NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 2, ISSUE 3 MARCH2015

# IEAACK-Secure Detection System For Packet-Dropping Attack In Manets

Ms. Preeti Sharanvijay. Chikkshetty
Department of Computer Science and Engg, N.B.N. Sinhgad College of Engg.
Solapur University, Solapur, India

Prof. Abhijit. V. Mophare,
Asst. Prof. in CSE Dept., N.B.N. Sinhgad College of Engg.
Solapur University, Solapur, India

Prof. Amarnath Shivanand Chadchankar
Asst. Prof. in CSE Dept., BMIT, Solapur University, Solapur, India

## Abstract

MANET is a collection of wireless independent nodes along with transmitter and receiver that communicate with each other via bidirectional link. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. But due to the changing topology and open access MANET become vulnerable to problems (such as receiver collision, limited transmission power, false misbehaviour report , packet dropping) To solve this problem we use three approaches of Intrusion Detection System (IDS) such as Watchdog, TWOACK, and AACK. We have proposed a new protocol design for MANET that is IDS based EAACK which consist of ACK, S-ACK and MRA for solving all the problems of Watchdog approach in IDS of MANET.

## Introduction

Over the past decade, there has been a growing interest in wireless networks, as the cost of mobile devices such as PDAs, laptops, cellular phones, etc have reduced drastically. The latest trend in wireless networks is towards pervasive and ubiquitous computing - catering to both nomadic and fixed users, anytime and anywhere. Several standards for wireless networks have emerged in order to address the needs of both industrial and individual users. One of the most prevalent forms of wireless networks in use today is the Wireless Local Area Network (WLAN). In such a network, a set of mobile nodes are connected to a fixed wired backbone. WLANs have a short range and are usually deployed in places such universities, companies, cafeterias, etc. There is still a need for communication in several scenarios of deployment where it is not feasible to deploy fixed wireless access points due to physical constraints of the medium. For example, consider communication amongst soldiers in a battlefield, involving troops spread out over a large area. In this case, it is not only feasible to deploy a fixed wireless access point, but also risky since an enemy attack would bring down the whole network. This problem has led to a growing interest among the research community in mobile ad hoc networks, wireless networks comprised of mobile computing devices communicating without any fixed infrastructure.

By definition, Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multi-hop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

## LITERATURE REVIEW

Elhladi M. Shakshuki, Nan Kang and Tarek R. Sheltami[1],The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbours to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery.

G. Jayakumar and G Gopinathmk[2] Mobile ad hoc networks(MANET) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self organize into arbitrary and temporary adhoc network topologies, allowing people and devices to seamlessly internet work in areas with no preexisting communication infrastructure e.g., disaster recovery environments. Tactical networks have been the only communication networking application that followed the ad-hoc paradigm. Recently the introduction of new technologies such as Bluetooth, IEEE 802.11 and hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent revolutions have been generating a renewed and growing interest in the research and development of MANET.

R. Rivest, A. Shamir, and L. Adleman[4],An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret prime numbers p and q. Decryption is similar; only a different, secret, power d is used, where e _ d _ 1 (mod (p - 1) _ (q - 1)). The security of the system rests in part on the difficulty of factoring the published divisor, n.

## Problem Definition And Scope

### Problem Statement:

***A)Watchdog:*** proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviours in the network. Watchdog detects malicious misbehaviours by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links.

***B.TWOACK:*** The main purpose of TWOACK is to solve the weakness of Watchdog such as receiver collision and limited transmission power also TWOACK can detects misbehaving links by acknowledging every data packets transmitted over each three consecutive nodes along the packet the from the source to destination [8].Upon retrieval of a packet, each node along the route is required to send back an acknowledgement packet to the node that is two hops away from it down the route. TWOACK work on routing protocols such as Dynamic Source Routing (DSR)[5].

***C. AACK:*** Adaptive ACKnowledgement (AACK) new scheme proposed by Sheltami *et al.* [6] based on TWOACK. AACK is a network layer based scheme which can be considered as a combination TWOACK (identical to TWOACK) and end to end acknowledgement scheme. As compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or surpassing the same network throughput [9].

