ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8 , August 2017

Hybrid Crypto-System Approach use in Secure Intrusion Detection System for MANET

[1] Mr. Ajit N. Gedam, [2] Prof. M. P. Wankhade
[1] ME (Computer Network), [2] Associate Professor
[1][2] Department of Computer Engineering, Sinhgad College of Engineering
Vadgaon (Bk), Pune. 411041

***Abstract*— Recent emerging trends in the world, many firewalls and Crypto-System mechanism play a vital part in network security. However, many of them protection mechanisms are not adequate and effective. Therefore, the study of (intrusion detection system) IDS goes increasing to monitor the network that notices misbehavior or anomalies and notifies to other nodes in the network to avoid the nodes misbehaving. Authentication and encryption acts as first phase of defense while an IDS acts as a second phase of defense. In Mobile Ad hoc Networks (MANET), many schemes are existing for intrusion detection system. One of the intrusion detection system used in MANET is Enhanced Adaptive Acknowledgement (EAACK), which is based on acknowledgement packets for detection of malicious activities. This system increases the network overhead significantly relative to other system. So, in this paper we adopt the hybrid Crypto-System Approach to reduce the network overhead cause by using digital signature in EAACK. The system is termed as Hybrid Crypto-System as it gives an improved security than the fundamental approaches. The concept of Hybrid Crypto-System used which include AES and RSA algorithm. This system proves advanced malicious behavior detection rates and packet delivery factor is improved and enhance the security**

***Keywords*— MANET, EAACK, Digital Signature, ACK, S-ACK, MRA, DSA, RSA**

I. INTRODUCTION

Mobile ad hoc network is an infrastructure less, self-maintained and self-configured network of mobile nodes. Directly or indirectly, they can communicate with each other in direction, have been transmitting and receiving factor in the wireless network. Mobile ad hoc networks are useful for the communication by using mobile devices in a disaster conditions like flood or earthquake, when the network infrastructure is unavailable. MANET mainly divided into two different networks one is called as single-hop network which exists in the same line of sight communication range which can interact directly with each other, i.e. in between there is no any intermediate nodes present. Moreover, another is known as multi-hop network in which if the destination node is out of their radio range, nodes rely on intermediate nodes to transmit.

In this paper, to deal with different issues related to security of the network, the focus is on cryptographic techniques used in intrusion detection systems [8] for MANET which will acts as a second phase of defense. A hybrid cryptography is proposed to improve existing secured MANET, which consists of mainly three parts attack prevention, enhanced security services, and misbehavior report.

The main purpose of this work is to present an advanced system, which is designed especially for MANET, to not only solve security issues and services but also false misbehavior report problem from source to destination during the packet transmission.

II. CRYPTOGRAPHIC TECHNIQUES

For securing the network, cryptography algorithm is necessary to be implemented. The cryptographic algorithms are fundamentally divided into two type's symmetric encryption algorithms and asymmetric cryptographic algorithm likewise called as public key cryptographic algorithms [5]. Symmetric encryption is oldest and best-known technique as shown in Figure 1. A secret key, which can be a number, a word or a just string of random letters, is applied to the text of message to change the content in a particular way. This is similar to be as simple as shifting each letter by a number of places in alphabet. Sender and recipient can encrypt and decrypt all message until they know secret key [6].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Figure 1: Symmetric Encryption

The main difficulty with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong mobile node. Any person who possesses the required secret key can decrypt the message. Therefore, the distribution of key securely over a channel is one of the challenging task related to symmetric key cryptography.

To manage such issue, we can utilize another technique called asymmetric key or public key cryptography in which there are two related keys, the pair of keys shown in figure 2. A public key is made uninhibitedly accessible to any individual who might need to send you a message. Another key, private key is kept secret so that only recipient know it. Encryption of any message using public key must be decrypted by applying the same algorithm, but by using the same private key [5]. Decryption of any messages, which is encrypted utilizing the private key, is possible by utilizing only the same public key. This implies that you don't need to stress over ignoring public keys the over Internet (the keys should be public). But asymmetric encryption is slower than symmetric encryption is the main problem. It requires much additionally preparing time to both encryption and decryption of message.

