ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 11 , November 2016

Detection of False Positive and False Negative Problem in Identification of Unsecured Node

Saurabh P. Ratnaparkhi, Prof. S. V. Sonekar

Project Scholar, Department of Computer Science & Engineering, RTM Nagpur University, Nagpur, India
Professor, P G Department of Computer Science & Engineering, RTM Nagpur University, Nagpur, India

ABSTRACT: Mobile ad hoc network (MANET) is a recent technology. MANET is infrastructure less, with no any centralized control exists and also each node contains routing capability. Each device in a MANET is independently free to move in all direction, and therefore change its connections to other devices frequently. Any unsecured node under attack in ad hoc network exhibits an anonymous behaviour called the malicious behaviour. In this situation, the entire operation of a network gets disturbed and to preclude such malevolent behaviour several security options have been discovered. In this project, malicious behaviour of an unsecured node is defined and to defend such behaviour, a testing solution False Positive and False Negative (FPFN) is presented which is used in furnishing a secure and reliable communication in ad hoc network. Operation of a network gets distressed and to exclude such malicious behaviour several security options have been discovered. In this paper, unsecured malicious behaviour of a node is defined and to defend such behaviour, security solutions are presented which are used in obtaining a secure and reliable communication in ad hoc routing.

Misbehaviour due to unsecured reasons can significantly reduce the performance of effectiveness of MANET. An unsecured node attempts to use the resources only for its own purpose and it hesitates to contribute to the resources with secured neighbours. So, it is very important to detect the unsecured nodes precisely to improve the performance of MANET. Initially, a structural model of a MANET is constructed and the communication between the mobile is generated.

KEYWORDS: MANET, Unsecured Node, False Positive, False Negative detection

I. INTRODUCTION

Mobile ad hoc network (MANET) is a wireless network type among mobile nodes. It is a self-configuring system of mobile nodes connected by wireless associations, which contains a network topology with many other surrounded nodes. This network is relatively a new communication pattern, which contains a group of mobile devices communicating entirely with a wireless medium. In general each mobile node in MANET requires the help of other neighbor nodes to route the packets. The nodes are expected to wait for a predefined time interval between successive transmissions. Node misbehavior due to unsecured or malicious reasons or faulty nodes can considerably decrease the performance of MANET.

Node misbehavior means divergence from the original routing and forwarding path. This makes network situation unsecured for routing process, which may intentionally delay, drop or add vulnerability to the packet. These misbehaviors of the unsecured nodes will impact the efficiency, reliability, and the fairness.

Trust evaluation and management contributes an integrated approach for interpreting and specifying security policies, credentials, and relationships. It involves trust establishment, trust revocation, and trust update in MANET.

Our false positive and false negative technique helps in identifying such unsecured nodes earlier on the basis of probabilistic concepts. Type II error which is knows as false negative has the better identification ratio as compare to other majors.

II. LITERATURE SURVEY

Singh et al. [5] implemented a security-based algorithmic approach in MANETs. In this analysis, an empirical and effective approach was proposed to optimize the packet loss frequency. Hernandez et al. [6] introduced a fast model to evaluate the unsecured node detection in MANET using a watchdog approach. They estimated the time of detection and the overhead of collaborative watchdog approach for detecting one unsecured node. Manoj et al. [7] introduced a novel trust-based certificate authority concept to transmit data packets through trusted nodes and insulates malicious nodes in MANET. Jawhar et al. suggested a reliable routing protocol for enhanced reliability and security of communication in the MANET and sensor networks [8]. In this paper, the reliability and security were achieved by the maintenance of a reliability factor by the nodes. Rodriguez and Gozalvez[9] recommended a reputation-based unsecured prevention technique for MANET. Disparate reputation-based protocols were proposed in this paper to observe the correct relaying of packets and to compile information about potential unsecured nodes. The authors discussed three techniques to detect unsecured nodes in MANET, namely reputation-based technique, credit-based technique, and acknowledgement-based technique.

III.RESEARCH METHODOLOGY

A. Analyse the Properties of Unsecured Node

In a network, a node is a connection point, either a relocation point or an end point for data transmissions. e.g.- a modem, hub, bridge, switch or router, etc.

