International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 2, April 2020, pp. 1592~1598
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i2.pp1592-1598

Trust-based secure routing against lethal behavior of nodes in wireless adhoc network

JyotiNeeli[1], N. K. Cauvery[2]
[1]Department of Information Science and Engineering, Global Academy of Technology, Bengaluru, India
[2]Department of Information Science and Engineering, RV College of Engineering, Bengaluru, India

Article Info

Article history:

Received Apr 20, 2019
Revised Oct 12, 2019
Accepted Oct 22, 2019

Keywords:

Analytical model
Probability
Secure routing
Trust management
Wireless sensor network

ABSTRACT

Offering a secure communication in wireless adhoc network is yet an open-end problem irrespective of archives of existing literatures towards security enhancement. Inclination towards solving specific forms of attack in adhoc network is majorly seen as an existing trend which lowers the applicability of existing security solution while application environment or attack scenario is changed. Therefore, the proposed system implements an analytical secure routing modeling which performs consistent monitoring of the malicious behaviour of its neighboring node and formulates decision towards secure routing by the source nodes. Harnessing the potential ofconceptual probabilistic modeling, the proposed system is capable as well as applicable for resisting maximum number / types of threats in wireless network. The study outcome show proposed scheme offer better performance in contrast to existing secure routing scheme.

Corresponding Author:

JyotiNeeli,
Department of Information Science and Engineering,
Global Academy of Technology,
Bengaluru, India.
Email: jyotirneeli@gmail.com

1. INTRODUCTION

Wireless Adhoc Network is suitable for the decentralized architecture deployment in wireless network [1]. Owing to the decentralized scheme, there are various challenges associated with the communication. Majority of the challenges are either associated with data forwarding / traffic related operation while other forms of problems are related to security problems in wireless adhoc network [2-5]. At present, there are many security schemes evolved toward secure applications of wireless adhoc network [6-10], but very few approach towards safeguarding the generalized architecture of wireless adhoc network. It is because the applications of the wireless adhoc network are very much different from each other in communication protocol perspective, therefore, the applicability of security solution of one application is never applicable to solve same security problem in another application. For an example, a same security solution cannot be offered towards securing black hole attack in mobile adhoc network and wireless sensor network as their routing management system is very different from each other. Various encryption-based schemes have been evolved up for secure routing scheme but there are very less studies with benchmarked outcomes in this regards. Hence, there is a need of such a security solution that offers security solution on the basis of the malicious behavior of the adhoc nodes which works on arena of all applications in wireless adhoc network. Therefore, the proposed system introduces a simplified analytical model that is meant for taking dynamic decision on the basis of current local and global trust in order to assess the intention of the nodes present in the network. The current work also presents a probabilistic modeling towards assessing various critical situations of the threats. The organization of the proposed manuscript is as follow: Section 2 discusses about the existing research work followed by problem identification in Section 3. Section 4 discusses about proposed methodology followed by elaborated discussion of algorithm implementation in Section 5. Comparative analysis of accomplished result is discussed under Section 6 followed by conclusion in Section 7.