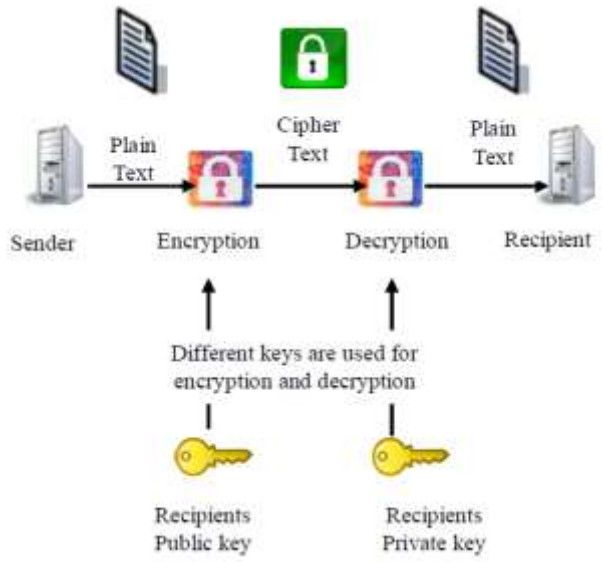

Figure 2: Asymmetric Encryption (RSA)

In asymmetric encryption it is required to find other public keys and there must an approach to find those public keys. The ordinary system is to utilize digital certificates. A certificate is a bundle of proof that recognizes a client or a server, contains confirmation, for example, the association name, the association that issued the certificate, the user's e-mail address and country, and the user's public key. At the point when a server and client require a protected scrambled correspondence, they send an inquiry over the network to the next party, which sends back a duplicate of the declaration. The other party's public key can be extracted from the certificate. A certificate is an entity also be used to identify uniquely the users [6].

III. LITERATURE SURVEY

The author depicts in [1] the performance of the digital signature in EAACK for the prevention of forging acknowledgment packets from the attacker. EAACK is consists mainly three parts, Secure-Acknowledge (S-ACK) [7], Acknowledge (ACK), and Misbehavior Report Authentication (MRA). To flag different types of packet two of the six bits were used in EAACK. It is presumed that the link between each node in the network is bi-directional in this scheme. Furthermore, both the source node and the destination node are not to be malicious for each communication process. All acknowledged packets are required to be digitally signed by its sender and confirmed by its receiver.

The author in [2] intends to study two major modules, named watchdog and path rater, to mitigate and detect, respectively. Nodes are operated in promiscuous mode in which the watchdog node overhears the medium to verify if the next-hop node forwards the packet successfully. It keeps a buffer of recently sent packets at the same time, when the watchdog overhears the same packet being forward by the next-hop node over the medium a data packet is vacant from the buffer. Then the watchdog module accesses the misbehaving next hop neighbor if the data packet will remain in the buffer for long time. Therefore, at the progressing level the watchdog enables misbehavior detection of the node.

The Author in [3] addressed the TWOACK scheme to detect misbehaving links on each three succeeding nodes by acknowledging every data packet transmitted along the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

path from the source node to the destination node. Every two successor nodes have send back acknowledgement to sender.

The author in [4] paper, an Enhanced-TWOACK (E-TWOACK) is considered as an AACK acknowledgment based scheme which is a grouping of ACK and TWOACK system. This system detects misbehaving node instead of misbehaving link [6] [9], and it is an end-to-end acknowledgment scheme. It works in two phases first it works ACK normal mode if there is any malicious activity found it enters into TWOACK mode, as a result minimized routing overhead of TWOACK. The AACK may not work on long distance route, as it will require a significant amount of time for the endwise acknowledgments. Because of this drawback, more time is required for dropping more packets to a misbehaving node [10] [11] [12] [13]. The issues are AACK still suffers from the partial dropping attack i.e. gray hole attacks and false misbehavior report.

