Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.72 – 79

RESEARCH ARTICLE

Towards Secure and Dependable Ticket Based Tracing System for Obtaining Forgery Attacks in WMN

Chandan Y.N[1], Manoj Challa[2], K. Sundeep Kumar[3]

[1]Department of CSE, VTU University, Bangalore, India
[2]Department of CSE, VTU University, Bangalore, India
[3]Department of CSE, VTU University, Bangalore, India

[1] chandan.reddy@ymail.com; [2] manojcmrit@gmail.com; [3] sundeepkk@yahoo.co.in

Abstract— Privacy is a very important component in any network deployment now a day's. Users are willing to enjoy the network services without letting their identity. Anonymity comes in to picture which means not letting the user identity whenever he is accessing the benefits of the network. This anonymity condition is important for few services e.g. Social Networking. But there are few services where user has to revel his identity e.g. on-line payment system, Internet banking or on-line transaction. We are mainly concentrating on Wireless Mesh Network (WMN). However, not all the users are honest when they are using the network services; there are certain situations where users are involved in misbehaving activities. Consequently we need a system which revels user identity. Pseudonym techniques are the best for this. The systems will help to conditionally trace the honest users and misbehaving users in the Wireless mesh network. In this paper, A Secure Ticket Based tracing system is developed that mainly serves the above mentioned condition. Furthermore this proposed architecture not only used to trace the user activities, it is also guaranties to hold the fundamental security aspects like validation, endorsement, Data Protection.

Keywords: - Pseudonym; Anonymity; misbehavior; Tickets; Wireless Mesh Network

I. INTRODUCTION

Wireless Mesh Network is a promising technology to meet the challenges of the present generation for providing flexible adaptive and reconfigurable architecture. Wireless Mesh Network provides cost-effective business solutions. The network topology of a typical of a typical WMN depicted in the above figure. The wireless mesh backbone consists of mesh routers (MR), gateway (GW), they are connected normal wireless links. The access points here are GW, MR. They are finally connected to Internet. This topology mainly can be seen in Hospital, Campus, Enterprise and residential buildings.

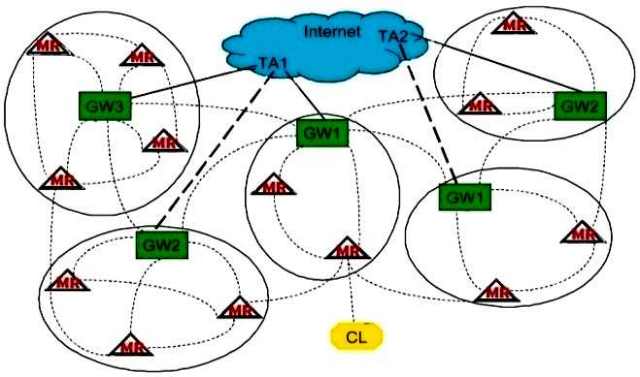

Fig 1. Network topology of a typical WMN

The cloud represents the service providers, where each service providers will have a Trusted Authority (TA) or Trusted Manager(TM). The solid and bold dash lines represent the association of TA and gateways with wired and wireless links respectively. Intensive task are handled by this gateway's and TM.

Security is the important factor that has to be considered before deploying any network. Wireless security is the hot topic in the literature for various network technologies. Anonymity and privacy issue have considerably gained a lot of attention [2][3]. Anonymity is important to hide the location information of the user to prevent tracing. Users are provided with the anonymity privileges to enjoy the services in the network [7]. There are certain situations where user might involve in doing some internal attacks, which here we are considering as the Forgery attacks. Once the user gains the access to the network it's not guarantee that all users will be loyal to the services which they are accessing. Misbehaving activities will takes place inside the network. In this Ticket based tracing system every user is provided with the Tickets, which are nothing but some of the access permissions inside the network. Even though tickets are provided users try to access non ticket services. Traceability becomes important to conditionally differentiate between the honest users and misbehaving users. In this paper we are motivated to remove the misbehaving users when internal attacks are made in our wireless mesh network. The initial system design was [1] which gives the idea of Ticket based secure system. But in this [1] we were not able to clearly understand the quality and usage of the architecture fully. As a result we provide a clear and detailed performance and feasibility in this paper. Wireless Spoofing attack will significantly impact the performance of network. To prevent this IP Spoofing attack we are implementing our tracing system with the filter [4].