Different variants of approaches has been evolved towards the securing the communication system in wireless adhoc network [11]. Most recently, a predictive scheme has evolved up towards securing applications of wireless adhoc network using neural network. The work was carried out towards resisting man-in-middle attack. Similarly, study towards resisting flooding attack has been carried out by Zant and Yasin [12] by incorporating isolation based scheme towards adversary on frequently used on-demand routing scheme. Adoption of similar routing scheme has been also carried out by Vadavi et al., [13] towards resisting black hole attack. The work carried out by Sekaran and Parasuraman [14] have deployed a cryptographic scheme for performing secure routing considering the mobility aspect of the wireless adhoc network. Study towards detection of identity-based intrusion was carried out by Faisal et al., [15] where the focus was offered towards resisting Sybil attack as well as replication attack. Usage of genetic algorithm as well as detection using bait has been carried out using Nithya et al., [16] using simulation-based study. Study towards trust modeling as a mechanism towards secure communication system has been carried out by Alnumay et al., [17]. Usage of cryptographic measure towards securing the routing scheme has been carried out by Babu et al., [18]. Existing system also witness the usage of key management considering the mobility as well as multicast tree-management as seen in the work of Madhusudhan et al., [19] and Zhang et al. [20]. Study towards joint addressing of the energy as well as trust-based factors has been carried out by Gong et al., [21]. Attack (gray and blackhole) specific solution was also discussed in work of Ahmed and Hussain [22] and Sibichen & Sreedhar [23]. Various other security schemes has been also discussed by Malhotra et al., [24], Das et al., [25], Esfandi et al., [26] and Sumathy and Kumar [27]. There are also studies carried out reviewing the existing security approaches in adhoc network (Chandan and Mishra [28], Moudini et al., [29], Wu and Liaw [30]). Neeli and Cauvery [31, 32] have reviewed existing security issue as well as focused about structure for gathering the intruders by using Zombie node. Although, various schemes have been evolved up towards secure routing in wireless adhoc network, there is lesser number of standard approaches being carried out towards offering potential secure routing.

After reviewing the work carried out towards the secure communication in the wireless adhoc network, it was seen that majority of the work carried out is towards addressing particular security breach which loses its applicability towards resisting other forms of attacks. It was also noticed that there are less quantity of research work being carried out towards addressing security problems in wireless adhoc network; however, there are some good number of work addressing specific application of it. There is few studies where attack resistivity strategy is developed on basis of generalize or complex malicious behavior. Therefore, the research problem is "*Developing a resistivity against maximum attack using cost effective modeling approach in wireless adhoc network using the unique characteristics of malicious behavior.*"

2. PROPOSED METHODOLOGY

The proposed study consider analytical research methodology in order to investigate the behavior of the lethal attacks in wireless adhoc network as well as develop a strategy for resisting the spread of such intrusion further. The block diagram of the proposed system is shown in Figure 1. The block diagram exhibits the scheme towards identification and prevention of the different variants of attacks on wireless adhoc network. The proposed model develop an adversarial model using three different strategy which is about observing the malicious behavior of the destination / intermediate node in the neighborhood. The complete observation is carried out on the basis of the trust management where trust is calculated using probability concept. The final stage of the study implementation is about identifying the malicious behavior which is further followed by either continuing the communication or stopping the communication using allocation of award / penalty. The next section further illustrates the algorithmic details.

3. ALGORITHM IMPLEMENTATION

The complete development strategy of the secured routing in wireless adhoc network depends on complex behavioral traits of malicious nodes that are challenging to be identified. Therefore, this algorithm considers all the complex behavioral factors where trust is the core component of the design. This section discusses about the important information associated with the construction of this algorithm.

