www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20606-20610
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.37

Adaptive Acknowledgement Techniques to Improving Security for MANETs Using MRA Scheme

[1]C.Muthupriya, [2]G.Sivakumar, [3]Dr.K.Ramasamy
[1] PG Student ,[2] Assistant Professor , [3]Principal
[1,2]P.S.R.Rengasamy College Of Engineering for women, Sivakasi
Email: [1] priya201994@gmail.com, [2] gsivakvp@gmail.com, [3]ramasamy@psrr.edu.in

ABSTRACT
The favour of wireless networks over wired networks has been increasing for the past few decades. The flexibility and accountability brought by wireless networks makes it preferable for several applications. In this midst all the present-day wireless networks, Mobile Ad hoc network (MANET) is among the most important types having distinctive applications.Each node in the Manet has a wireless interface to Communion with each other. In the Propone system adaptive acknowledgement approach (AACK) Digital signature algorithm is used which increases causes the network overhead if more malicious node involved. Thus system is used with Rijndael algorithms as a session key cryptography to reduce the network overhead caused by digital signatures in AACK. It scope of hybrid encryption is combination of Rijndael algorithm and RSA for the acknowledgement packets

Keywords
Mobile Ad Hoc Networks (MANET), Intrusion Detection System (IDS), Adaptive ACK,,,AODV, RivestShamiAdleman , Rijndael Algorithm and Digital Signature.

I. INTRODUCTION
MANET (Mobile Ad hoc network) is a set of mobile nodes consists of both a wireless transmitter and receiver connect with each other using bidirectional wireless links. Delegated as a peer to peer system each node or user in the network behaving as a data endpoint or intermediate repeater. MANETs are frequentlya self-forming, self- maintained and self-repairs itself process allowing for extreme network flexibility, which is generally used in penetrating mission appplications like military purposes or emergency recovery, the minimum composition and quick distribution of nodes in preparation for work make MANET ready to be used in emergency circumstances. MANET is becoming more and more widely implemented in the industry. Manet iscontinuously self-maintained, support network of mobile devices that are connected without wires. These have highly dynamic and free topology. The contrary to traditional Network architecture, Manet does not require a stable network infrastructure; every single node works as both transmitter and the receiver. Nodes communicate directly with each other when they both with the communication range .The routing algorithm in MANET can be a single hop or multi hop .single hop communication is simpler in terms of structure and implementations but has lesser functions and application compared to multi hop communication. In multi hop communication, the destination is raised the transmissioncoverage of the source and hence the packets are forwarded via one or more intermediate nodes Fig.1 shows a MANET network consisting of nodes and their transmission ranges.
As shown in Fig.1, Node 2and Node 3 neighbours of node 1whilst Node 4 and Node 5 are not .Therefore, data transmission to Node 4 and Node 5 will have to be relayed by Node 2.

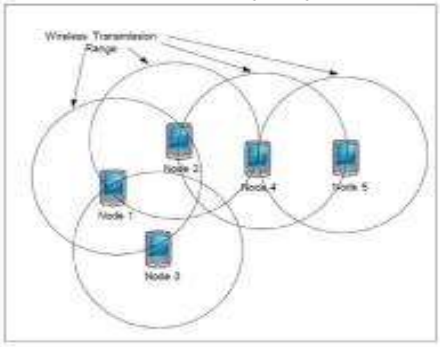


Fig 1. Representation of Manet

Manet is highly vulnerable to attacks because node configuration and maintenance are done on its own .In such case, it is crucial develop efficient Intrusion detection mechanisms (IDS) to protect MANET.

II. RELATED WORK
Elhandi M. Shakshuki, Nan Kang, Tarek R. Sheltami, the author has explains peculiar intrusion detection in MANETs and its disadvantages. EAACK supported for solving false misbehaviour report problem and some new techniques, which are related to the enhanced adaptive acknowledgement. The techniques are used to solves the problem of ACK, TWO ACK & Watchdog scheme. On acknowledged packets the techniques depend on the attacker prevent by Digital Signature from attacking packets. ACK, S-ACK, MRA & Digital Signature are the parts which namely consist by EAACK. A novel intrusion detection system called as EAACK protocol that is uniquely designed for MANETs .

Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balkrishnan, in this paper, the author has explains that it is work for TWO-ACK on routing protocols such as Dynamic Source Routing (DSR). The advantage of the two-acknowledgement scheme described has the flexibility to control the network overhead and check the performance declination caused by such misbehaving nodes in MANETs also explains a technique, term TWO-Acknowledgement to distinguish and reduce the effort of such routing misbehaviour. The TWO-Acknowledgement technique is situated on a simple TWO-Acknowledgement packet, which is sent back to the receiver of the next hop link, having the comparison with other approaches set to the problem, such as the overhear technique, the TWO-Acknowledgement scheme reduces the problems including uncertain collision, receiver collision and limited transmission power. The TWO-Acknowledgement scheme can be used as to routing the protocol such as Dynamic Source Routing (DSR) in MANETs. Ali Dorri , Seyed Reza Kamel ,Esmail kheyrkhah in this paper progresses of wireless technology and increasing popularity of wireless devices, made wireless networks . Mobile Ad Hoc Network (MANET) is an infrastructure seperate network with wireless mobile nodes. MANET is a kind of Ad Hoc networks with special characteristics like open network boundary, dynamic topology, distributed network, fast and headlong implementation and hop-by-hop communion. These characteristics of MANET made it famous, especially in military

and disaster management applications. Due to special features, wide-spread of MANET faced lots of threats. Peer to peer applications [1], integration with internet [2], security [3], maintaining network topology [4] and energy [5, 6] are some of the most important challenges in MANET. We presented an test and exchange in MANET [7]. In MANET all nodes are free to join and leave the network, also called open network boundary. All neutral nodes between a source and destination take part in routing, also called hop-byhop communications. As communication media is wireless, each node will receive packets in its wireless range, either it has been packets destination or not. Due to these inclination, each
node can easily gain access to other nodes packets or inject gulit packets to the network. Therefore, securing MANET against malicious misbehaviours and nodes, became one of the most important challenge in MANET [8]. The aim of this paper is to provide a brief delibration and search on MANET security. Based on MANET accept three important security parameters for MANET. In addition, two different MANET security are discussed in details. Furthermore, we presented an test and consideration in security attacks and bock approaches. Moreover, the most effective block approaches for MANET and their limitations are introduced. Three combinational challenges with security are presented in presents our analyses and classifications on security of MANET and presents some research interest in security. They introduces open research issues and directions of researches in MANET security. Finally concludes the paper and introduces best ways to secure MANET and presents some future works.

KhaldounAl Agha, Marc-Henry Bertin, Tuan Dang,Alexandre Guitton in this paper WIRELESS communication represents a major industrial stake in the coming years. It offers large regulatiion and helps industry save operating costs as well as upgrade operational efficiency. In the recent years, WiFi and Bluetooth technologies have known terrible development and have enter small office and home office as well as large trade office. These are wide-public wireless technologies may find their limited rule in industrial installations because of harsh environments, electromagnetic congurity and interference point of departure, safety and information technology (IT) security constraints, and battery autonomy. Few issues have been addressed by addenda to existing standards.

II .BACK GROUND

IDS in MANETs

Intrusion Detection system in MANETs are established in each and every node. Following are the basic intrusion detection systems, which are available, are

1. Watch dog scheme

2. TWO ACK Scheme

3. Adaptive Acknowledgement Scheme

1.1 Watch dog

This scheme is designed to improve the throughput of network with the presence of malicious nodes. The watchdog scheme has two parts-watchdog and pathrater. Watchdog serves as IDS for MANETs and is responsible for detecting malicious nodes by listening to its hop transmission. The watchdog fails to detect attacking nodes with the presence of the following: 1) ambiguous collisions 2)receiver collisions 3)limited transmission power 4)False misbehaviour Report 5)collisions 6)partial dropping.

2) TWO ACK:

TWOACK is neither an enhancement nor a watchdog scheme. Aim to resolve the receiver collisions and limited transmission power problems .TWO ACK scheme aims at detecting misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

3) AACK:

Adaptive acknowledgement is the combination of TWOACK and ACK. Source sends packet to every node till it reaches the destination. Once reached, receiver sends an ACK in the reverse order. If ACK is not received within predefined interval, it switches to TWOACK scheme. The major drawbacks are that it suffers from 1) False misbehaviour report 2) Forged acknowledgment packets.