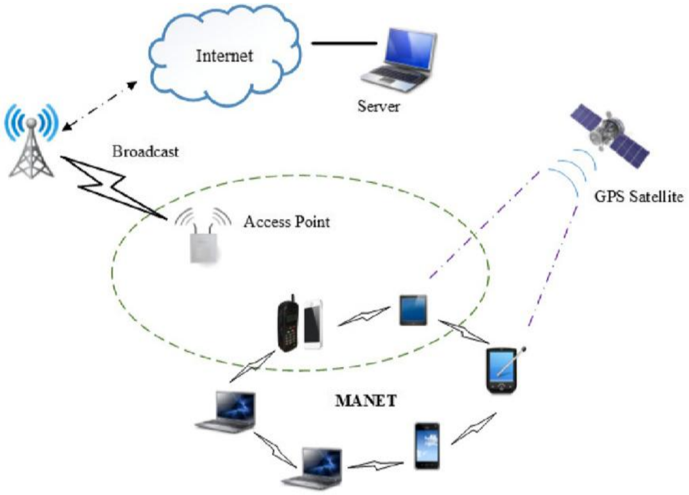


Fig. 1- Mobile Ad Hoc Network

B. Nature of Unsecured Node

Any unsecured node which may be malicious or selfish in the network area can either disturb the routing process or can even put packet data at risk or stop it. Several attacks like black hole, wormhole, rushing, etc. In normal behavior , when any operation is performed in an MANET while maintaining the security principles confidentiality(CF), integrity(IN), availability(AV), authenticity(AU) and non-repudiation(NR), then it is called the ‘Normal Behavior of a node’.

C. False Positive and False Negative Problem Technique

In order to find out the above problem for computationally efficient unsecured node detection, we take help of the statistical binary testing of finding node error rate as a testing technique for the available MANET nodes. This testing module is applied on nodes in MANET to identify true unsecured node with more accuracy. It has four strategies to examine the node as True Positive, True Negative, False Positive (Type I Error) and False Negative (Type II Error).

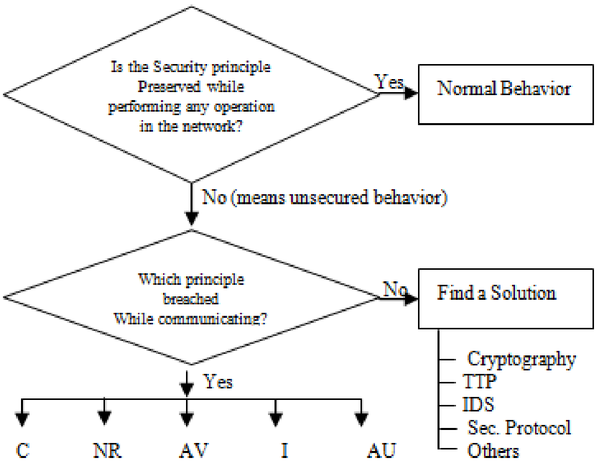

Is the Security principle Preserved while performing any operation in the network?
Yes
Normal Behavior
No (means unsecured behavior)
Which principle breached While communicating?
No
Find a Solution
Cryptography
TTP
IDS
Sec. Protocol
Others
Yes
C
NR
AV
I
AU

Fig. 2- Defining Normal and Unsecured Behavior of a Node

	ATTACK	NO ATTACK
ALARM	TP	FP
NO ALARM	FN	TN

Fig. 3- FPFN working Principle

In above figure, simple choice based logic is put down which is used to detect the node unsecured nature probability. Out of all the four reasons, last two are more prominent for consideration. Type-I error is rejecting the null hypothesis when it is true. Type-II error is accepting the null hypothesis when it is false. By calculating node parameters and then analysing them for false alarm case of unsecured behaviour is very important to be notified.

Detection relies on the ability of a given node to efficiently analyze its own states and events with all observable events and states in its physical neighborhood. This testing module is applied on nodes in MANET to identify true unsecured node with more accuracy by computing for trust evaluation model (TEM) and record. Trust evaluation model is essential to distinguish forged data of unsecured nodes from innocent data of secured nodes in MANET.

