Novel Pseudonym Generation for Secured Privacy in Vehicular Adhoc Networks

Swapna.ch ,Vijayashree R Budyal

Abstract: ***Intelligent Transport Communication (ITC) has gained popularity in the present day scenario, where communication in vehicle is possible and it can be between Vehicle to Vehicle or Vehicle to Infrastructure. Security is one of the important issue in Vehicular Adhoc Networks (VANETS) and some of the main features of security are Privacy, Confidentiality, Integrity, Authentication and Non-repudiation. In the present scenario privacy along with security is considered to be one of the important factor, since the malicious nodes can attack the vehicles at any point of time during communication. Thus , Secured Privacy in Vehicular Adhoc Networks by Generating Efficient Pseudonym based on Weil Pair Algorithm (SPGPWP), is developed to address secured privacy in VANET's . In the proposed algorithm, communication between vehicles are provided by using pseudonyms generated by road side units with the help of main authority. Our SPGPWP also includes that the pseudonyms received by vehicles from road side units are modified within the vehicle by using Weil pairing algorithm and provides secure communication between vehicle to vehicle without revealing its original identity, thus making the communication anonymous between all the vehicles except the intended vehicles. Simulation is performed to test the performance parameters such as latency, encryption, decryption time, and total time for communication. These performance parameters are compared with RSA (Rivest-Shamir-Adleman).***

Keywords- Road Side Units, public and private keys, Weil pairing, Main Authority, Security, Privacy.

I. INTRODUCTION

Importance of smart vehicles in Vehicular Adhoc Networks (VANETS) has increased drastically. In VANETs the mobility of the nodes is very high compared to the nodes in the MANETs (Mobile Adhoc Networks). The nodes in VANETS are dynamic vehicles and static Road Side Units (RSU). Communication takes place between vehicles through RSU's.

In VANETs [1] it is very important to provide flexibility to the drivers by providing the information regarding the traffic jam, accidents, lane change, security information etc by using Dedicated Short Range Communication (DSRC). The information exchange between the vehicles is crucial, hence Security[2] is the major issue in VANETS, as there are many internal and external attacks [3] from the other nodes.

As per the aforementioned presentation, it is essential to have an efficient identity secure scheme in Vehicular networks and VANET scenario should also satisfy the properties such as low pseudonym generation latency, high scalability and constant connectivity of RSU to the registered vehicles.

Privacy to the vehicles is one of the important parameter in communication. During communication, the malicious nodes should not know the real identity of the source node from where the information being transmitted. If the malicious node identifies the real identity of the vehicle from where message is being transmitted, then there may be the possibility of various attacks. These attacks may be due to internal or external attackers. Internal attackers are the attackers who are in the network and participate in the communication. External attackers are the attackers who are outside the network but absorb and take messages and may try to decrypt the messages. In our proposed work Secured Privacy in VANETs by Generating Efficient Pseudonym based on Weil Pair Algorithm (SPGPWP), both the attacks will be avoided. To obtain secured privacy, SPGPWP has created an environment where the vehicles will register with the main authority (MA), and gives User Id to the vehicle. These vehicles will send its user id to RSU's and obtains pseudonyms. Obtained pseudonyms are further modified by the vehicle by using weil pairing algorithm [4] and sends to other vehicles during communication to maintain privacy.

A. Our Contribution

Our main contribution in the SPGPWP, is to make the vehicles to have secret and privacy communication. The three main contribution in our proposed work are:

- Communication will take place only between the vehicles which are registered by the main authority. Thus Conditional privacy is provided to the vehicles to have more security.
- Our Scheme construction is based on ECC (Eliptical Curve Cryptography) based PKI (Public key Infrastructure) which is advantageous than RSA (Rivest-Shamir-Adleman) based PKI algorithm as ECC requires low cost for computations and small key size.
- The RSU's of ;the VANETS will receive pseudonyms from Main Authority and these pseudonyms are transmitted to the registered nodes, which further Encrypts the pseudonyms to rovide more secure communication by using weil pairing algorithm. The intended vehicles will decrypt the information by using the private key.

B. Paper organization

The organization of the rest of the paper is as follows. Related work is presented in Section-II. Section-III details the proposed work, Section IV describes Simulation, results and the results are compared with RSA. Finally Section-V concludes our work and gives the scope for the future work.