Specifically the main scope of this paper includes 1) Providing Access to user via Issuing Tickets. 2) Forgery attack in depositing the ticket. 3) Sinkhole and IP spoofing attack to gain the unauthorized service or data. 4) List the fraud users in the network and remove these misbehaving users from the network by revoking the tickets which are issued.

II. RELATED WORK

In the system, as mentioned above Tickets are issued by the Trust Manager (TM). These tickets have to be deposited in the network before client gains the access. Here these tickets are nothing but the privileges given to users.

A. *Ticket Issuance*

To maintain the security of the network from the attack and to have the fairness between clients, the TM will have the access of each client by issuing tickets. Tickets from the TM will be issued depending of the client's misbehavior history. Ticket issuance takes place when client initially wants access to network or after tickets are revoked. The TM will not link the user identity with the ticket, because of this user will employ in blind identity to TM.

Some of the notations used here are as follows

->*:* single-hop communications;

->->*:* multi-hop communications;

||*:* concatenation;

ID_x*:* Identity of an entity x;

PS_x*:* the self-generated pseudonym by a client x by using his identity ID_x;

$H_1(ID_x)/\Gamma_x$*:* public/private key of the entity x;

PS_x/Γ_x*:* the self-generated pseudonym/private key pairs based on the above public/private key pairs;

$SIG_{\Gamma x}(m)$: signature on a message m using Γ_x;

VER(SIG): verification process; symmetric encryption on plaintext D using the shared secret key k;

$HMAC_k(m)$: keyed-hash message authentication code on amessage m using k;
C, TM, G : Client and Trust Manager, Gateway respectively;

1. $C->->TM: ID_C, m, t1, HMAC_K(m \| t1);$
2. $TM->->C: IDTM, X=e(m,\Gamma_{TM}), Y=e(P,Q), Z=e(m,Q), U=rH_1(ID_{TM}), V=rp,t_2,HMAC_K(X \| Y \| Z \| U \| V \| t_2);$
3. $C->->TM: ID_C$
   $B=1\lambda H_2(m'\|U'\|V'\|R\|W\|X'\|Y'\|Z')+\mu, t_3,HMAC_K(B\|t_3);$
4. $TM->->C: ID_{TM}, \sigma_1=Q+B\Gamma_{TA,}\sigma_2=(r+B)\ \Gamma_{TA}+rH_1(c),t_4,HMAC_K(\sigma1\|\sigma2\|t4).$

B. *Ticket Deposit*

When client obtain a valid ticket, the client has to deposit it in the network to experience the network services[1]. This scheme restricts in depositing the ticket only once at the entry. Here a batch of tickets is issued each time and the client may hold unused tickets. Since there won't be any separate expiry time for the tickets issued, they will expiry at once.

1. $C->->G:PS_C,m',W,c,\ \sigma = (U',V',X',\rho,\sigma'_1,\sigma'_2),t_5, SIG_{\Gamma c}\sim(m'\| W \| c\|\|\sigma\|\|t_5);$
2. $G->->C:ID_G,d=H_3(R\|\|W\|\|ID_G\|\|T), t_6,HMAC_K(d\|\|t_6);$
3. $C->->G:PS_C,r_1=d(u_1\alpha)+v_1, r_2=d\alpha+v_2,t_7,HMAC_{K'}(r_1\|\|r_2\|\|t_7);$ *and*
4. $G->->C:ID_G,misb,exp,t_8,SIG_{TG}(PS_C\|\| ID_G\|\|misb \| \| exp \| \| t_8)$.

C. *Ticket Revocation*

When the client is compromised, reveling all his identity and secret to the advisory the tickets will be revoked. A valid revocation must be sent by compromised user to gain genuine tickets again. A record of the revocation report will be sent to the TA, which will update and distributes the tickets to the users again.
The main retreat is, Tickets which are deposited by one user might deposit by even others, i.e. if User A is provided with ticket number 2, and User B is provided with ticket number 3 then if A indulges in having the access of B, by knowing B's ticket number, A can clearly go ahead and deposit the Ticket[6]. Attacks showed that the client can impersonate the Pseudonym Manager to sign some tickets. There was no sign of tracing the misbehaving users. Clients who deposit the wrong ticket only traced. Cryptographic techniques which are used to provide the security for the data was not up to the expectation, i.e. DES techniques were used. Analysis clearly showed that Ticket Based anonymity scheme cannot satisfy the traceability [6].