IV. EXISTING METHODOLOGY AND ALGORITHMS USED IN SECURE IDS WITH DIGITAL SIGNATURE

Intrusion detection system (IDS) is responsible for the detection of internal as well as external misbehaving actions in mobile ad hoc networks. EAACK [1] serves as IDS for MANETs, which is based on acknowledgement packets in response to received data packets for detection of abnormal activities in the network. This is a hybrid system, which consist of mainly three phases namely acknowledgement (ACK), secure acknowledgement (S-ACK) and misbehaviour report authentication (MRA) as explained in [1]. Due to the adaption of digital signature to authenticate the acknowledgement packets for detection of false misbehaviour reports, there is increase in network overhead. So, it is necessary to reduce that increased overhead to acceptable values in order to enhance the network performance by using EAACK. In existing system, digital signature algorithm is used for authentication of acknowledgement packets as shown in Figure 3. In existing systems authors in [1] implemented both RSA and DSA methods. The network overhead of RSA is considerably larger than DSA. Routing overhead depends on the number of malicious nodes and will vary with change in number of malicious nodes. An application generates a random symmetric key to encrypt a message. The symmetric key is encrypted with the public key and transmitted with the encrypted message. At the receiver end symmetric key can be decrypted by using private key.

A. Existing System with DSA Approach

In existing system, DSA (Digital Signature Algorithm) [14] is used to transfer the message with signature of user access. An important part of the cryptography is digital signature. It is a part of security of data and it deals with the encryption and decryption mechanisms [15]. It includes the security of information like authentication, data integrity, and confidentiality. It divides into two categories.

1. Digital signature with addition: It is needed an original message in the signature verification algorithm. Examples contain a digital signature algorithm (DSA).
2. Digital signature with retrieval of message: In this type, the signature is required rather than the information in the process of verification. Examples contains RSA.

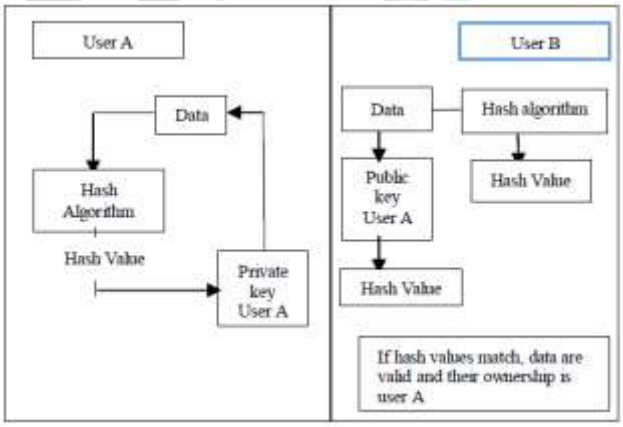

Figure 3: Digital Signature

B. Existing System with RSA Approach

RSA stands for the name of the three researchers Ron Rivest, Adi Shamir and Leonard Adleman who designed it. Two major prime numbers factorization is utilized as a part of RSA. It comprises of a public and private key. The public key is being used for Encrypting messages and known by everybody. RSA utilized Public key for secure transmission of information or data. For encrypting,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

public key is required key and private key is required for decrypting the data as shown in figure 2.

RSA Algorithm

Step 1. Select two major prime numbers as p and q.
Step 2. The two variables p and q are to be chosen constantly at odd and should be of similar bit for security guidance.
Step 3. Compute m= p * q, such that the modules for both the private and public key.
Step 4. Calculate $\phi = (p-1)(q-1)$.
Step 5. Randomly choose an odd integer t such that t and ϕ comparatively prime and $t < \phi$.
Step 6. (gcd (t, k) =1) Where t is released as the Public Key exponent (gcd-greatest common divisor).
Step 7. Generating decryption key formula is dk = t -1 mod ϕ.
Step 8. The pair of Public Key is (t, k) and Private Key is dk.

RSA also termed as "Public key Cryptography or Asymmetric Key Cryptography" [5], which works with two keys generally i.e. public key and the private key. In RSA algorithm, two keys i.e. public and private keys are utilized and produced. Public key is accessible to everybody, which is common key whereas private key is not accessible to everybody and is not common key.