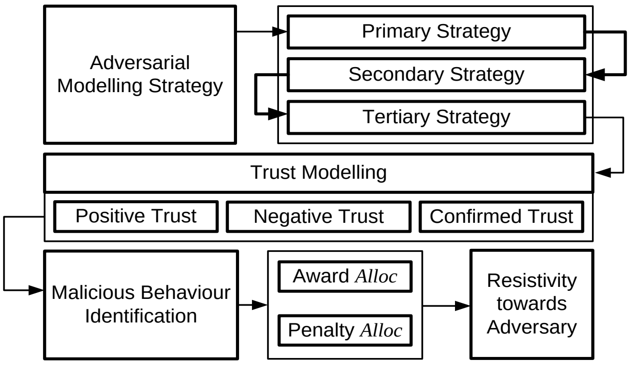

Figure 1. Block diagram of proposed methodology

3.1. Strategies consideration

The *primary strategy* of algorithm design is to extract the legitimacy of the destination node or intermediate node on the basis of trust from its neighboring node in prior to establishing routes. It will eventually mean that there is no priorly established information about the nodes to be communicated about in wireless adhoc network and there are all the possibilities that any node could be malicious node (or compromised or victim node). Hence, secure routing is carried out only on the basis of dynamic value computed with respect to trust and no prior routing information is considered. The *secondary strategy* of algorithm is that proposed algorithm is designed on the basis of finite number of possible actions that could be adopted by the regular node and malicious node as the study assumes that behavior of malicious node is not possible to be distinguished in the preliminary rounds of communication. The modeling also considers that there are some sets of actions that are common between regular and malicious node while some actions are quite distinct. In order to incorporate challenging adversarial module, the study considers that number of distinct characteristics of regular and malicious node is very small than number of common characteristics. The *tertiary strategy* of the algorithm design is a new policy of award and penalty allocation for the node against their behavior. According to this strategy, if a node assists in carrying legitimate task than they are allocated award or else they are allocated with penalty. Both award and penalty is related to the increment and decrement of trust factor the node. If the node is found to assists in carrying out legitimate task with harmful intention (which is calculated using probability), the node is considered as suspicious node but still award with lower value is allocated. Until and unless the node is not confirmed to be a malicious node, they are allocated with award but with lesser value. It is because the system will need to optimize the data forwarding scheme with equal emphasis on secure routing.

3.2. Important parameters involved

There are various forms of parameters considered for this modeling aspect. The parameters related to *assessing the legitimacy of the node* are positive and negative trust (P_t, N_t) which is obtained only from the neighboring node of the destination / intermediate node to be communicated. The parameters related to decision making are threshold *thres* and statistical variance *var*. The threshold value is used for ensuring if the set of observed values of confirmed trust T_c is less than *thres*.

3.3. Algorithm execution flow

The algorithm takes the input of *s* (source node) and *d* (destination node) which after processing yields an outcome of flag message (confirmation/rejection of routing). The steps involved in proposed secure routing algorithm.

Algorithm for secure routing

Input:*s* (source node), *d* (destination node)

Output:flag message (confirmation/rejection of routing)

Start

```
init$s$, $d$
For i=1:n
    $s \rightarrow prob(P_t, N_t)^d$
    If $P_t=N_t$
        $t_c \rightarrow f(P_t, N_t)$
```

```
6.      If $(t_c(d))^T$>thres
7.          flag d as malicious node & break communication through d
8.          Ifflag(d)=outlier
9.              allocate penalty
10.         Else
11.             allocate reward
12.           update routing table
13.       else
14.          flagd as regular node & continue communication through d
15.          update routing table
16.     End
17. End
18. End
End
```

The operations involved in the proposed algorithm are as follow: The algorithm selects a source and destination where there are possibilities that destination nodes could be regular or malicious node (Line-1). For all the nodes (Line-2), the algorithm performs computation of the positive and negative trust (P_t, N_t) using probability. The trust is computed by obtaining probability of one common action divided by the summation of two common actions. This computation is carried out by the source node *s* towards destination (or intermediate) node *d*. After the computation of the trust is carried out, the proposed system checks if the value of the positive and negative trust is equivalent. In case both are found to be same, than the proposed algorithm further confirms the trust value using a discrete function *f*(x) is developed (Line-3). If the series of observed value of confirmed trust T_c is found to be same over a period of time T, the conclusion can be made with respect to the threshold (0.02-0.05). A second check is done towards node that has been found to malicious for final confirmation with respect to statistically developed outliers (Line-8). Hence, presence of falsified claim attracts penalty (Line-9) otherwise reward is given followed by updating routing table. Routing operation is continued only after confirming the destination node is legitimate member (Line-14). The next section discusses about results obtained.

4. RESULTS DISCUSSION

The scripting of the proposed logic was carried out in MATLAB over normal 64 bit windows platform. The simulation environment consists of 200 mobile nodes combining both regular and malicious nodes with no direct input of node identity for malicious node prior to simulation. The assessment is carried out with respect to throughput, routing overhead, latency, and processing time. A comparative analysis is carried out with respect to SEAD [33] and SRP [34] protocol which is also secured routing schemes in wireless adhoc network.

The graphical outcome shows that proposed system offer better throughput as shown in Figure 2 and lower routing overhead as shown in Figure 3 compared to existing SRP and SEAD protocol. The prime reason behind the throughput improvement is that proposed system offers better formulations of routes in faster track as it has frequent updates about the global trust values. Moreover adoption of probability based modeling further boost up the process of exploring and confirming the secured path.