III. PROPOSED SYSTEM

A. *Software Architecture*

Pseudonym manager will first have the access to the network. He will set a system .The next step of PM is to create a new user who seeks to enter in to the network. PM will be granting the tickets along with the user creation. Now user has to get connected to the servers to enter in to the Wireless Mesh Network through the Server which is shown in Fig 2.

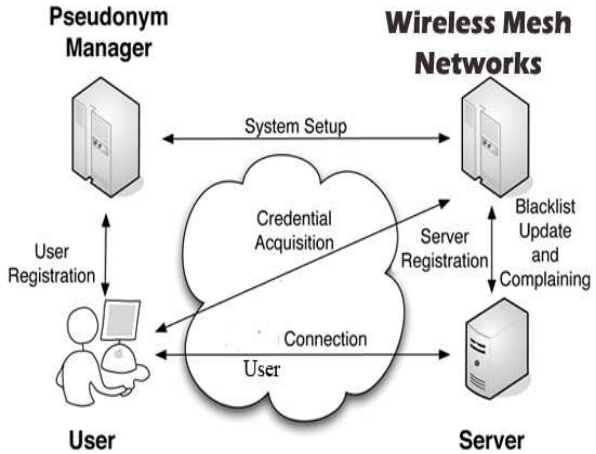

Fig 2: Software Architecture for proposed system

Server will be collecting all the activities of the user. If the user under goes any misbehaving activates which we have mentioned in above section, the report of that will be provided to the PM. User will have the credential

Acquisition to the WMN. The below section let us see how the user will misbehave and how it has been controlled.

B. *Forgery Attack In Depositing The Ticket*

Forgery, Fraud and misbehaving are used interchangeably in this section, which is mainly an insider attack. The reuse of ticket from the user generally means that whenever user fails to acquire the tickets from the PM. This may be due to the past misbehaving history of the user which causes the PM to constrain the ticket request. Multiple-Deposit can also be termed users coalition, which is useful when the coalescing parties are unauthorized users with misbehaviour history having difficulty in acquiring ticket from the PM.

A possible remedy to this situation is to specifying the no overlapping activity period of a ticket instead of merely the expiry date/time such that each time only 1 ticket is deposited. Another solution is to adopt the tamper proof secure module so that a client or user cannot disclose his secret to other parties. This approach will eliminate the multiple deposits of tickets. PM Will detect duplicate deposit using the ticket record report by the Server.

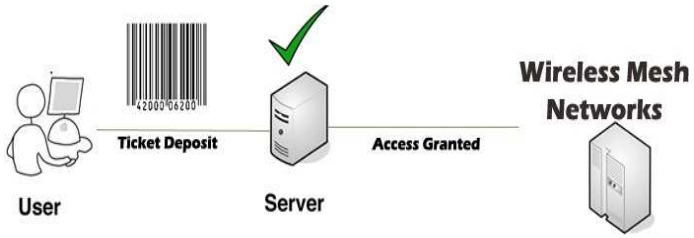

Fig 3: Valid ticket deposition by user

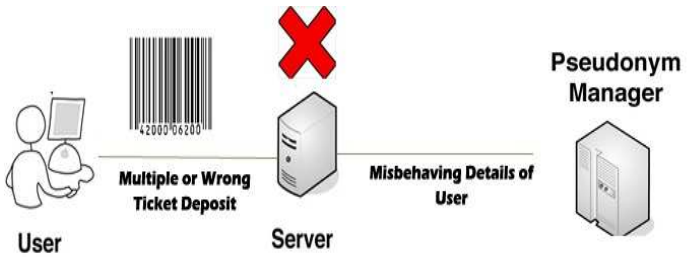

Fig 4: Invalid ticket deposition by user, misbehaving details sent to PM.

Here we are linking the user Identity with the tickets, which will be issued to the user. If the client or the user misbehaves, the client anonymity is no longer guaranteed because PM will identify this user, and accordingly penalize him by revoking the client network access privileges by investing traceability property offered by our security architecture.