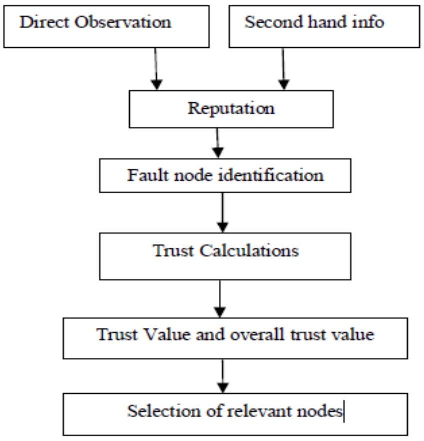

Direct Observation
Second hand info
Reputation
Fault node identification
Trust Calculations
Trust Value and overall trust value
Selection of relevant nodes

Fig. 4- Trust Evaluation Model for *Ad Hoc* Network

IV. PROPOSED METHODOLOGY

A. Route Discovery

Route discovery allows any node in a MANET to dynamically discover a route to any node in MANET. The first step of route discovery is to form the number of nodes with the indicated position. By sending the RREQ packet, the route is revealed between the source node and the destination node. This is explain in following algorithm.

Algorithm 1: Processing of RREQ and REP messages

```
Begin
        Initiate route discovery through secured neighbors;
        Node
                Processes RREQ ();
                Propagates RREQ ();
                Generate and unicast RREP ();
        Switch to monitoring and identification Routine ();
        Modifies and unicast RREP ();
        Processes RREP ();
End
```

B. Record and Trust Evaluation Model Technique

The main intent of this analysis is to handle and detect unsecured nodes in MANET using the Record TEM technique. The trust factor of a node is computed based on their behavior. The basic idea is to build a trust model that provides a mechanism to estimate the trust of its neighbors. The proposed trust system contains a powerful tool for the detection of unexpected unsecured node behaviors. Once these unsecured nodes are detected, their neighbors can use this information to shun cooperating with them, either for data forwarding, data assembling or any other supportive function.

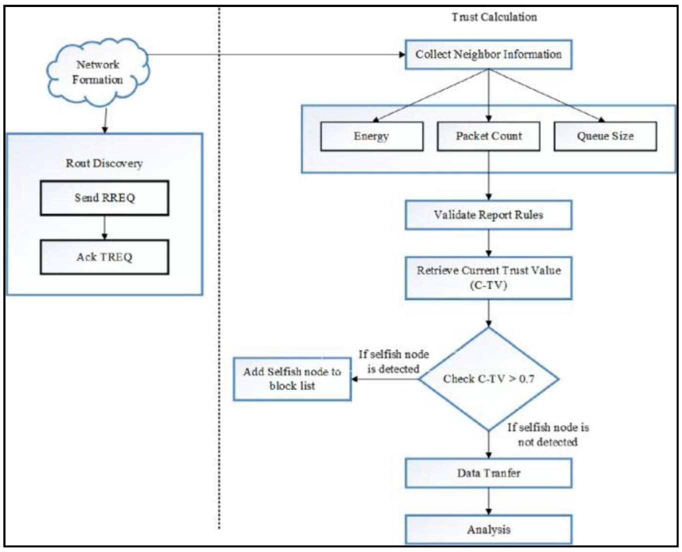
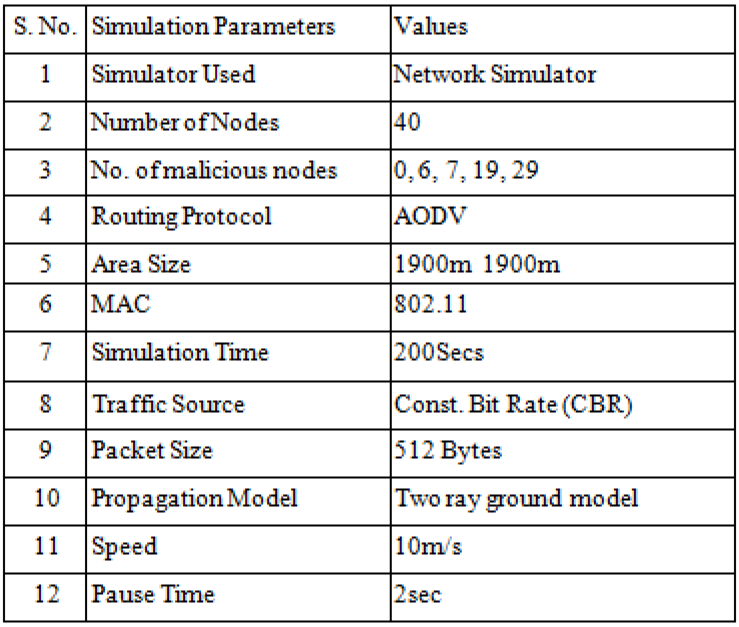