## System Description:

EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK. According to the Internet draft of DSR [11], there is 6 b reserved in the DSR header. In EAACK, we use 2 b of the 6 b to flag different types of packets.

***A. ACK:*** ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network Misbehavior is detected. In ACK mode, node S first sends out an ACK data packet $Pad1$ to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives $Pad1$, node D is required to send back an ACK acknowledgment packet $Pak1$ along the same route but in a reverse order. Within a predefined time period, if node S receives $Pak1$, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

***B. S-ACK:*** The S-ACK scheme is an improved version of the TWOACK scheme proposed. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. In S-ACK mode, the three consecutive nodes (i.e., F1, F2, and F3) work in a group to detect misbehaving nodes in the network. Node F1 first sends out S-ACK data packet *Psad*1 to node F2. Then, node F2 forwards this packet to node F3. When node F3 receives *Psad*1, as it is the third node in this three-node group, node F3 is required to send back an S-ACK acknowledgment packet *Psak*1 to node F2. Node F2 forwards *Psak*1 back to node F1. If node F1 does not receive this acknowledgment packet within a predefined time period, both nodes F2 and F3 are reported as malicious. Moreover, a misbehaviour report will be generated by node F1 and sent to the source node S.

***C. MRA:*** The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehaviour report. The false misbehaviour report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be lethal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a DSR routing request to find another route. Due to the nature of MANETs,

***D. Digital Signature:*** As discussed before, EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviour in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA [33] and RSA [23] digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

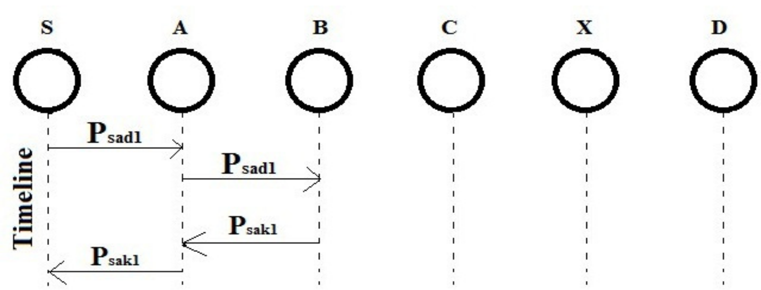


**Fig.1 ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet.**

**Proposed Work:**

Proposed System:

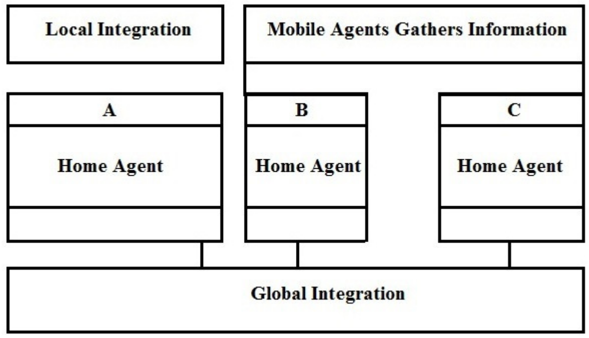


**Fig.2: Proposed System Architecture**

**Current node:** If an attacker sends any packet to gather information through this system, Home agent calls the classifier construction to find out the attacks. If an attack has been occurred, it will filter the respective system from the global networks.

**Home agent***:* It is present in every system and it collects information about its system from application layer to network layer.

**Neighbouring node*:*** In this any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message it send mobile agent to the neighbouring node.

**Data collection*:*** This module is used for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario and attack data is collected during the attack scenario.

**Data process*:*** Data pre-processing is a technique to process the information with the test train data. The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. In the entire layer anomaly detection system, the above mentioned preprocessing technique is used.

**Local integration*:*** This module concentrate on self system and it find out the local anomaly attacks. Every system under that wireless network follows the same methodology to provide a secure global network.