C. *Sinkhole Attack*

The sinkhole attack is a particular node attack that prevents the base station from obtaining complete and correct data, thus forming a serious threat to higher level protocols[8]. In a sinkhole attack, a compromised node tries to draw all or as much traffic as possible from particular nodes. Making it look attractive to the surrounding nodes with respect to the routing metric values .Figure 1 explains how malicious node redirects with modified route sequence numbers. Here malicious node sends greater sequence number to misguide that it is a fresh route. Figure 2 depicts how malicious node redirects with modified hop count. Here malicious node sends lesser hop count value to tell that this is shortest path. In fact there is no such path exists. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, M absorbs all the data. So the attacks can be accomplished [9].

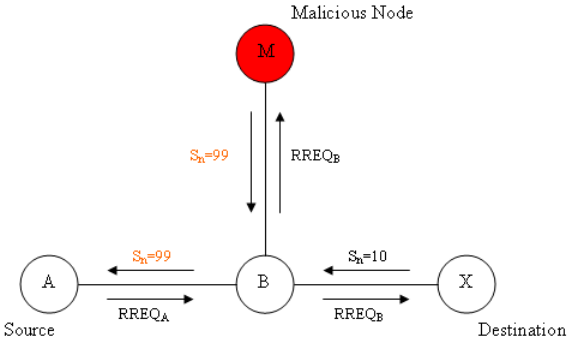

Fig.5 Sinkhole attack with modified sequence number

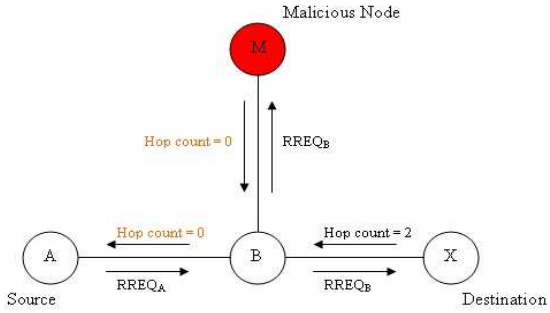

Fig.6 Sinkhole attack with modified hop count value

Just advertising a link with high quality for other nodes might not be enough. Since most of the protocols which are present try to be robust, it means they don't allow a frequent change in parent for no good reason(parent is source and child is destination). For ex. When parent try to change node, routing cycle in the network is created, this will cost extra effort to resolve. Therefore, beside from advertising a higher link quality from itself, another way for the attacking node to launch the sinkhole attack is to make a current parent look like they have a very poor link quality which triggers the parent changing mechanism in the children. To prevent this attack PM in our proposed system will predefine the source and the address communication. As we discussed above if parent tries to send the packets or data through some other nodes, soon the details will be sent to PM by the server. PM will eliminate this parent from the network preventing further attacks.

D. *IP Spoofing*

In networking the term IP address Spoofing or IP spoofing refers to the creation of internal protocols packets with forged origin [5]. IP address, call spoofing, with the purpose of concealing the identity of sender or impersonating another computing system. The basic protocol sending data over the Internet network and many other computer network is IP. The packet with IP header contains, along with other things, the numerical sender and receiver address of the packet. By forging the header so it contain a different address, an assaulter will make it look like that the packet was actually sent by a dissimilar machine. When machine receives the spoofed packets will normally send a reply back to the forged source address. IP spoofing is most frequently used a Denial-of-service attack. In such attack the goal is to flood the victim with overwhelming amount of traffic, and the attacker does not care about receiver response to the attack packets. They have additional advantage for this purpose they are more difficult to filter since each spoofed packet appears to come from different address, and hide true source of attack. Below figure shows the simple spoofing attack in the network.