II. RELATED WORK

Privacy in security is the major concern in VANETS and some of the related works are presented.

Revised Manuscript Received on December 5, 2019.

Dr. Vijayashree R Budyal ,working as Professor and Head Department of Mechatronics at Sri Venkateshwara College of Engineering Bengaluru, Karnataka, India.

Swapna Ch, Assistant Professor in Department of Electronics and Communication Engineering at Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India.

In [5] identity based security is proposed, where unique identity of the vehicles are generated and communication between vehicles is done using this unique id. RSA based algorithm has been proposed in [6], in which malicious nodes are removed from the network and provides better security features in VANETS.

The Vehicle Safety Communication (VSC) [7] is a project which proposed the use of a short lived pseudonyms which guarantees anonymity through privacy.

A scheme has been developed to provide safety to the vehicles by sharing the information related to road and traffic as in [8].

The main drawbacks of the existing schemes are large key size, high pseudonym key generation latency, more encryption and decryption time and enormous presence of RSU's are required in order to provide connection between the vehicles. SPGPWP overcomes the drawbacks and provides secrete communication in VANETS.

III. PROPOSED WORK

This section presents the network model, various attacks and proposed solution, Secured Privacy in VANETs by Generating Efficient Pseudonym based on Weil Pair Algorithm (SPGPWP), simulation results and comparison of SPGPWP with the RSA [6].

A. Network Model

The network contains Main Authority (MA), Vehicles (nodes) and RSU’s (acts as routers). Registration of vehicles takes place at MA. Each of the node holds an On Board Unit (OBU) for vehicle to vehicle communication or vehicle to RSU communication. Nodes also contain Tamper Proof Devices (TPD), used to store vehicle secrets such as drivers identity, number plate details, registration details, route map, speed and acceleration of the vehicles, and private key.

The network scenario for the SPGPWP is shown in Fig.1. It contains MA, vehicular nodes (V_1,V_2,V_3,V_4 and V_5) and RSU's (R_1,R_2 and are placed at equidistant and the distance between them is provided based on time interval required to complete total communication).

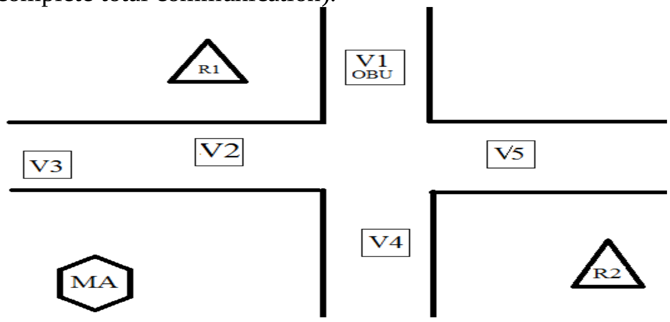

Fig.1 SPGPWP Network scenario.

In SPGPWP, privacy to the vehicles is provided by maintaining their identity secure and pseudonyms are used for communication between the vehicles. The vehicles receives pseudonyms from RSU's, which generate pseudonyms by using hash algorithm and these vehicles will generate new pseudonyms by using weil pairing algorithm. Obtained pseudonyms helps to communicate and provide security through privacy.

B. Registration, Verification and Generation, Encryption and Decryption phase

In the SPGPWP the Pseudonyms are generated in the three different phases as shown in Fig.2. The three different phases are Registration phase, Verification and Generation phase, Encryption and Decryption phase.

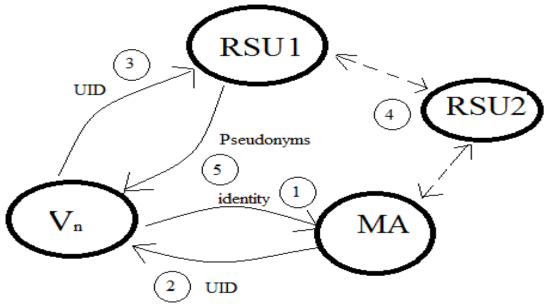

Fig.2. Pseudonyms generation phases

In Fig 2, the first step (1) shows that vehicles get registered with MA by providing their personal details such as vehicles identity, drivers details etc which are available in its TPD. MA generates Unique User Identity (UID) and sends it back to the vehicle as in step two(2). The first two steps are processed in the Registration phase.