**Global integration:** Global integration module is used to find the intrusion result for entire network. The aim of this module is to consider the neighbour node(s) result for taking decision towards response module.

**DSA Algorithm**: In EAACK, Digital Signature is used to prevent the attackers from acknowledgment packets. All the parts of EAACK scheme (ACK, S-ACK, MRA) are acknowledgement based detection schemes. They all are relay on the ACK packets to detect malicious node in MANET network. Thus it is extremely vital to ensure that all acknowledgement packets in EAACK are authentic and contaminated. In another way, if the attackers are insolent enough to forge acknowledge packet all the three schemes will be vulnerable. To overcome this problem, we use Digital Signature Algorithm (DSA) [7] in IDS. To ensure the integrity of IDS, EAACK requires to all the ACK packets to be digitally signed before they are send out and verified when they are accepted by the receiver.

**Step 1:** A fixed length message is digested by using hash function H for every message m, mathematically this can described as: H (m) =d

**Step 2:** The sender Alice needs to apply its own private key $P_{r\text{-}Alice}$ on the message digest d and produces result signature $Sig_{Alice}$, which is attached to message m and Alice's private key.

$$S_{Pr\text{-}Alice\ (d)} = Sig_{Alice}$$

The sender Alice is obliged to always keep her private key $P_{r\text{-}Alice}$ as a secret without concealed to anyone else. Otherwise, if the attacker Eve gets this secret private key, she can intercept the message and easily forge malicious messages with Alice's signature and send them to Bob. As these malicious message signed by Alice, Bob sees them as legit and authentic messages from Alice. Thus, Eve can attacks on the entire network and generate malicious attacks to Bob.

**Step 3***:* Alice can send message m along with the signature $Sig_{Alice}$ to Bob via an unsecured channel. Bob then decrypts the received message m' against the pre agreed hash function H to get the message digest d'. This process can be generalized as,H (m') =d'

**Step 4:** Bob can verify the signature by applying Alice's public key $P_{k\text{-}Alice}$ on $Sig_{Alice}$ ,by using $S_{Pr\text{-}Alice}$ ($Sig$Alice) = d

**Step 5***:* If d == d' then it is original message m' transmitted through an unsecured channel is indeed sent from Alice and the message it itself is intact.

## Result

1) **Simulation Results**—Scenario 1: In scenario 1, malicious nodes drop all the packets that pass through it. Fig.3 shows the simulation results that are based on PDR. In Fig. 3, we observe that all acknowledgment-based IDSs perform better than the Watchdog scheme. Our proposed scheme EAACK surpassed Watchdog's performance by 21% when there are 20% of malicious nodes in the network. From the results, we conclude that acknowledgment-based schemes, including TWOACK, AACK, and EAACK, are able to detect misbehaviours with the presence of receiver collision and limited transmission power. However, when the number of malicious nodes reaches 40%, our proposed scheme EAACK's performance is lower than those of TWOACK and AACK. We generalize it as a result of the introduction of MRA scheme, when it takes too long to receive an MRA acknowledgment from the destination node that the waiting time exceeds the predefined threshold. The simulation results of RO in scenario 1 are shown in Fig. 4. We observe that DSR and Watchdog scheme achieve the best performance, as they do not require acknowledgment scheme to detect misbehaviors. For the rest of the IDSs, AACK has the lowest overhead. This is largely due to its hybrid architecture, which significantly reduces network overhead. Although EAACK requires digital signature at all acknowledgment process, it still manages to maintain lower network overhead in most cases. We conclude that this happens as a result of the introduction of our hybrid scheme.
2)