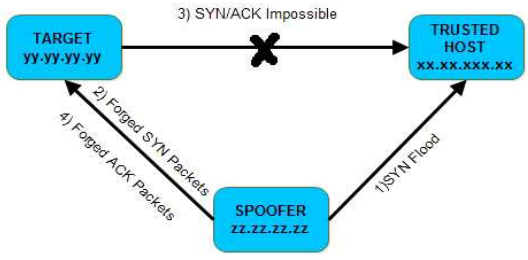

Fig 5 : Spoofing attack

Packet filtering is one of the defense against IP Spoofing attack. The gateway to the network is usually performs Ingress Filtering, block's the packets from outside the WMN with a source address inside the WMN, i.e. Ingress Filtering ensures that outgoing packets of a deploying selected carry an "Inside" source address and incoming packets carry an "Outside" source address[5].

$$Strength_F = 2.\ |IP_{ing}|\ .\ |IP_{allc} - IP_{ing}| = |IP_{allc}|^2$$

Because the extends address space is always much larger than the internal one. Ingress Filtering prevent from random-spoofing by the participating network and is thus an altruistic defence.

Data security also plays a very important role in any network or topology. As we have already mentioned that our system will also concentrate on the fundamentals of security i.e. data security and authentication. For this our system will make use of two famous algorithms 1)RSA Public Key Generation 2) Random Number Generator.

E. *RSA Public Key Generators*

RSA make use of two keys i.e. a public key and a private key. Encryption of any message is done using the public key, which is known to everyone. This encrypted message with the public key can be decrypted in a considerable amount of time with the private key.

The RSA Key Generation makes use of following steps :

1. Select two discrete prime numbers p and q.
2. Work out $n = p.q$
3. Calculate $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function.
4. Prefer an integer e such that $1 < e < \varphi(n)$ and $GCD(e, \varphi(n)) = 1$;
5. Determine d as $d^{-1} \equiv e\ (mod \varphi(n))$, i.e., d is the multiplicative inverse of e *(modulo* $\varphi(n)$*).*

By calculation, $d \cdot e \equiv 1 (mod \varphi(n))$.The modulus n which is part of public key and the exponent e for encryption. The modulus n which is the part of private key and the exponent d for decryption, which must be kept hidden. p, q, and φ(n) must also be kept confidential because cryptanalyst might use it to calculate d. The RSA is considered to be the best for its convenience way for security, because the sole responsible of the key is user itself compared to any other asymmetric key cryptography.

F. *Random Symmetric Key Generator*

A random number generator (RNG) is device designed to generate a sequence of symbols or numbers with any pattern. Many applications are stated to make use of this random number generation. Since ancient times, including coin, dice the playing card which are shuffled, and many other techniques. The mechanical nature of these techniques, to generate large numbers of random numbers required a lot of time and man power. Nowadays, after the invention of computational random number generators, people started using it in lottery game, instead of more traditional drawing methods RNGs are used. Even today to find any odds in slot machine RNGs are used. Random number generators (RNGs) are algorithms can automatically generate long runs of numbers with beneficial random properties. The value of the string which is generated by this is determined by a fixed number called Seed. One of the most common RNG is the linear congruential generator, which makes use of the recurrence to generate any numbers.

$$X_{n+1} = (aX_n + b)\ m = mod\ m$$

Modulus represents the maximum number of numbers the formula can produce. There are certain non-random number properties of a single linear congruential generator, to avoid this several such random numbers with slightly different values of a can be used in parallel with initial or master random number generator that selects from different generators. John Von Neumann proposed simple pen-and-paper method for generating random numbers is the so-called middle square method. Which was very simple to implement, its output is of poor quality. Now a day's most computer programming languages admit functions or library routines that aim to be random number generators. Basically they are designed to often provide a random words or bytes, or a floating point number but uniformly distributed between 0 and 1. In the proposed system this random number generator is used for password or we can say as authentication key for the user. This is generated at the time of creation of new user from the PM. These keys are distributed to the users.

IV. **RESULT**

Our Security architecture will clearly shows about the internal attack that user may indulge. Depending on these attacks, the system has proposed a solution for attacks i.e. Forgery attacks in depositing the tickets, Sinkhole attack which is considered as a serious threat in the network, IP Spoofing which the system will control the attack by implementing the ingress filter technique. This is considered to be the secure in ticket based tracing system for conditional anonymous user and tracing misbehaving users in anonymous Wireless Mesh Network.

Below Fig(6) show the Tickets or privileges provided to the users and number of attempts where he misbehave. X-axis shows the type of tickets issued and Y-axis show the number attempts. This system helps us to understand where exactly the number attack happens.

