Improved Adaptive Acknowledgment-A Secured Intrusion Detection System for MANETs

Dr. L. M. Varalakshmi
Associate Professor
SMVEC
Puducherry-605 107
India

V. Aiswarya
Student
SMVEC
Puducherry-605 107
India

S. Dharani
Student
SMVEC
Puducherry-605 107
India

***Abstract*—The wireless network has been a global trend in the past few decades because of its mobility and scalability Among all the contemporary wireless networks, Mobile Ad hoc NETwork (MANET) is one of the most important and unique applications. As our contribution for EAACK, we propose methods to solve packet dropping problem in MANET. We know that, Mobile ad hoc network (MANET) is a self-organizing, self-configuring confederation of wireless systems. The dynamic topologies, mobile communications structure, decentralized control, and anonymity creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. In this paper, we propose a new routing mechanism to combat the four problems such as common selective packet dropping attack, receiver collision, limited transmission power and false misbehavior report. Simulation results show the effectiveness of our scheme compared with conventional scheme.**

***Keywords*—Mobile Ad hoc NETwork (MANET), Improved Adaptive ACKnowledgment (IAACK).**

I. INTRODUCTION

Due to its affordability, convenience of access and ease of movement, wireless technology is rapidly gaining in popularity. Rapid expanding range of capabilities and various uses of mobile computing devices have made mobile ad-hoc networks (MANETs) of great interest to both researchers and commercial developers. A mobile ad-hoc network (MANETs) is a collection of mobile devices falling within the transmission range of each other. It does not have a centralized controller or fixed infrastructure. It is said to be dynamic topology, as nodes are capable of moving actively.

Due to node mobility, the routing topology in MANET is different from traditional routing found on infrastructure network. It depends on many factors such as topology, selection of routers, initiation of request, and other characteristics that could efficiently find the path. Some well-known routing protocols include DSR and AODV. The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly. Most ad hoc network routing protocols becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available.

As a result, intrusion detection system (IDS) has gained its importance in MANET. An IDS is a device or software application that monitors network for malicious activities and produces reports to a management station. Proposed work focus on such misbehavior for its detection and isolation from network.

II. BACKGROUND

A. IDS in MANETs:

Ad hoc wireless networks are totally dependent on collective participation of all nodes in routing of information through the network. In this section, we mainly describe existing approaches, namely, Watchdog, TWOACK, Adaptive ACKnowledgment (AACK) and Enhanced Adaptive ACKnowledgment (EAACK).

1. Watchdog: The watchdog method is the basic IDS technique which detects the misbehaving nodes. It has two parts- watchdog and path rater. When a node forwards a packet, the watchdog set in the node ensures that the next node in the path also forwards the packet by listening to all nodes within transmission range promiscuously. If the next node does not forward the packet then it is reported as malicious. It maintains a failure counter, whenever malicious node is reported.

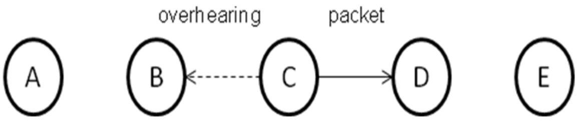

Fig.1.watchdog scheme

If it exceeds a predetermined threshold, the Path rater avoids the particular node for future data transmission.

The Watchdog Scheme fails to detect malicious misbehaviors with the presence of the following:

- Ambiguous collisions

- Receiver collisions
- Limited transmission power
- False misbehavior report
- Collusion
- Partial dropping

We discuss these weaknesses with further detail in Section III.

2) TWOACK: TWOACK scheme resolves the receiver collision and limited transmission problems faced by watchdog. Every three consecutive nodes work in a group to detect misbehaving nodes. When a first node forwards a packet, the nodes routing agent verifies that the packet is received successfully by the node that is two hops away on the source route. This is done through the use of a special type of acknowledgment packets, termed TWOACK packets. Then, the third node sends the TWOACK packet to the first node. If the sender/forwarder of a data packet does not receive a TWOACK packet, the next-hop's forwarding link is claimed to be misbehaving. Though it improves network throughput, the acknowledgment process required in every packet transmission process creates significant amount of unwanted network overhead.