IV. PROBLEM DEFINITION

Our proposed approach EAACK is designed to tackle of six weakness of watchdog scheme, namely, receiver collisions, limited transmission power, false
Misbehav iour report,

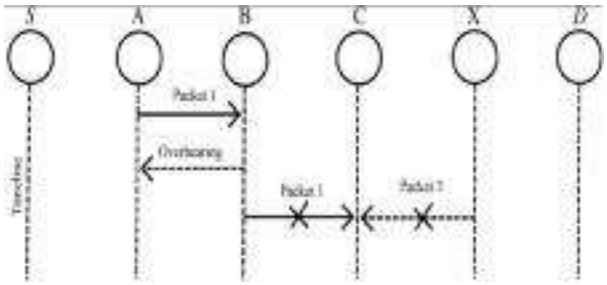
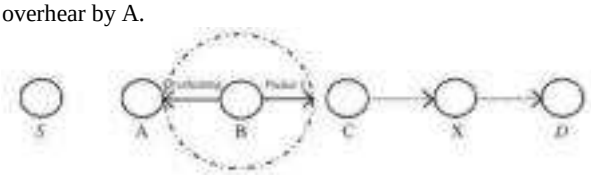


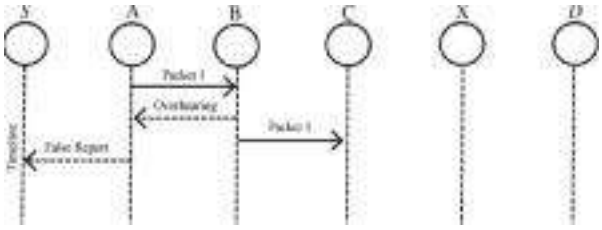
Fig. 3.1. Receiver Collisions occurs at receiver C because both nodes B and X are trying to send packets at same time. In above figure: S=Source, D=Destination and A, B, C…X=Nodes which shown the example of receiver collision in which after Node A packet 1 sends to the Node B, it tries to spy if Node B forwarded this packet to Node C, for the moment Node X is forwarding packet 2 to Node C. In such case, Node A spy that Node B has successfully delivered packet 1 to Node C but unable to detect that node C did not accept the packet due to a collision between packet 1 and packet 2 at Node C.

Fig. 3 2. Limited transmission power problem too weak to receive packet 1, which point to Node C from Node B but it, can be overhear by A.



Above figure shown the example of limited power transmission in order to preserve its self battery resources, node B intentionally check its transmission power so that it is strong suitable to be overhead by node A but not strong suitable to be received by node C.

Fig.3.3 False Misbehaviour Report at Node A send back a misbehaviour report even through Node B forwarded the packet to Node C.



Above figure shown the example of false misbehaviour, still node A successfully overhead that node B forwarded packet to node C, node A still reported node B as misbehaving.

V. METHODOLOGY

EAACK is based on both RSA and Rijndael algorithm .The three important parts of the EAACK scheme are ACK, S-ACK, MRA, Digital signature. EAACK is an acknowledgement based IDS.

1) Creating network formation
2) Key generation
3) (ACK) Acknowledgement implementation
4) (S-ACK) Secure-ACK implementation
5) (MRA)Misbehaviour Report Authentication

5.1 CREATING NETWORK FORMATION

In our simulations, the network area is 1200m*300m with 60 nodes initially and uniformly distributed .The channel capacity is 2mpbs.The Transmission range is 150m.A total UDP based CBR sessions are used to generate the network traffic. For each session, the data packet are generated with the size of 512 bytes in the rate of 16kpbs.The source – destination pairs are chose randomly from all nodes.

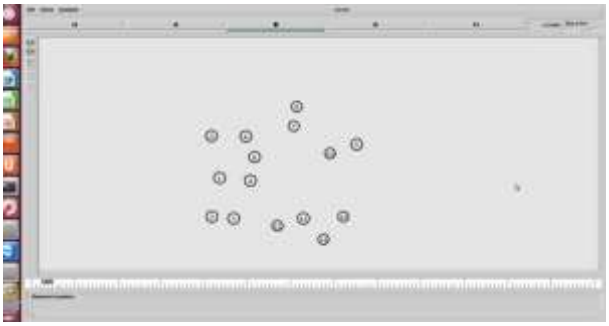


Fig 5. 1. Network formation.

5.2 KEY GENERATION

Each network assigned from key to send data securely over the network .The key consists of two types that are Encryption key and session key.

SESSION KEY:

A session key is an encryption and decryption key is randomly generated to ensure the security of a communication session between user session key sometimes called as symmetric key, because same key are used to both encryption and decryption

E.g.) Alice would like to establish a secure communication with bob. Alice send some message from bob at the time she cannot provide the key in plain text, otherwise some ones are hack the message and send the bob. How to avoid the hackers?