V. PROPOSED SYSTEM

A. Hybrid Crypto-System

A hybrid Crypto-System consists of mainly two different parts i.e., key encapsulation and data encapsulation scheme. Key encapsulation scheme also known as public-key or asymmetric key cryptosystem. Data encapsulation scheme is known as symmetric-key cryptosystem. Sometimes many malicious nodes are existing in the network that requires more acknowledgement packets, at that time the percentage of digital signature in the entire network overhead is high. To reduce the network overhead caused by the digital signature in EAACK, a hybrid Crypto-System is proposed. By using hybrid Crypto-System, routing overhead reduced even in the presence of malicious nodes. Our propose system which consists of AES along with RSA. By using these methods speed and security of the network expressively boosted. For data transmission, the secure route is to be find out first by using reactive routing protocol called AODV (Ad hoc On-demand Distance Vector) which finds the route to the destination whenever essential and then sender sends a data to the destination securely.
The encryption with a hybrid Crypto-System takes place as follows: First, the symmetric key is generated using RSA algorithm. Then with generated symmetric key the original packet is encrypted using AES algorithm. The symmetric key is encrypted with the public key of RSA algorithm. Now the encrypted packet and key is sent to the receiver side as shown in figure 4.

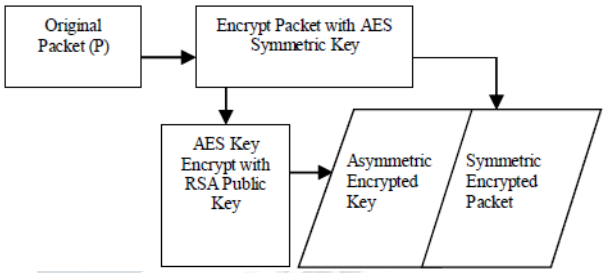

Figure 4: Encryption with Hybrid Cryptosystem

The decryption with hybrid Crypto-System takes place as follows as shown in figure 5. First asymmetric encrypted key is decrypted with the private key using RSA algorithm. Using AES key, encrypted packet is decrypted and then original packet will be the output.

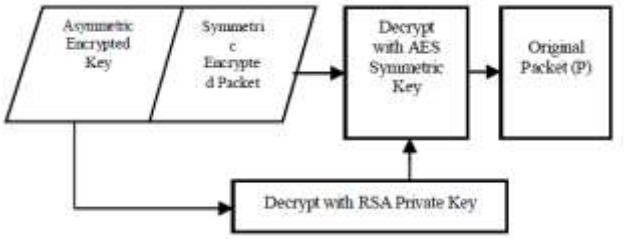

Figure 5: Decryption with Hybrid Cryptosystem

B. Proposed System Architecture

The Packet is send from Source node to the number of destination nodes hence the activated path can be anyone. When packet is sent from the source node to successive node then back acknowledgement is sent to the source node, is called activation node. When provided packet,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

text, data is reached at destination node then destination node sent back acknowledgement to the source node with the same root. At the same time, the text, data, packet is encrypted at the source node. In this proposed work, AES is used for symmetric encryption and RSA is used for asymmetric encryption. Packet, text, data, is decrypted at original message when it is reached at destination node. Proposed system architecture is shown in figure 6.

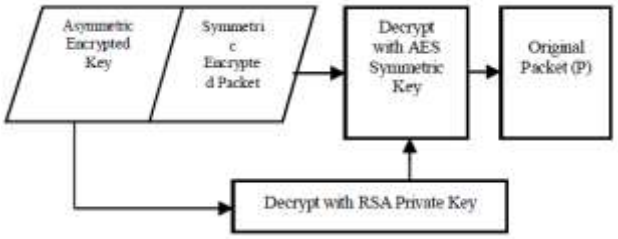

Figure 6: Proposed system Architecture

VI. PERFORMANCE EVALUATION

The simulation is done with the help of network simulator (NS3.20) running on a fedora LINUX platform.