RSU's will periodically acknowledge the vehicles and identifies vehicles within its range. Once the vehicles recognizes the RSU it will send it's UID to RSU's as in step 3 and requests RSU's to provide Pseudonyms which are useful for communication with other vehicles to maintain privacy. RSU's are connected with MA through other RSU's as shown in step 4. These RSU’s checks whether the UID sent by the vehicle is authorized or not and if it is authorized then it will send the Pseudonyms to the vehicles as shown in step 5 otherwise ignores. Step 3 and 4 are processed in Verification and Generation Phase.

RSU's, after proper authentication, broadcasts Pseudonyms to the registered vehicles. Once the vehicle receives the pseudonym it will encrypt the pseudonyms by using public key of the vehicle and communicate to the other vehicles. The intended vehicle can decrypt the message by using private key. This process will take place in Encryption and Decryption phase.

Registration phase

During registration phase the vehicle provides all the personal and vehicle details to the MA. MA generates UID_i , by using vehicles master key, S_{vi} . S_{vi} is computed by applying hash function using vehicle identification IDE_i and the random number, *rand* is selected and is very large.

Algorithm for Registration phase

1) Choose a random number, $rand \in Z^*$

2) Obtain vehicle identity IDE_i

3) Compute S_{vi} , a private key as in Eq.1

$$S_{vi} = H_1\left(IDE_i,\ rand\right) \qquad (1)$$

4) Compute $UID_i = S_{Vi}P$.

5) Compute Digital Signature as in Eq.2

$$SIN\left(UID_i,\ S_{va}\right) \qquad (2)$$

6) Store digital signature in MA's data base by mapping as in Eq.3

$$map_i^{va} = \left(UID_i, S_{va} \right) \tag{3}$$

7) Store Eq.4 in vehicles OBU

$$\left(UID_i, SIN\left(UID_i, S_{va} \right), S_{vi} \right) \tag{4}$$

where Z^* is a set of numbers which varies from $\left[1, \ldots, p-1\right]$, where p is the number of points in a group, IDE_i is the vehicle identification details, S_{vi} is the vehicles master key, *H₁* is the hash function which performs hashing and finds value from the hash table, *P* is the generator group, SIN generates the signature by taking the private key S_{va} and unique user id UID_i. UID_i is mapped using map_i^{va} and private key and stores it in the data base. Finally obtained UID_i, signature and private key are stored in the vehicles TPD.

- **Verification and Generation phase**

The vehicles receives UID_i from MA and during exchange of information vehicles uses UID_i instead of its original identity to nearest RSU and requests to provide pseudonyms. The RSU_i which is connected with MA checks whether the UID_i is valid or not and if it is valid, then RSU will generate the Pseudonyms by using hash functions and then transmits to the vehicular nodes. These pseudonyms expires based on the time allotted for expiration, a signature is sent to the vehicle and the mapping is stored in RSU_i.

Algorithm for verification and generation protocol

1) RSU sends its Cer_i to all the vehicles in the entity

2) The vehicles check the Cer_i received from the RSU and send its UID_i to the RSU.

3) RSU_i checks $SIN\left(UID_i,\ S_{va}\right)$ using P_{Ri}

4) if matches RSU has to generate Pseudonyms

- **Using H_1 and RSU_i generates Pseudonyms as in Eq.5**

$$\delta = H_1\left(RSU_i, S_{Ri} \right) \tag{5}$$

- **Generate signature in Eq.6**

$$SIN\left(\delta, t\left(\delta \right), S_{Ri} \right) \tag{6}$$

- RSU has to store the generated pseudonym in the database $map_i^{RSUi} = \left(\ \delta, UID_i \right)$
- Send $SIN\left(\delta, t\left(\delta\right), S_{Ri}\right)$ to vehicle V_i

Cer_i is the certificate of RSU_i which RSU broadcasts to vehicles in the entity. Vehicles sends its signature $SIN\left(UID_i,\ S_{va}\right)$ to RSU's, where S_{va} is the private key of the vehicle. The RSU's checks the signature $SIN\left(UID_i,\ S_{va}\right)$ by using P_{Ri}, where P_{Ri} is the public key of the RSU. RSU_i generates Pseudonyms δ by using hash function H₁ as given by $\delta\ = H_1\left(RSU_i, S_{Ri}\right)$, where S_{Ri} is the RSU's private key. RSU_i also generates signature $SIN\left(\delta, t\left(\delta\right), S_{Ri}\right)$, where $t\left(\delta\right)$ is the expiration time of the pseudonyms and send this signature to vehicle and store the mapping in the RSU_i 's database.