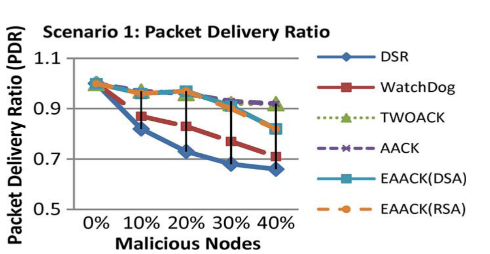


**Fig. 3. Simulation results for scenario 1—PDR**.

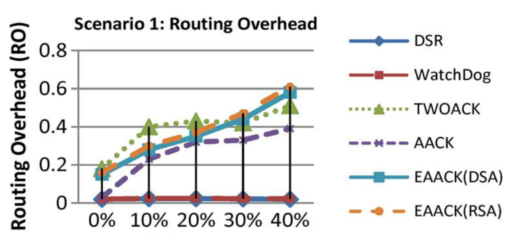


**Fig. 4. Simulation results for scenario 1—RO.**

**2) Simulation Results**—Scenario 2: In the second scenario, we set all malicious nodes to send out false misbehavior report to the source node whenever it is possible. This scenario setting is designed to test the IDS's performance under the false misbehavior report. Fig. 5 shows the achieved simulation results based on PDR. When malicious nodes are 10%, EAACK performs 2% better than AACK and TWOACK. When the malicious nodes are at 20% and 30%, EAACK outperforms all the other schemes and maintains the PDR to over 90%. We believe that the introduction of MRA scheme mainly contributes to this performance. EAACK is the only scheme that is capable of detecting false misbehavior report. In terms of RO, owing to the hybrid scheme, EAACK maintains a lower network overhead compared to TWOACK in most cases, as shown in Fig. 6. However, RO rises rapidly with the increase of malicious nodes. It is due to the fact that more malicious nodes require a lot more acknowledgment packets and digital signatures.

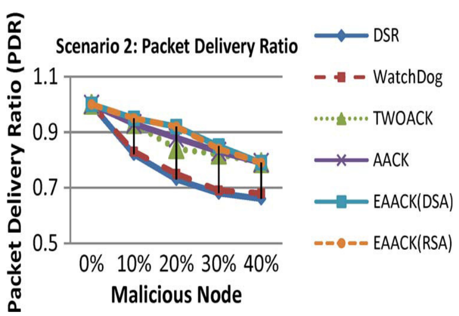


**Fig. 5. Simulation results for scenario 2—PDR.**

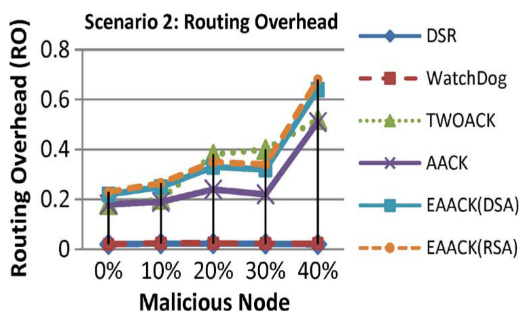


**Fig. 6. Simulation results for scenario 2—RO.**

**3) Simulation Results**—Scenario 3: In scenario 3, we provide the malicious nodes the ability to forge acknowledgment packets. This way, malicious nodes simply drop all the packets that they receive and send back forged positive acknowledgment packets to its previous node whenever necessary. This is a common method for attackers to degrade network performance while still maintaining its reputation. The PDR performance comparison in scenario 3 is shown in Fig. 7. We can observe that our proposed scheme EAACK outperforms TWOACK and AACK in all test scenarios. We believe that this is because EAACK is the only scheme which is capable of detecting forged acknowledgment packets. Fig. 8 shows the achieved RO performance results for each IDS in scenario 3. Regardless of different digital signature schemes adopted in EAACK, it produces more network overhead than AACK and TWOACK when malicious nodes are more than 10%. We conclude that the reason is that digital signature scheme brings in more overhead than the other two schemes.