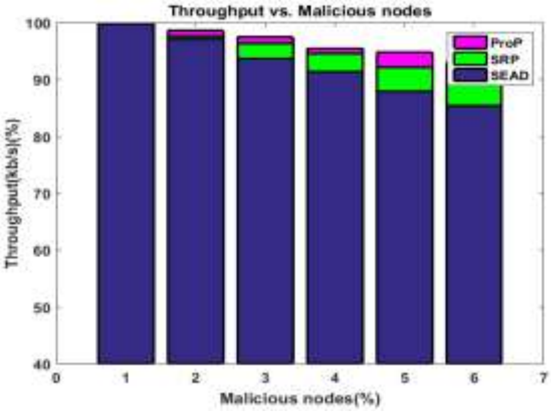

Figure 2. Comparative analysis of throughput

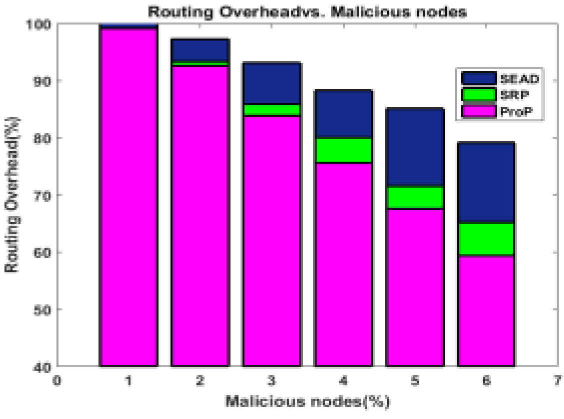

Figure 3. Comparative analysis of routing overhead

The outcome shown in Figure4 exhibits that there is considerably lower routing overhead. A closer look into Figure 2 to Figure 4 shows that increase of malicious nodes in terms of percentile do notoffer much challenges to communication performance. As the mobile nodes access their routing table from their shared memory, hence, obtaining global trust factor is quite faster. Moreover, the proposed system offers faster processing time as shown in Figure 5 as it has no inclusion of any iterative operation e.g. encryption as well as it do not have any dependency of storing any secret keys as authentication is always done when demanded. Therefore, the proposed system can be said to offer better security options in cost effective manner.

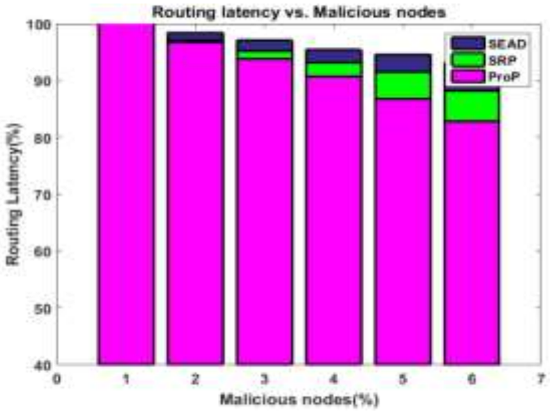

Figure 4. Comparative analysis of routing latency

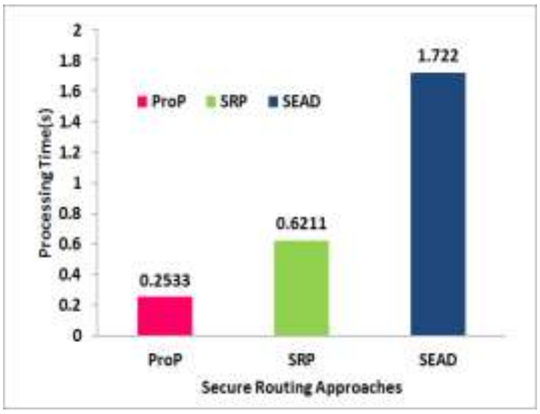

Figure 5. Comparative analysis of processing time

5. CONCLUSION

This paper has presented a sophisticated as well as unique modeling of secure routing scheme in wireless adhoc network. According to the proposed scheme, the malicious behavior of the mobile node is monitored using a probabilistic model where various probability parameters are assessed. The proposed scheme also introduces logic of award and penalty allocation which boost up the system of data forwarding and restrict any form of activities that deal with harmful intention. The proposed system is also compared with the existing secured routing to find that it offers better data forwarding performance as well as robust security.