Solution:

Alice generate the session key then Alice encrypt the message by using Rijndael algorithm the session key are used to send secure from original message to bob. The key are able to securely get the symmetric key.

ENCRYPTION KEY:

Encryption key is the most effective way to achieve data security. In Encryption key are used from in Rijndael algorithm.

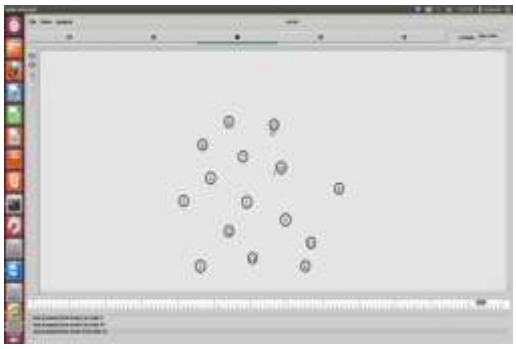


Fig 5.2.Key generation

5.3 ACK IMPLEMENTATION:

ACK is an end to end acknowledgement. It is the primary approach in EAACK, for increasing network overhead in times where there is no misbehaviour in network. In ACK node, node S first sends the ACK packet to the destination node D. Then the node S sends the packet to destination D and successfully receives the ACK packet. Otherwise node S will switch to S-ACK data packet to detect the misbehaving nodes in the route.

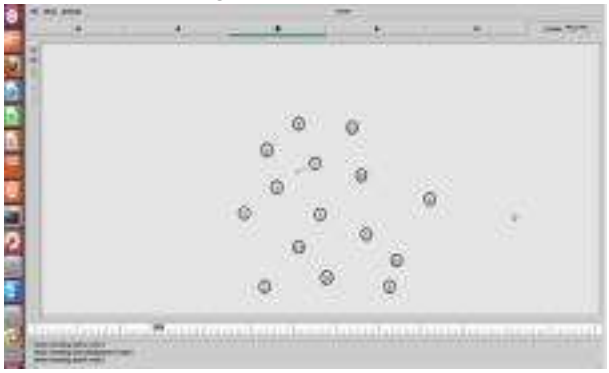


Fig 5.3. Acknowledgement Implementation

5.4 S-ACK IMPLEMENTATION:

S-ACK scheme is an improved version of TWO ACK scheme. The S-ACK is intended to detect misbehaving node in the presence of collision and limited transmission power.

In S-ACK three nodes are work in one group to find out misbehaviour node in the network its better version of two ack scheme. The nodes are required to send an S-ACK node to the firstnode.

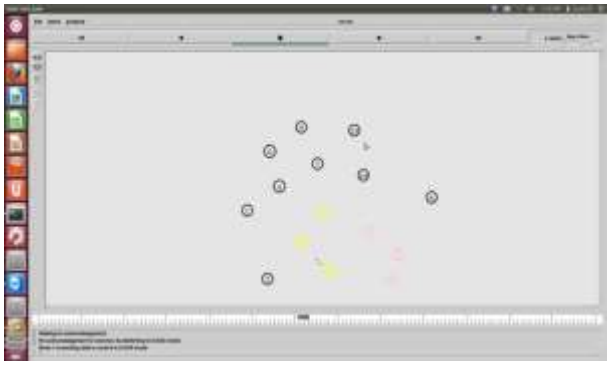


Fig 5.4. Secure Acknowledgement Implementation

5.5 MISBEHAVIOUR REPORT AUTHENTICATION:

In MRA scheme is to validate where the destination node is receive the reported packet through different route. The MRA scheme rectify the weakness of watchdog when its fail to detect misbehaving nodes with presence of false misbehaviour report. The false misbehaviour report can be reproduce the malicious attackers to falsely report innocent nodes as malicious. This attack can be entire the network when the attackers break down the sufficient nodes cause the network division.