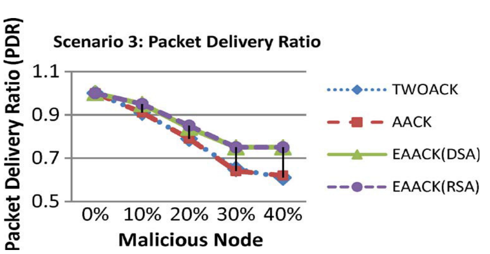


**Fig. 7. Simulation results for scenario 3—PDR.**

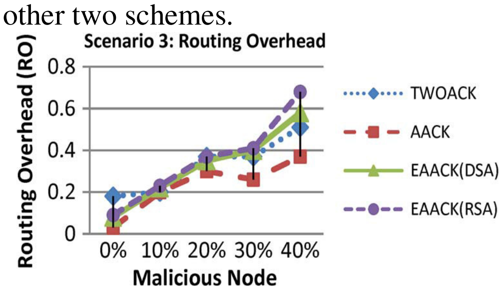


**Fig. 8. Simulation results for scenario 3—RO.**

## CONCLUSION

In this paper we have studied various IDS's in MANET, with their merits and demerits. Our proposed IDS IEAACK scheme removes the weakness of watchdog approach (such as receiver collision, limited transmission power etc) and provides a secure end to end acknowledgement for all the nodes. Also we studied the digital signature algorithm is used to provide authentication of data and validating the sender. In the future, we plan to follow hybrid cryptography techniques to reduce the network overhead caused by digital signature.

## References

[1] Elhladi M. Shakshuki, Nan Kang and Tarek R. Sheltami," EAACK—A Secure Intrusion-Detection System for MANETs", *in IEEE Transactions ON Industerial Electronics*, vol. 60, NO. 3, MARCH 2013.

[2] G. Jayakumar and G Gopinath,"Ad hoc mobile wireless networks routing protocol-A review*", J Comput, Sci*., vol. 3, no.8, pp.574-582,2007.

[3] N. Nasser and Y. Chen," Enhanced *intrusion detection systems for discovering malicious nodes in mobile ad hoc network",* in *Proc. IEEE Int.Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[4] R. Rivest, A. Shamir, and L. Adleman,"A Method for Obtaining Digital Signatures and Public-key Cryptosystems. In the Communications of ACM" , vol .20,pp 120-126,1978.

[5] D. Johnson and D. Maltz," Dynamic Source Routing in *ad hoc* wireless networks", in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch.5, pp. 153-181.

[6] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis."Secure Routing and Intrusion Detection in Ad hoc Networks", *In the Proceedings of 3rd International Conference on Pervasive Computing and Communications, pp. 191-199, 2005.*

[7] N. Kang, E. Shakshuki , and T. Sheltami ," Detecting misbehaving nodes in MANETs", in *Proc. 12th Int. Conf. ii WAS*, Paris, France, Nov. 8-10,2010, pp. 216-222.

[8] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs", *IEEE Trans. Mobile Compu.,vol. 6, no.5, pp. 536-550,May 2007.*

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud ," Video transmission enhancement in presence of misbehaving nodes in MANETs" *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] A. Singh, M. Maheshwari, and N. Kumar, "Security and trust management in MANET ", in *Communications in Computer and Information Science*, vol. 147. New York: Springer-Verlag, 2011, pt. 3, pp. 384-387.

[11] B. Sun "Intrusion detection in mobile ad hoc networks", Texas A&M Univ., College Station, TX, 2004.

[12] Prof. Anushka K. Rajyalakshmi G. V., "Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System", *International Jouranal of Engineering Research in Management & Technology(IJERMT)*, India, ISSN: 2278-9359,vol.2, issue 7.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in *Proc. 6th Annu. Int. Conf. Mobile Comput. Net.* , Boston, MA, 2000, pp. 255–265.

[14] R.H. Akbani, S. Patel , D.C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey", *The proceedings of the Second International Meeting of Advanced Computing &Communication Technologies(*ACCT)*,* pp. 535-541, Rohtak, Haryana, India. 2012. – here1.

[15] Akshatha Y, Dr. Rashmi M. Jogdand, "A Study on Enhanced Adaptive Acknowledge (EAACK) Scheme – A Secure Intrusion Detection System in Wireless MANETs", *International Journal of Latest Trend in Engineering and Technology (IJLTET)*, Special Issue- IDEAS-2013, ISSN: 2278-621X.