2 shows the packet delivery graph.

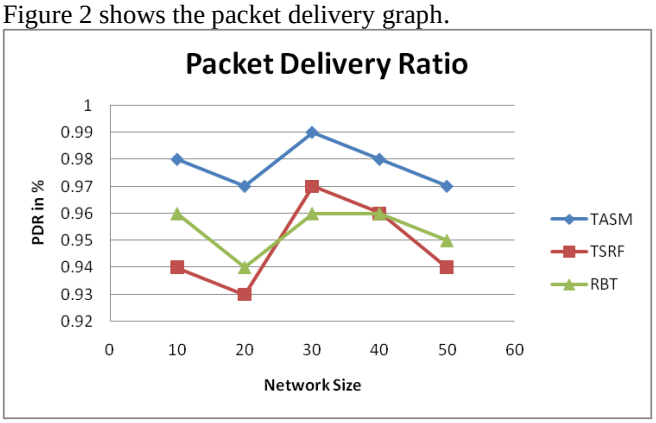

Fig. 2. PDR graph

C. Average end-to-end delay

It is a mean time, the difference between source and destination. It is calculated as packet sent time minus packet arrival time. It also includes route discovery delay process and queue processing while data transmission. It can be expressed as:

$$\sum (T_1 - T_2)/N$$

Where, T_1 is the arrival time of first packet to the destination and T_2 is the time at which, first packet sent from source and N is the summation of packets sent. The average end to end delay is depicted in Fig. 3. TASM discovers reliable and honest node while routing data and delivers packet with less interval time compared to TSRF and RBT.

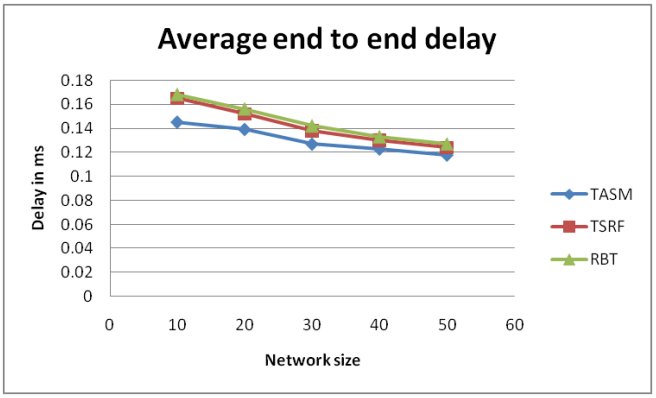

Fig. 3. Delay graph

D. Routing overhead

It is a summation of control packets or routing packets generated by total number of received packets. It is crucial part while designing routing protocol and proportional to PDR and throughput. The Routing overhead is conveyed as:

$$Routing\ overhead = \frac{N_1}{N_2}$$

Where, N_1 represents the routing packets dispatched and forwarded. N_2 is the received data packets. The overhead of the proposed scheme is illustrated in Fig. 4. It can be observed that TASM has low routing overhead as it selects trusted nodes for reliable routing compared to TSRF and RBT.

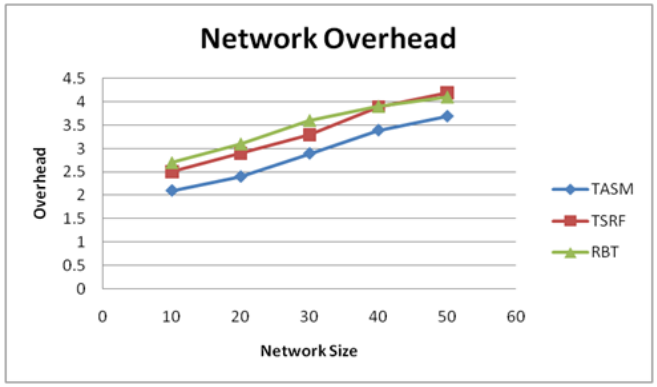

Fig. 4. Network overhead graph

VI. CONCLUSION

In future MANET's applications will have great revolution in smart computing. Mobile ad hoc networks (MANETs) are self-configuring, dynamic networks in which nodes are free to move. These nodes are susceptible to various malicious attacks Securing the data from intruder has to be solved for reliable data transmission. In this paper we propose trust aware scheme for moving nodes (TASM) which discovers efficient node by computing each node's trust value. In this scheme moving nodes exchange their trust information and analyses the received trust value and makes judgement. RSSI selects the trusted nodes within the transmission range for reliable routing This scheme can be easily integrated to routing protocol, this scheme prevents attacks by periodically updating the trust values of neighbour nodes through location information. Simulations were performed using NS-2 to analyze the functionality and performance of the TASM and compared with TSRF [23] and RBT [24] and performance analysis shows our scheme outperforms throughput, delay and packet delivery ratio. Proposed ahead work to achieve QoS requirements with cross layer routing approach by selecting potential nodes to support multipath routing considering link quality and minimum path interference can be considered which is essential for MANET routing

REFERENCES

1. P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, ``Wireless Sensor Networks: A survey on recent developments and potential synergies," *J. Supercomput.*, vol. 68, no. 1, pp. 1-48, 2014.
2. B. Rashid and M. H. Rehmani, ``Applications of Wireless Sensor Networks for Urban Areas: A Survey," *J. Netw. Comput. Appl.*, vol. 60, pp. 192-219, Jan. 2016.
3. J. Granjal, E. Monteiro, and J. S. Silva, ``Security in the Integration of Lowpower Wireless Sensor Networks with the Internet: A survey," *Ad-Hoc Netw.*, vol. 24, pp. 264-287, Jan. 2015.
4. M. A. Mahmood, W. K. G. Seah, and I. Welch, ``Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead," *Comput. Netw.*, vol. 79, pp. 166-187, Mar. 2015.
5. C. E. Perkins, E. M. Belding-Royer, and S. R. Das, Ad-hoc On Demand Distance Vector Routing: IETF RFC 3561, July 2003.
6. W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, ``A Resilient Trust Management Scheme for Defending Against Reputation Time-varying Attacks Based on BETA Distribution," *Sci. China Inf. Sci.*, vol. 60, no. Article number: 040305, 2017.