Trust Calculation
Network Formation
Collect Neighbor Information
Energy
Packet Count
Queue Size
Rout Discovery
Send RREQ
Ack TREQ
Validate Report Rules
Retrieve Current Trust Value (C-TV)
If selfish node is detected
Add Selfish node to block list
Check C-TV > 0.7
If selfish node is not detected
Data Tranfer
Analysis

Fig. 5- Proposed Record and Trust Evaluation Model Technique

V. IMPLEMENTATION

Specified statistical readings can be beneficial with our approaches. NS version 2.37 Simulation represents the above inferences. We modify the AODV protocol in ns-2 to enable some nodes to be configured as misbehaving. The unsecured misbehaviour here is define as either drop the packets or not to forward the packet in the specified time interval. The following table shows the sample simulation parameters.



S. No.	Simulation Parameters	Values
1	Simulator Used	Network Simulator
2	Number of Nodes	40
3	No. of malicious nodes	0, 6, 7, 19, 29
4	Routing Protocol	AODV
5	Area Size	1900m 1900m
6	MAC	802.11
7	Simulation Time	200Secs
8	Traffic Source	Const. Bit Rate (CBR)
9	Packet Size	512 Bytes
10	Propagation Model	Two ray ground model
11	Speed	10m/s
12	Pause Time	2sec

Fig. 6 - Simulation Parameters

A. Detection Effectiveness

This deliberates the performance of the RTEM algorithm. This is calculated as total number of detected nodes divided by the total number of unsecured nodes in the network.

$$\text{Detection Effectiveness} = \frac{\text{Detected nodes}}{\text{Total unsecured nodes}} \times 100$$

B. False Positive

This is calculated as total number of good performing nodes but detected as unsecured divided by the total number of good behaving nodes.

$$\text{False Positive} = \frac{\text{Good performing detected nodes}}{\text{Total good behaving nodes}} \times 100$$

C. False Negative

This is calculated as total number of malicious nodes which are not detected divided by the total number of malicious nodes.

$$\text{False Negative} = \frac{\text{Unsecured Undetected nodes}}{\text{Total unsecured nodes}} \times 100$$

D. Record – Trust Evaluation Method

Every node maintains a global trust state. The trust state is maintained in the form of a trust table. A trust table has two fields, namely *n-id* (*node id*) and *t-val* (*trust value*). When a node receives a new trust certificate, the trust state of a node is updated. The certificate is estimated by verifying the response from every neighbor in the group. The effect of trust certificate in the final trust value of a suspected node depends on the trust state of the node. To update the trust value of a node, the following function is applied as shown in (1):

$$(1-Tnew) = A\ (1-Told) + B\ (1-Tc) - Trf \qquad (1)$$

In above equation A and B denotes the weighs corresponding to the old trust and new trust values of the node. Trf is the trust replacement factor over time. B depends on three factors a_1, a_2, and a_3. The parameter B can be expressed in (2):

$$B = a1 \times a2 \times a3 \qquad (2)$$

The parameter a_1 is shown in (3):

$$a1=\sum majWiTi\ \ / Wn \qquad (3)$$

Where Wi and Ti depicts the weights and trust value, respectively, belonging to the majority group of the neighbors of the blame node. Wn is a factor that depends on the size of the network. a2 represents the weight given to the new trust value, and the value of a3 is obtained using (4):

$$a3=\begin{cases}1 \text{ if } k = 1\\ 1 \text{ if } k > 1\end{cases} \qquad (4)$$

Here, the number of packets sent to the unsecured node is reduced to mitigate the routing misbehavior.

E. Trust Value Calculation Parameters

Qrsr is defined as the query request success rate, which is computed based on the number of neighboring nodes who have successfully received RREQ from the source. Qrfr is defined as the query request failure rate, which is computed based on the number of neighboring nodes who have not received RREQ. Qpsr represents the query reply success rate, which is computed based on the successful replies received by the source. Qrfr describes the query reply failure, which is calculated based on the number of neighboring nodes, who have not sent the replies. Qdsr defined as the data success rate, which is calculated based on successfully transmitted data. Qdfr determines the data failure rate based on the data, which have failed to reach the destination.

$$Qreq = (Qrsr - Qrfr) / (Qrsr + Qrfr) \qquad (6)$$

$$Qres = (Qpsr - Qpfr) / (Qpsr + Qpfr) \qquad (7)$$

$$Qdata = (Qdsr - Qdfr) / (Qdsr + Qdfr) \qquad (8)$$

where Qreq, Qres and Qdata are transitional values, which are used to compute the node request rate, response rate, and data transmission rate, successively.

$$TLV = T(RREQ)\times Qreq+T(RREP)\times Qres+T(DATA)\times Qdata \qquad (9)$$

Where TLV represents the trust level value and *T*(RREQ), *T*(RRES), and *T*(DATA) are time factorial for route request, response, and data sent by the node, respectively.