- *Encryption and Decryption phase*

In this phase if the communication is between vehicle V_{ia} and V_{ib} , V_{ia} as a transmitter that sends information to V_{ib} and if there is congestion on the road then, the signature obtained from the RSU_i is verified by the vehicle V_{ia} and it encrypt the message *M*. Hence the encrypted message is *C* and is generated by using weil pair algorithm in which hash functions are used and *C* is sent to the vehicle V_{ib} and the received message is decrypted to get back the original signal M .

Algorithm for Encryption and Decryption

1) To extract the pseudonyms the following protocol need to be executed

Randomly select δ which are sent by RSU_i.

Choose a random value r_a

Compute $\sigma_a\ =\ r_a S_{va}$

Compute Pseudonym PN_i as in Eq.7

$$PN_i\ =\ \left(\sigma_a P, \delta, SIN\left(\delta, t\left(\delta \right), S_{Ri} \right), Cer_i \right) \tag{7}$$

where δ is the public key of PN_i

Store $S_i\ =\ \Upsilon_i S_{va}$ as the private key of PN_i

2) The vehicle has to generate the cipher text by using the following Encryption phase which modifies the message *M*.

Verify $SIN\left(\delta, t\left(\delta\right), S_{Ri}\right)$

Choose random value $k \in \left\{0,1\right\}^n$

Compute Cipher text as in Eq.8

$$C\ =\ (H_1\left(k,\ M\right)P,\ k \oplus H_2(\hat{e}\left(Q_{id},\ SP\right), M \oplus H_3\left(k\right)) \tag{8}$$

where $P, Q_{id} \in E / F_p$, and E is the Elliptical curve and F_p is the field on Elliptical curve with p points.

3)Transmit *C* to V_{ib} .

4) Vehicle V_{ib} receives C and has to decrypt the message as shown below

- Let $C = \langle U, V, W \rangle, P_{vi}$ which is a cipher text encrypted by using the public key of the vehicle.
- Compute σ as shown in Eq. 9 $\sigma = V \oplus H_2(\hat{e}\left(S_{va}, U\right)$ (9)

where S_{va} is the private key of the vehicle which is decrypting the message and $U \in E / F_p$

- Compute Message as in Eq.10

$$M = (\ W \oplus H_4\left(\sigma\right)) \tag{10}$$

- Set $r\ = H_3\left(\sigma, M\right)$ and check whether $U = rP$, if this is not satisfied it will reject the cipher text else M is the message of the cipher text C .

Retrieval Number: D10571284S519/2019©BEIESP
DOI:10.35940/ijrte.D1057.1284S519

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

δ is the pseudonyms generated by RSU. r_a is the random number generated by the vehicle V_{ia} where $r_a \in [0,1]^*$, σ_a is the value generated using private key of the vehicle , σ_a is further used to generate PN_i which are the new pseudonyms generated by vehicle V_{ia}. During the encryption of the message the signature $SIN(\delta, t(\delta), S_{Ri})$ is verified by the vehicle V_{ia} . and using the random value k the cipher text C is generated which uses the original message M,k,P,Q_{id} and hash algorithms such as H_1,H_2,H_3 on this parameters and $\oplus$ is the XOR operation. The vehicle V_{ib} receives this cipher text C and decrypts the message by using the private key of the vehicle V_{ib} .

IV. SIMULATION AND RESULTS

A. Simulation

The assumptions made in SPGPWP are:

The vehicles are considered to be registered under Main Authority before they are allowed on the road for driving.

In the present scenario we are assuming that all the odd numbered vehicles are registered.

RSU are assumed to be compromised as they are located in the outside environment, however the compromise can be detected by using the expiration time

During registration the details such as owners name, address, owner's membership, license plate details and license number, etc., are collected, which are the owners real identity. Main Authorities will accept all the details and generates user id for the vehicles which is helpful for further communication with RSU's and with other vehicles.