7. J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, ``Location-based Key Management Strong Against Insider Threats in Wireless Sensor Networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 494-502, Jun. 2017.
8. F. Ishmanov and Y. B. Zikria, ``Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues,"*J.Sensors*, vol. 2017, 2017, Art. no. 4724852, doi:10.1155/2017/ 4724852, 2017.
9. D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, ``Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," *IEEE Access*, vol. 5, pp. 9599-9609, 2017, doi: 10.1109/ ACCESS.2017.2706973.2017
10. A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, ``Energy-aware and Secure Routing with Trust for Disaster Response Wireless Sensor Network," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 216-237, 2017.
11. V. R. S. Dhulipala and N. Karthik, "Trust Management Technique in Wireless Sensor Networks: Challenges and Issues for Reliable Communication: a Review," CSI Transactions on ICT, vol. 5, no. 3, pp. 281–294, Sep 2017.
12. T. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR): IETF RFC 3626, October 2003.
13. [13] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR): IETF RFC 4728, February 2007.
14. D. Djenouri, L. Khelladi, and A. N. Badache, "A Survey of Security Issues in Mobile Ad-hoc and Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 7, pp. 2-28, 2005.
15. Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust- Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 18, pp. 1287-1309, 2016.
16. A. A. Pirzada and C. McDonald, "Secure Routing Protocols for Mobile Ad Hoc Wireless Networks," in Advanced Wired and Wireless Networks, Boston, MA: Springer US, 2005, pp. 57-80.
17. M. G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," in Proc. of ACM WiSe'02, Atlanta, GA, 2002, pp. 1-10.
18. Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a Secure On-demand Routing Protocol for Ad Hoc networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
19. Wang, X.; Liu, L.; Su, J. Rlm: A General Model for Trust Representation and Aggregation. IEEE Trans.Serv. Comput. 2012, 5, 131–143.
20. Virendra, M.; Jadliwala, M.; Chandrasekaran, M.; Upadhyaya, S. Quantifying Trust in Mobile Ad-hoc Networks. In Proceedings of the IEEE International Conference on Integration of Knowledge IntensiveMulti-Agent Systems, Waltham, MA, USA, 18–21 April 2005; pp. 65–71.
21. Jiang, T.; Baras, J.S. Cooperative Games, Phase Transition on Graphs and Distributed Trust in MANETs.In Proceedings of the 43th IEEE Conference on Decision and Control, Nassau, Bahamas, 14–17 December2004; pp. 93–98.
22. Zhu H, Du S, Gao Z, Dong M, Cao Z (2014) A Probabilistic Misbehavior Detection Scheme Toward Efficient Trust Establishmentin Delay-tolerant Networks. IEEE Trans Parallel Distrib Syst 25:22–32
23. J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, ``TSRF: A Trust-aware Secure Routing Framework in Wireless Sensor Networks," Int. J. Distrib. Sensor Netw., to be published, doi: 10.1155/2014/209436.2014.
24. Banerjee A, Neogy S, Chowdhury C (2012) Reputation Based Trust Management System for MANET. In: Third International Conference on Emerging Applications of Information Technology (EAIT), pp 376–381
25. Moresh Madhukar Mukhedkar, Uttam Kolekar, "Trust-Based Secure Routing in Mobile Ad Hoc Network Using Hybrid Optimization Algorithm," The Computer Journal, Volume 62, Issue 10, October 2019, Pages 1528 1545, https://doi.org/10.1093/comjnl/bxz061
26. L. Yang, Y. Lu, S. Liu, T. Guo and Z. Liang, "A Dynamic Behavior Monitoring Game-Based Trust Evaluation Scheme for Clustering in Wireless Sensor Networks," in IEEE Access, vol. 6, pp. 71404-71412, 2018.
27. Saadoune M, Hajami A, Allali H, "Distance's Quantification Algorithm in AODV protocol," Int. Journal Computer Science, Information Technology, 6(6):177–188, (2014).
28. Dempster, A.P. A Generalization of Bayesian Interface. J. R. Stat. Soc. **1968**, 30, 205–447.
29. Shafer, G. A Mathematical Theory of Evidence; Princeton University Press: Princeton, NJ, USA, 1976.

AUTHORS PROFILE

Dr. Lata B T is an Assistant Professor in the Department of Computer Science and Engineering at University Visvesvaraya College of Engineering. Bangalore University, Bengaluru, India. She obtained her B.E in Computer Science and Engineering from Karnataka University, Dharwad and M.Tech degree in Computer Network Engineering from Visvesvaraya Technological University, Belgaum. Ph.D degree in the area of Wireless Sensor Networks from Bangalore University. Her research interest is in the area of Sensor Networks, IOT and Image processing.

Dr. Venugopal K R, is currently the Vice Chancellor, Bangalore University, Bengaluru. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology,
Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE and ACM Distinguished Educator.