REFERENCES

[1] Habib F. Rashvand, Han-Chieh Chao, “Dynamic Ad Hoc Networks,” Institution of Engineering and Technology, pp. 447, 2013.

[2] S. Sharmila and T. Shanthi, "A Survey on Wireless ad hoc Network: Issues and Implementation," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, pp. 1-6, 2016.

[3] S. Meguerdichian, F. Koushanfar, M. Potkonjak and M. B. Srivastava, "Coverage Problems in Wireless ad-hoc Sensor Networks," *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213)*, Anchorage, AK, USA, vol. 3, pp. 1380-1387, 2001.

[4] V. Ramasamy, "Recent Advances in ad-hoc Networks," *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, pp. 132-132, 2017.

[5] A. Vij and V. Sharma, "Security Issues in Mobile adhoc Network: A Survey paper," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 561-566, 2016.

[6] M. S. Athulya and V. S. Sheeba, "Security in Mobile Ad-Hoc Networks," *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, Coimbatore, pp. 1-5, 2012.

[7] R. K. Singh and P. Nand, "Literature review of routing attacks in MANET," *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, pp. 525-530, 2016.

[8] T. Zheng, H. Wang, J. Yuan, Z. Han and M. H. Lee, "Physical Layer Security in Wireless Ad Hoc Networks Under A Hybrid Full-/Half-Duplex Receiver Deployment Strategy," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3827-3839, June 2017.

[9] A. Kannammal and S. S. Roy, "Survey on secure routing in mobile ad hoc networks," *2016 International Conference on Advances in Human Machine Interaction (HMI)*, Doddaballapur, pp. 1-7, 2016.

[10] V. S. Bhargavi, M. Seetha and S. Viswanadharaju, "A hybrid secure routing scheme for MANETS," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, pp. 1-5, 2016.

[11] Sowah, Robert A., Kwadwo B. Ofori-Amanfo, Godfrey A. Mills, and Koudjo M. Koumadi, "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, pp.14, 2019.

[12] AbuZant, Mahmoud, and AdwanYasin, "Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)," *Security and Communication Networks*, pp. 12, 2019.

[13] Vadavi, J. V., and Ashwini G. Sugavi, "Detection of black hole attack in enhanced aodv protocol," In *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, pp. 118-123. IEEE, 2017.

[14] Sekaran, Ramesh, and Ganesh Kumar Parasuraman.,"A secure 3-way routing Protocols for Intermittently connected Mobile ad hoc Networks," *The Scientific World Journal*, pp. 13, 2014.

[15] Faisal, Mohammad, Sohail Abbas, and Haseeb Ur Rahman, "Identity Attack Detection System for 802.11-based ad hoc Networks," *EURASIP Journal on Wireless Communications and Networking*, pp. 128, 2018.

[16] NithyaSavarimuthu, “Detection and Prevention of Collaborative Attack and Energy Efficient Routing in Wireless and Ad hoc Network”, *Research Gate*, vol. 9, pp 1-6, 2016.

[17] Alnumay, Waleed S., Pushpita Chatterjee, and Uttam Ghosh, "A trusted Framework for Secure routing in Wireless ad hoc Networks," In *2015 International Conference on Collaboration Technologies and Systems (CTS)*, pp. 190-195. IEEE, 2015.

[18] Babu, E. Suresh, C. Nagaraju, and M. H. M. Prasad, "A secure routing protocol against heterogeneous attacks in wireless adhoc networks," In *Proceedings of the Sixth International Conference on Computer and Communication Technology 2015*, pp. 339-344. ACM, 2015.

[19] Madhusudhanan, B., S. Chitra, and C. Rajan, "Mobility based key Management Technique for Multicast Security in Mobile ad hoc Networks," *The Scientific World Journal*, pp.10, 2015.