SPGPWP network simulation consists road junction and N number of nodes. In which odd number of nodes are considered to be registered with MA and even number of nodes are not registered. All these nodes are placed in the area with A x B, where A is the length and B is the breadth of the area considered.

Some of the simulation parameters are listed in Table.1.

Table.1 Simulation Parameters

Parameters	Values
Area of road	1000x1000m
Number of Nodes considered	100
Registered nodes	Odd nodes
Non Registered nodes	Even nodes
Speed of the vehicles considered	50m/s

B. Results

SPGPWP scenario is simulated using Microsoft Visual c++ software. The total communication time, Encryption time, Decryption time and the latency is calculated and these results are compared with the RSA algorithm [7].

Fig. 3 depicts the total time required to complete the total communication process. The time required for the total communication of SPGPWP is less when compared with RSA algorithm because of low pseudonym generation time in ECC algorithm.

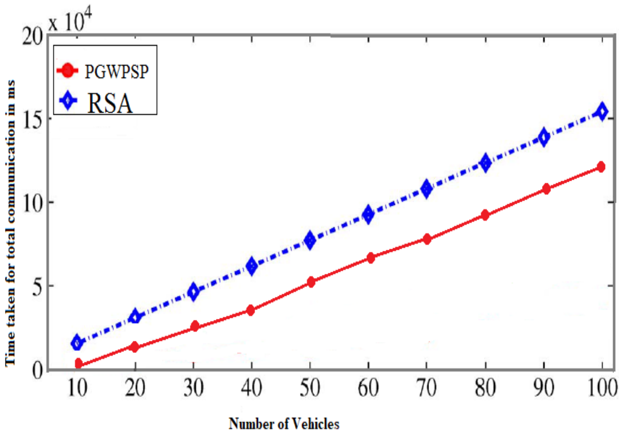

Fig.3 Time requirement for the total communication

Fig.4 and Fig 5. shows the encryption time and the decryption time. The time is less when compared with RSA for varying number of nodes as ECC uses small key size when compared with RSA and hence leads to less number of computations with low transmission and reception time, which further leads to less Encryption and Decryption Time.

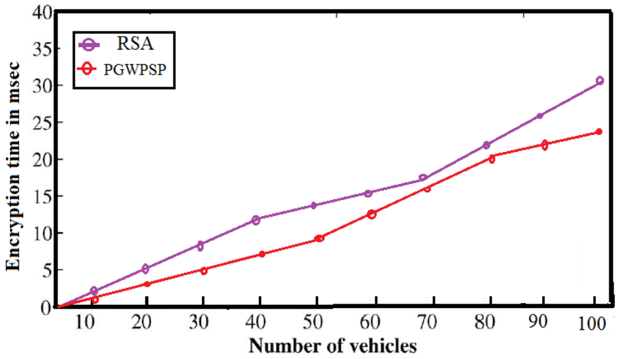

Fig.4. Encryption time.

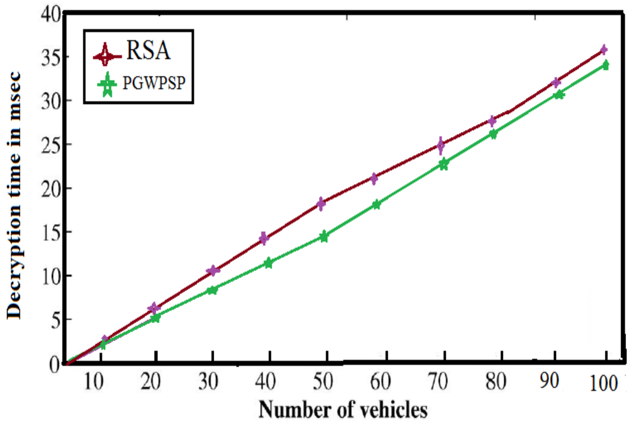

Fig.5. Decryption time.

The Latency in generating the pseudonyms is low in the SPGPWP algorithm than the other existing algorithms like RSA algorithm. Fig.6 Shows that the latency of SPGPWP is less when compared with the latency of the RSA algorithm. The Latency of the RSA algorithm is more when compared with SPGPWP algorithm, as the number of computations in producing pseudonyms are more.