- Testing and Result Analysis (Test Scenario)

PARAMETERS	PERFORMANCE
Data packet received	Increased by 55.1%
Packet Delivery Ratio	Increased by 15.4%
End to End Delay	Increased by 29.4%
Packet Overhead	Increased by 25.2%

Scheme	Packet Delivery Ratio
EAACK AES-RSA	0.97
EAACK DSA-RSA	0.94

A. Packet Delivery Ratio (PDR)

It is the ratio of the total number of received packets at the destination to the total number of sent packets by the source.

$$PDR = \frac{\sum Received\ packet\ at\ destination}{\sum Sent\ packet\ by\ source}$$

B. Routing Overhead (OH)

It is the ratio of routing related packets in bytes (RREQ, RREP, RERR, AACK,) to the total routing and data transmissions (sent or forwarded packets) in bytes. That means the acknowledgments, alarms and switching overhead is included.

$$OH = \frac{\sum \text{Routing transmissions}}{\sum \text{Data transmissions} + \sum \text{Routing transmissions}}$$

C. Average end-to-end delay (D)

D is the average end-to-end delay for all successfully received packets at the destination. It is calculated for each data packet subtracting the sending time of the packet from the received time at destination.

$$D = \frac{\sum(\text{TRceived} - \text{Tsent})}{N}$$

Where, N is number of successfully received packets

VII. EXPERIMENTAL RESULTS

The following graphs helps to analyzing the performance between existing scheme and proposed scheme. The below figure 7, shows the no of packet received with speed of 100000, 200000, 300000, 400000, 500000, 600000 milliseconds and compared with the existing system.

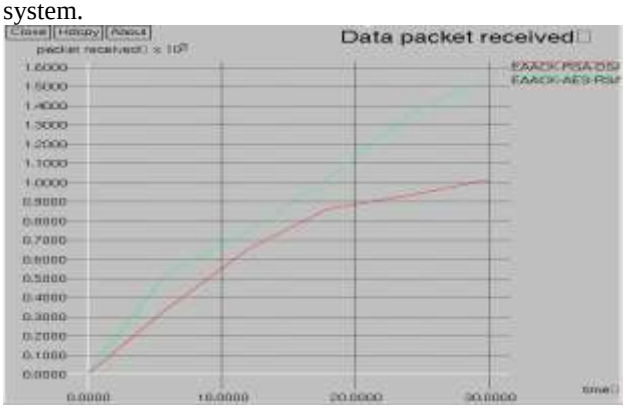

Figure 7: Comparison of data packet received in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

EAACK AES-RSA with EAACK-DSA-RSA

Figure 8: Comparison of packet delivery ratio in EAACK AES-RSA with EAACK-DSA-RSA.

The packet delivery ratio can be defined as the ratio of total no of packet received by total no of packet sent. Proposed system achieves high throughputs even when the mobile nodes travel at a relatively high speed. As the nodes start to move faster, the throughput of the proposed approach gradually drops and eventually degrades, when the nodes travel much faster. It clearly shown in figure 8 that delivery ratio is better in the proposed system.

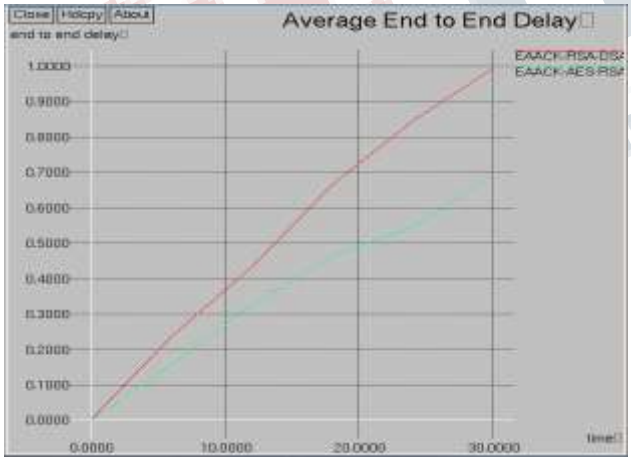

Figure 9: Comparison of Delay Performance in EAACK AES-RSA with EAACK-DSA-RSA.

Figure 9 shows the average end-to-end delay in proposed system is reduced by 29.4% as compared with existing system.