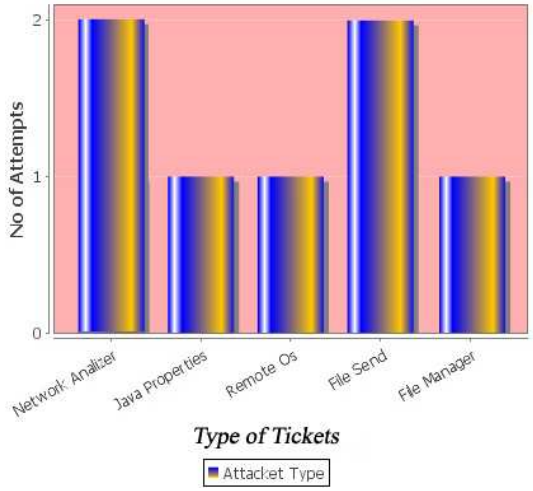

Fig 6: Type of tickets issued and number of misbehaving attempts made.

V. CONCLUSION

The principles behind next generation network security architectures proposed by various parties to address some of the most critical shortcomings faced by the Internet today. The proposed solutions while successful in solving the issues of resolve the conflicts between the unconditional anonymity for honest users and traceability of the misbehaving users. Internal attacks are clearly seen and have the perfect solution to prevent. Misbehaving users will no longer exist in the network to use any further services, they are completely eliminated. The proposed architecture is demonstrated to achieve desired security objective and efficiency. The future work of this may include the implementation of different types of filters for IP Spoofing.

REFERENCES

[1]. J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "*SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks*," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 295-307, 2011.

[2]. M. Raya and J-P.Hubaux, "*Securing Vehicular Ad Hoc Networks*," J. Computer Security, special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39 68, 2007.

[3]. Y. Zhang and Y. Fang, "*ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks*," IEEE J. Selected Areas Comm., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[4]. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, and Jerry Cheng "*Detecting, Determining and Localizing Multiple Spoofing Attackers in Wireless Networks*". Ieee transactions on parallel and distributed systems, vol. 24, no. 1, january 2013

[5]. Ezra Kissel, University of Delaware and Jelenairkovic, USC/ISI"*Comparative Evaluation of Spoofing Defenses*"

[6]. Huaqun Wang and Yuqing Zhang, Member, IEEE" *On the Security of a Ticket Based Anonymity System with Traceability Property in Wireless Mesh Networks*" IEEE transactions on dependable and secure computing, vol. 9, no. 3, may/june 2012.

[7]. Matt Blaze1, John Ioannidis2, Angelos D. Keromytis3, Tal Malkin3, and Avi Rubin" *Anonymity in Wireless Broadcast Networks*" International Journal of Network Security, Vol.8, No.1, PP.37–51, Jan. 2009.

[8]. HassenRedwan and Ki-Hyung Kim Department of international communication and Engineering"*Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks*" Japan-China Joint Workshop on Frontier of Computer Science and Technology 2008.

[9]. D. Sheela, Nirmala. S, SangitaNath and Dr. G Mahadevan *"A Recent Technique to Detect Sink Hole Attacks in WSN"*

AUTHORS

Mr. Chandan Y N is presently doing Master of Technology in Computer Networks and Engineering at CMR Institute of Technology, Bangalore, Karnataka. He obtained is Bachelor of Engineering degree in Information Science and Engineering from Sri Krishna Institute of Technology, Bangalore, Karnataka in the year 2011.

Mr.Manoj Challa is pursuing Ph.D(CSE) in S.V.University, Tirupati, India. He completed his M.E(CSE) from Hindustan College of Engineering, Tamil Nadu in 2003. He is presently working as Associate Professor, CMR Institute of Technology, Bangalore. He presented nearly 18 papers in national and international conferences. His research areas include Artificial intelligence and computer networks.

Mr.Sundeep Kumar K received the M.Tech (IT) from Punjabi University in 2003, ME (CSE) from Anna University in 2009 and pursuing Ph. D (CSE) from JNTUA. He is with the department of Computer Science & Engineering and working as an Associate Professor, CMR Institute of Technology, Bangalore. He presented more than 10 papers in International and national Conferences. His research interests include OOMD, Software Engineering and Data Warehousing. He is a life member in ISTE.