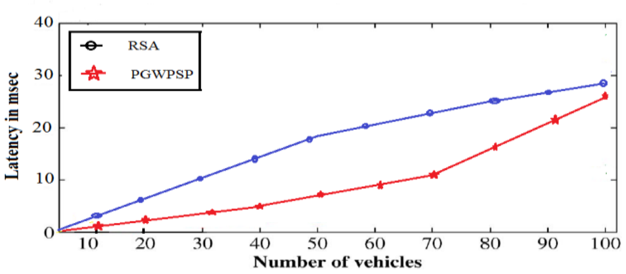

Fig.6. Latency of generating pseudonyms

V. CONCLUSIONS

The proposed work, SPGPWP provides secured privacy for the communication amongst the vehicles. The privacy communication is achieved by using weil pairing method which is used to generate pseudonyms. The communication is totally secret as the vehicle itself is generating the required pseudonyms and the generated pseudonyms will be known only to the vehicle in the entity, which ensures security during communication. The SPGPWP is compared with the existing scheme RSA and proved that it provides optimum results.

Future work can be carried out by considering variavle mobile nodes with high mobility and the simulation area of the test bed can also be increased.

REFERENCES

1. Kajal Jain, Amutha Jeyakumar, "An RSU based approach: A solution to overcome major issues of routing in VANET", IEEE International conference on Communication and Signal Processing (ICCSP), pp.1265-1269, 6-8 April 2016
2. Prasad S. Halgaonkar, Atul B Kathole, Jubber f. Nadaf, K P Tambe," Providing Security in Vehicular Adhoc Network using Cloud Computing by secure key Method ", 2018 International Conference on Information, Communication, Engineering and Technology (ICICET), Narhe, Pune, India, pp.1-3, Aug 29-31, 2018.
3. Vinh Hoa LA, Ana Cavalli," Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey ", International Journal on AdHoc Networking Systems (IJANS), Vol. 4, No. 2, April 2014
4. Neetu Sharma, Hemlal Sahu, Birendra Kumar Sharma, "ID-Based Signature Scheme with Weil Pairing", Int. J. Advanced Networking and Applications, Volume: 05, Issue: 02, Pages:1893-1897, 2013.
5. Arpita chaudhuri, Suparna Dasgupta, Soumyabrata saha, "Identity based secure algorithm for VANETS" Published by Elsevier Ltd, Procedia Engineering 38, 2012.
6. Glymalakshmy G, Latha R Nair," Backbone –based Interflow Network Coding and RSA Encryption Technique in VANETs", International Conference on Intelligent Computing and control systems ICICCS 2017, pp.366-370,2017.
7. Pairing-Based Cryptography Library. [Online]. Avaialble: http://crypto. stanford.edu/pbc.
8. P. Suresha Barani, N. Edna Elizabeth," Registration and Verification of Vehicles in VANET's ", IEEE ICCSP conference, pp.1087-1092, 2015.

AUTHORS PROFILE

Dr. Vijayashree R Budyal received Ph.D degree in Electrical and Electronics from Visvesvaraya technological university Belagavi, Karnataka, India. She is currently working as Professor and Head Department of Mechatronics at Sri Venkateshwara College of Engineering Bengaluru, Karnataka, India. She has vast experience of more than 24 years in teaching. She received best research publication award from VGST, Karnataka in 2014. She has received a research grant by VGST Govt. of Karnataka, Bengaluru under Technology Related Innovative Project in the year 2015-16. To her credit she has published papers in reputed International Journals like Elsevier, Springer and IEEE conferences, about 42 papers in international conferences and 8 papers in International Journals. She has co-ordinated number of sponsored faculty development programme and presented many technical talks. She is a Fellow Institute of Engineers, member of IETE and ISTE. Her area of research includes Soft computing, Mobile Adhoc Networks, Wireless Sensor Networks, Distributed Mobile Computing, Vehicular Ad-hoc Networks.

Swapna Ch is currently pursuing her PhD in Visvesvaraya technological university Belagavi, Karnataka, India and received M.Tech Degree in Systems and Signal Processing from Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh.

She is currently working as an Assistant Professor in Department of Electronics and Communication Engineering at Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India. She has experience of around 11 years in teaching and 2 years in Research. She has published papers in reputed International Journals and Conferences. Her area of research includes Soft computing, Wireless Sensor Networks, **Vehicular Ad-hoc Networks, Network Security.**