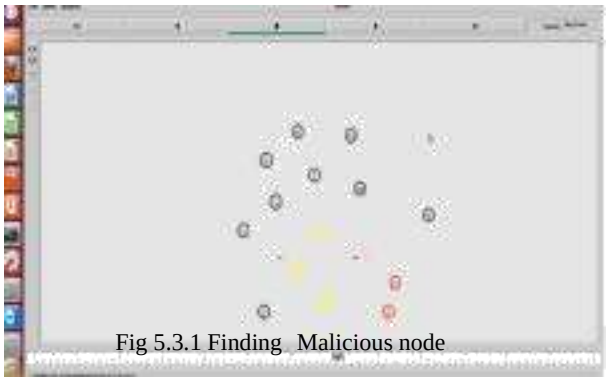


Fig 5.3.1 Finding Malicious node

5.6 DIGITAL SIGNATURE:.

Digitally sign packets are used by the Digital Signature both at the sender and the receiver side for avoiding the forging of packets. For implementing digital signature the required resources need to be integrated and both the algorithms RSA and Rijndael algorithm are used.

VI. PROPOSED SYSTEM

In this paper, we can propose session key Cryptography Technique that helps to reduce the network overhead. The count of acknowledged packet increases when the number of malicious node in network increases due to this reason, network overhead increases. Therefore, to reduce the network overhead we can use session key Cryptography Technique.

System Architecture

The Proposed system uses the technique of RSA and AES (Data Encryption Standard) due to which session key Cryptography scheme provides three cryptography primitives called as Integrity, Confidentiality and Authentication. A key exchange mechanism eliminating the requirement of pre-distributed key, which examine the possibilities of adopting. For providing security encryption mechanism and RSA key exchange mechanism is to be considered. To perform encryption and decryption technique each node must have approach to other nodes neighbourhood key. At origin, neighbourhood key is encrypted with the public key of the receiver and transmitted to the terminal node. At terminal neighbourhood key is decrypted with the node's own private key. The message specific key is having the advantage of making it to improve the security of the message being forwarded in the wireless ad hoc network. .

RIJNDAEL ALGORITHM

1. Rijndael algorithm: It is symmetric secure cipher cryptography. It is High performance and security.

2. RSA: It is public key cryptography can be used for encryption. The key management is an essential feature in RSA algorithm.

A.ENCRYPTION PROCESS:

Step1: An Rijndael algorithm key 'k' of 128-bit, 192, bit is chosen.

Step2: Encrypt message (M) using AES algorithm above selected key K.

eM =Rijndael algorithm-encryption (M)

Step 3: Rijndael algorithm key K is encrypted by making use of RSA algorithm

Ek =RSA-encryption (k)

Step 4: The encrypted message (em), Digital signature (DS), and Rijndael encrypted key (ek) is transmitted to user network.

In these algorithms are used for private key symmetric block cipher .It used in 128-bit data and its stronger and faster than triple DES.

SCHEME DESCRIPTION

The Rijndael algorithm has reach to providing security. Hybrid combination of RSA and Rijndael alg to achieves greater competency by combining two cryptosystem.

HYBRID ENCRYPTION SYSTEM

Hybrid encryption is the combination of Rijndael algorithm and RSA. Rijndael is very popular symmetric encryption algorithm which involves key size and block size. It perform the round transformation is performs sub bytes, shift rows, add around key. Using the RSA scheme the private key of Rijndael is encrypted which generate a key cipher text.

HYBRID DECRYPTION SYTEM

When the receiver receives the cipher text, the receiver use private key of Rijndael decryption module to decrypt the key cipher and then uses the decrypted key recovering the data cipher and digital signature

VII. PERFORMANCE EVALUATION:

7.1 Simulation Configuration:

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with ubuntu. The system running with 3-GBRAM. In order to better compare our simulation. In NS2.34, the default configuration specifies 50 nodes in a flat space with size of 670×670m.The language we are using are TCL and AWK script. User Datagram Protocol traffic with constant bit rate is implemented with a packet size of 521B.

In order to measure and compare the performance of our propone scheme, we adopt the following performance metrics:

7.1.1. Packet delivery ratio:

It is defined by the ratio of number of the packets received by the destination node to the number of the packets sent by the source node.

Fig 7.1.1 Packet Delivery Ratio Graph

7.1.2 AVERAGE END TO END DELAY

The average end to end delay for all well received packets at destination is calculated sending time of the packet from the received time at the final destination.

Fig 7.1.2. Average End to End Delay Graph

7.1.3. CONTROL OVERHEAD:

Routing over head refers to the ratio of routing related transmission.