VI. PERFORMANCE ANALYSIS

A. Identifying unsecured node

The initial step involves the detection of the verified block listed or unsecured nodes among the other mobile nodes of the MANET. The difference between the normal nodes and the verified block listed nodes is shown in figure 7. The blue-colored nodes are the normal nodes, while the yellow-colored nodes indicate the verified block listed unsecured nodes.

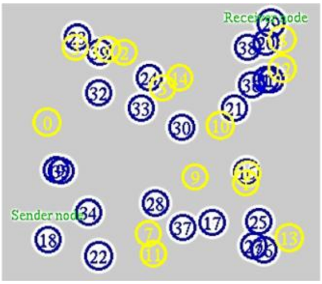


Fig.7- Normal and Unsecured node

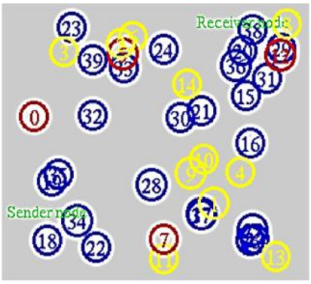


Fig.8- MANET with Unsecured node

B. Detection of unsecured node

The unsecured nodes among the verified block listed nodes are detected in the second step. The detected unsecured nodes are highlighted in red color which is shown in figure 8.

C. Packet delivery ratio

Packet delivery ratio (PDR) is the ratio between the number of packets delivered by a traffic source node and the number of packets acknowledged by a traffic drop. It measures the loss rate as seen by transport protocols, and it describes both the rightness and effectiveness of mobile ad hoc routing protocols as in figure 9.

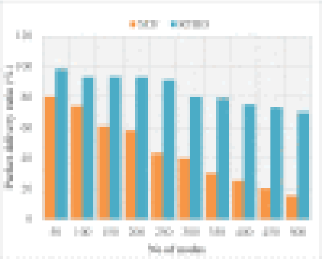


Fig.9- Packet delivery ratio

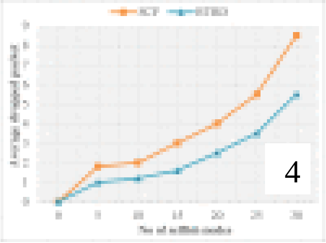


Fig. 10- Avg. packet drop

D. Avg. packet dropping

The inference of not forwarding the packets or dropping the packets in MANET leads to a serious problem. So, this analysis deals with this event and gives higher priority for packet dropping in MANET. The packet drop rate is observed in the unsecured node detection methods, namely SCF and RTEM. The comparative analysis with respect to the number of nodes is shown in Figure 10.

E. Detection ratio

Unsecured node detection is an central concern in MANET, so this study fully concentrates the detection of unsecured nodes in an proficient manner by using RTEM technique. The detection rate of the unsecured behavior is observed by using the RTEM method. Compared to the SCF method, the proposed RTEM method significantly increases the detection ratio shown in figure 11.

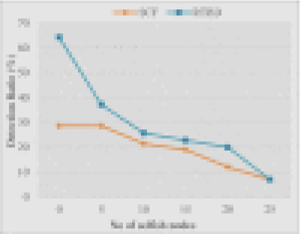


Fig. 11- Detection ratio of unsecured node

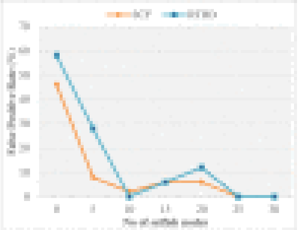


Fig. 12- False negative rate

F. False negative rate

The false alarm will be differentiated from the overall selfishness alarm for unsecured nodes. The detection of this false alarm leads to better performance in the overall network. The probability of parameters such as energy, memory space, and CPU time in packet drop rates is analyzed with respect to the false alarm rate as shown in above figure 12.