[20] Zhang, Qingwei, Mohammed Almulla, and AzzedineBoukerche, "An Improved Scheme for Key Management of RFID in Vehicular Adhoc Networks," *IEEE Latin America Transactions*, vol. 11, no. 6, pp. 1286-1294, 2016.

[21] Gong, P., Chen, T.M. and Xu, Q., “ETARP: An Energy Efficient trust-aware routing protocol for Wireless Sensor Networks,” *Journal of Sensors*, pp.10, 2015.

[22] Ahmed,Mozmin, and Md Anwar Hussain, "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks," In *International Conference on Electronics, Communication and Instrumentation (ICECI)*, pp. 1-4. IEEE, 2014.

[23] Sibichen, Sisily, and SreelaSreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in adhoc Networks," In *2013 Annual International Conference on Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy*, pp. 1-6. IEEE, 2013.

[24] Malhotra, Amarjit, Saurabh Kirtani, and Tushar Agarwal, "Detection of malicious route in wireless adhoc networks," In *2012 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-4. IEEE, 2012.

[25] Das, Abhijit, SoumyaSankarBasu, and Atal Chaudhuri, "A novel security scheme for wireless adhoc Network," In *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE)*, pp. 1-4. IEEE, 2011.

[26] Esfandi, Abolfazl, "Efficient anomaly Intrusion Detection System in adhoc Networks by mobile agents," In *2010 3rd International Conference on Computer Science and Information Technology*, vol. 7, pp. 73-77. IEEE, 2010.

[27] Sumathy, S., and B. Upendra Kumar, "Secure key Exchange and Encryption Mechanism for group Communication in wireless ad hoc networks," *arXiv preprint arXiv:1003.3564* (2010).

[28] ChandanRadha Raman Mishra, “A Review of Security Challenges in Ad-Hoc Network,” *Research Gate*, vol. 13, no. 12, pp. 16117-16126, 2018.

[29] Moudni, Houda, Mohamed Er-rouidi, HichamMouncif, and Benachir El Hadadi, "Secure routing protocols for mobile ad hoc networks," In *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, pp. 1-7. IEEE, 2016.

[30] Wu, Wei-Chen, and Horng-TwuLiaw., "A study on high secure and efficient MANET routing scheme," *Journal of Sensors*, pp.10, 2015.

[31] Neeli, Jyoti, “Insight to Research Progress on Secure Routing in Wireless Ad hoc Network,” *International Journal of Advanced Computer Science and Applications*, vol.8, no. 6, pp. 68-76, 2017.

[32] Neeli, Jyoti, and N. K. Cauvery, "Framework for Capturing the Intruders in Wireless Adhoc Network Using Zombie Node," In *Computer Science On-line Conference*, pp. 346-355. Springer, Cham, 2018.

[33] Hu, Yih-Chun, David B. Johnson, and Adrian Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc network," *Ad hoc networks*, vol. 1, no. 1, pp. 175-192, 2003.

[34] Liu, Zhiyuan, Shejie Lu, and Jun Yan, "Secure routing protocol based trust for ad hoc Networks," In *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, vol. 1, pp. 279-283. IEEE, 2007.

BIOGRAPHIES OF AUTHORS

JyotiNeeli is Associate professor in Department of Information Science & Engineering, Global Academy of Technology. She has completed M .Tech form VTU University and is currently pursuing Ph.D from VTU University under the guidance of Dr. N K Cauvery. She has teaching experience of 17years, research 5 years. Her area of interest includes Computer networks, System modeling & simulation, Software Engineering. She has published more than 7 papers in conferences & journals.

Dr. Cauvery N. K., is a Professor in Department of Information Science & Engineering, R V College of Engineering. She has Completed Ph. D from VTU, ME (CSE from Bangalore University).She has total experience of 30 years with teaching: 20 Years ,R&D: 10 Years. Her area of interest includes Computer Network, Compiler Design, and Genetic Algorithm. She has published 21 papers in international journals, 10 papers in international conference.