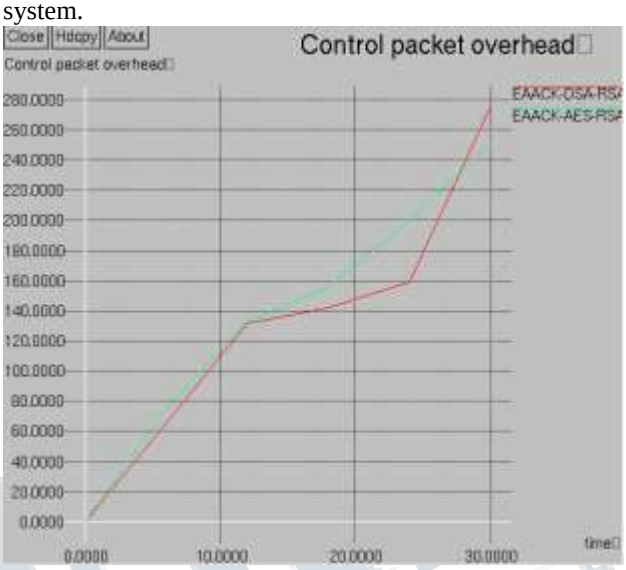

Figure 10: Comparison of Control Packet overhead in EAACK AES-RSA with EAACK-DSA-RSA.

As shown in figure 10, control packet overhead is reduced by 25.2% by using AES-RSA hybrid Crypto-System.

VIII. CONCLUSION

This proposed work, design a hybrid Crypto-System to presented the both symmetric-key (AES) and asymmetric key (RSA) cryptographic algorithms with EAACK system. This system has a powerful prevention control, which is one of the important and necessary conditions to guarantee the security of the data and it will become difficult for attacker to breakdown the network as well as retrieval of the information. The main purposed of this system is to reduced network overhead and increased packet delivery ratio.

ACKNOWLEDGMENT

I would like to take this prospect to express my profound appreciation and deep regard to my guide Prof. M. P. Wankhade for his exemplary guidance, valuable feedback and unvarying back up throughout the duration of the project. His priceless suggestions were of immense help throughout my project work. His observant analysis kept me working to make this project in a much better way.

Working under him was an extremely conversant experience for me.

REFERENCES

[1] Shakshuki Elhadi M, Senior Member, IEEE, Nan Kang, and Sheltami Tarek R., Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE transactions on Industrial electronics, Vol. 60, No. 3 March 2013.

[2] Marti S., Giuli T. J., Lai K., and Baker M.. "Mitigating Routing Misbehavior In Mobile Ad hoc Networks". In the Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, ACM, pp. 255-265, Boston, Massachusetts, US, 2000.

[3] Balakrishnan K.; Jing Deng; Varshney, V. K., 2005 "TWOACK: preventing selfishness in mobile ad hoc networks", In Proceedings of Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp.2137-2142(March 2005).

[4] Liu K., Deng J., Varshney P. K. and Balakrishnan K., 2007, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs". IEEE Transactions on Mobile Computing, May, 536-550.

[5] William Stallings, "Cryptography and Network Security", Fourth Edition, June 3, 2010.

[6] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[7] Kang, N., Shakshuki, E and Sheltami, T., 2010." Detecting Misbehaving Nodes in MANETs", In Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services (iiWAS2010), ACM, pp. 216-222.

[8] Kang, N., Shakshuki E and Sheltami T. 2011 "Detecting Forged Acknowledgements in MANETs", The 25thInternational Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society, Biopolis, Singapore.

[9] Alriyami Qasim M., Asimakopoulou Eleana, NikBessis School of Computing and Mathematics, University of Derby, UK "A Survey of Intrusion Detection Systems for Mobile Ad-Hoc Networks". 2014 International Conference on Intelligent Networking and Collaborative Systems.

[10] Samreen Shirina , G. Narasimha "An Efficient Approach for the Detection of Node Misbehaviour in a MANET based on Link Misbehaviour" 2013 3rd IEEE International Advance Computing Conference (IACC).

Ajit Narendra Gedam received the B.E. from YCCE Nagpur, Rastrasant Tukdoji Maharaj Nagpur University, Nagpur and Pursuing M.E degree in Computer Engineering (Computer Network) from Sinhgad college of Engineering, Pune,

Prof. M. P. Wankhade (HOD) Associate Professor in computer engineering department, Sinhgad college of engineering, Wadgaon (BK), Pune.