VII. CONCLUSION

The misbehavior of unsecured nodes is a major problem in MANET. The unsecured nodes do not participate in the routing process, which intentionally delay and drop the packet. These misbehaviors of the unsecured node will impact the efficiency, reliability, and fairness. The unsecured node utilizes the resources for its own purpose, and it neglects to share the resources to other nodes. So, it is important to detect the unsecured nodes in MANET. This study proposes a new technique, namely RTEM, to detect the unsecured nodes in an efficient manner. The suggested RTEM method is an effective method, which enhances the performance of MANET. It significantly improves the performance metrics such as PDR and detection ratio. Moreover, it diminishes the overhead, latency, and packet dropping ratio. Compared to the existing SCF method, the proposed method competently detects the unsecured nodes in MANET.

The future enhancement can be done by providing the security to the neighbor node. This avoids the neighbor node being compromised by the unsecured node.

REFERENCES

[1] R Singh, P Singh, M Duhan, An effective implementation of security based algorithmic approach in mobile adhoc networks. Hum Centric Comput Inf Sci **4**, 1–14 06/19014 bIOmED Central Full Text

[2] E Hernández-Orallo, MS Olmos, J-C Cano, C Calafate, P Manzoni, A fast model for evaluating the detection of unsecured nodes using a collaborative approach in MANETs. Wirel. Pers. Commun. **74**, 1099–1116 02/01 2014 Publisher Full Text

[3] V Manoj, N Raghavendiran, M Aaqib, R Vijayan, Trust based certificate authority for detection of malicious nodes in MANET. in *Global Trends in Computing and Communication Systems*, ed. by Krishna PV. vol. 269 (Springer, Berlin, 2012), pp. 392–401

[4] I Jawhar, Z Trabelsi, J Al-Jaroodi, Towards more reliable and secure source routing in mobile ad hoc and sensor networks. Telecommun. Syst. **55**, 81–91 (2014). Publisher Full Text

[5] A Rodriguez-Mayol, J Gozalvez, Reputation based unsecuredness prevention techniques for mobile ad-hoc networks. Telecommun. Syst., 1–15 (2013)

[6] Biswas, J. ; Gupta, A. ; Singh, D., “A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol,” in Proc. Industrial and Information Systems (ICIIS), 2014 9th International Conference IEEE, 15-17 Dec. 2014, Page(s):1 - 6

[7] Patdar, K. ; Dubey, V.,“A Modified AODV Protocol to Detect and Prevent The Wormhole: A Hybrid Approach”, IEEE 2010, Page 233-238

[8] Mehto, A.; Gupta, H. “A dynamic hybrid approach for wormhole detection and prevention,” Computing, Communications and Networking Technologies ICCCNT),2013 Fourth International Conference on IEEE, Page(s): 1-4

[9] Anuradha T.; Sandeep “Improving Performance of Neighbor Discovery in MANET by using Threshold value and Time out Parameter,” International Journal of Computer Applications, IJCA Aug. 2014, Vol. 99-No.-10, pp- 52-57

[10] M. Tamer Refaei, Yanxia Rong ; Luiz A. DaSilva; Hyeong-Ah Choi, “Detecting Node Misbehavior in Ad hoc Networks,” Communications, 2013. ICC '07. IEEE International Conference, Page(s): 3425-3430

[11] Sejun Song; Haijie Wu; Baek-Young Choi, “Statistical wormhole detection for mobile sensor networks,” Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conf. IEEE, Page(s): 322-327.

AUTHOR'S BIOGRAPHY

Saurabh P. Ratnaparkhi was born in Nagpur, India, in 1983. He received the B.E. degree in computer engineering from the Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, India, in 2008, and completing the M.Tech. degree in computer science & engineering from the J D College of Engineering, Nagpur India, in 2015-16 Batch.

In 2008, he joined the Department of Computer Technology, RTM Nagpur University, as a Lecturer, and in 2013 became an Assistant Professor. Since December 2008, he has been with the Department of Computer Science & Engineering, RTMNU. His current research interests include wireless computing and communication, mobile computing, business intelligence, analytics, testing. He is a Life Member of the Indian Society for Technical Education (ISTE), the Computer Society of India.

He has also worked as software analyst role in an IT company for more than two years. Currently he is also a part of software consultant and project analyst for IT firms.

S. V. Sonekar was born in Nagpur, India. He received the B.E. degree in computer engineering from the Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur, India, and completing the M.E. in WCC from the G. H. Raisoni College of Engineering, Nagpur India.He is Professor in Nagpur University. His current research includes Computer Security and Reliability. He is a Life Member of the Indian Society for Technical Education (ISTE), the Computer Society of India.