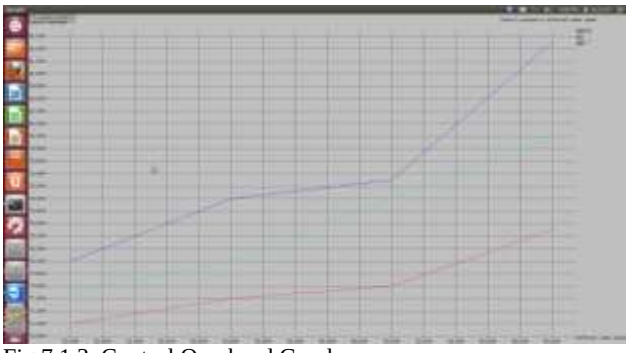


Fig 7.1.3 .Control Overhead Graph

7.1.4 KEY GENERATION SPEED

Key generation is almost as fast as signing. There is a slight penalty for key generation to obtain a secure random number.

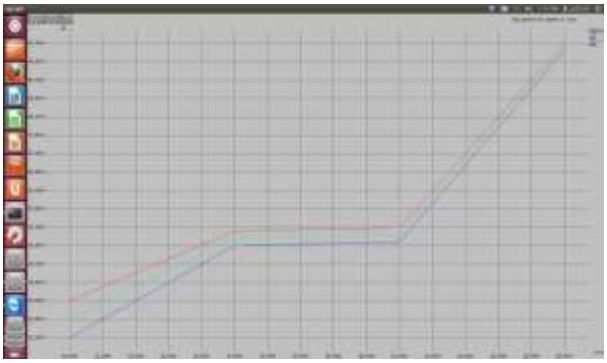


Fig 7.1.4 Key generation speed

VIII .CONCLUSION:

In these paper we have purpose the terminologies in security of MANET using EAACK.EAACK method are concentrating only detection of malicious nodes .we use session key cryptography used in encryption to strengthen the security of nodes. Detection of malicious node can be done by EAACK using Rijndael algorithm and RSA algorithm. To improve the PDR and security.

REFERENCE:

[1]] E.M.Shakshuki, N Kang, and T.R.Sheltanmi,"EAACK-A Secure Intrusion Detection System for MANETs", IEEE Trans. Induct. Elect vol .60, no.3, March 2013.

[2] Ali Dorri , Seyed Reza Kamel ,Esmail kheyrkhah"security challenges in mobile adhoc"2014.

[3] B.Reddy Sumanth, Dr E.Madhusudhana Reddy" Management secure ids for manet" Engineering and Scientific International Journal (ESIJ) ISSN Volume 1, Issue 1, October - December 2014.

[4] Muthu Kumara Raja, Bala Sujitha.T.V," Intrusion Detection System in Web Services", Volume 2 Issue 2, February 2013.

[5] R.Akbani, T.Korkmaz, and G.V.S.Raju,"MobileAdhoc Network Security" IEEE Transaction, vol .no. 127 Network: 2012.

[6] N.Kang, E.Shakshuki, and T.Sheltami,"Detecting Forged acknowledgements in MANETs" in Proc.IEEE 25th Int.Conf. AINA, March 2011.

[7] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micro power generator," IEEE Trans. Ind. Electron., vol. 57,no. 3, pp. 840–849, Mar. 2010.

[8] V.C.Gungor and G.P Hancker," Industrial wireless sensor networks challenges, design principles, and technical appproach,"IEEE Transaction, vol .no.56 Oct 2009.

[9] T.Anantvalee and J.Wu,"A Survey on Intrusion Detection in Mobile Adhoc Networks, "in Wireless/Mobile Security.springer-2008.

[10].K. AlAgha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

Author Profile

Dr.K.Ramasamy received the Ph.d in communication Engineering from Multimedia University, He received M.E degree in Applied Electronics from the PSG Engineering College and Technology, He received B.E degree in Electronics and Communication Engineering in Mepco schlenk Engineering college . He has over 28.5 years experience as faculty in various reputed colleges . Area of Interest Manet and Wireless Sensor Network,Digital Image Processing.

G.Siva Kumar received the M.E degree in communication and Engineering from the National Engineering College, He received B.E degree in Electronics and Communication Engineering in RVS Engineering college and Technology. Area of Interest Manet and Wireless Sensor Network,Digital Image Processing.

C. Muthupriya doing M.E degree in communication and Networking from P.S.R.Rengasamycollegeof Engineering for Women(2017).Received B.E degree in Electronics communnication and Engineering from P.S.R.Rengasamy College of Engineering for Women(2015).Area of Interest WSN and Mobile Adhoc Network