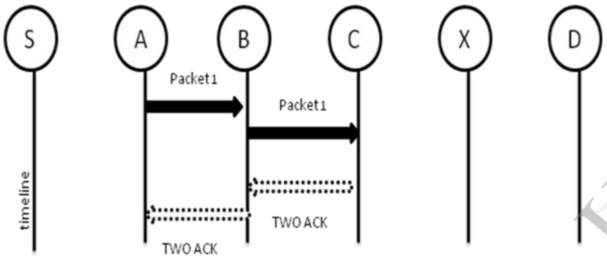

Fig.2. TWOACK scheme

3) AACK: Based on TWOACK, AACK (Adaptive acknowledgment) scheme is proposed. It is an acknowledgment-based network layer scheme which is a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduces network overhead which is caused by TWOACK scheme.

4) EAACK: EAACK consists of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA).

ACK implementation: ACK is basically an end – to – end acknowledgment scheme. That is, a source node sends a data packet to destination through the number of intermediate node. Then the destination node after receiving the data sends the acknowledgment packet in a reverse direction along the same route.

Secure Acknowledgment (S-ACK): It is similar to that of TWOACK scheme. In the S-ACK principle, every three consecutive nodes work in a group to detect misbehaving nodes. Its aim is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

Misbehavior Report Authentication (MRA): The MRA scheme is designed to resolve the false misbehavior report problem. Here, source node checks the alternate route to reach destination. Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation: To ensure that all acknowledgment packets in EAACK are authentic and to avoid the attackers to forge these acknowledgment packets, digital signature technique is used. RSA is an encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It involves three steps: key generation, encryption and decryption RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

III. PROBLEM DEFEINITION

Our proposed approach Improved Adaptive Acknowledgment is designed to tackle partial dropping and link breakage problem. In this section, we discuss these six weaknesses in detail.

A. False Misbehavior

Node A successfully forwards the packet to node B which successfully forwards the same packet to node C. But node A sends a misbehaving report that node B is misbehaving. This is called as false misbehavior report.

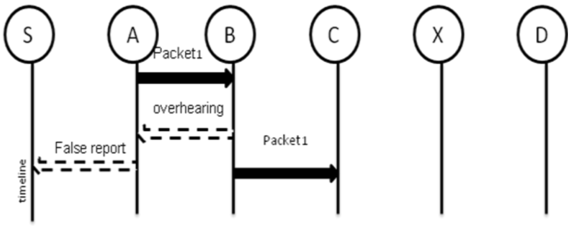

Fig 4: False misbehavior report

B. Limited power transmission:

The limited power transmission is due to malicious node which limits the power so that node A can overhear that packet has been received by node B but node B do not have enough power to transmit the packet to node C. This is mainly due to selfish nodes.

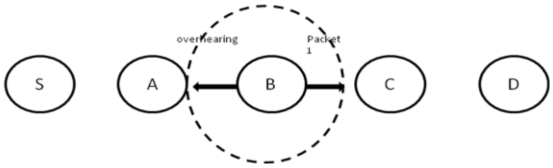

Fig 5: Limited power transmission

C. Partial dropping

While transmitting n number of packets, few packets are dropped silently. This is called partial dropping. This is very difficult to detect.

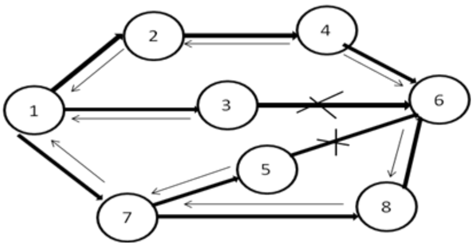

Fig 6: partial dropping

D. Collusion

Source *S* is sending packets via X and Y to destination D. S recognizes that X is forwarding all packets to Y. But Y drops all the packets which were not generated by malicious nodes, but received from a colluding malicious node. X is able to detect the misbehavior of Y. Since X1 and X2 collude, X1 silently accepts the misbehavior, which goes unnoticed for the benign nodes S and D. This is termed as collusion.

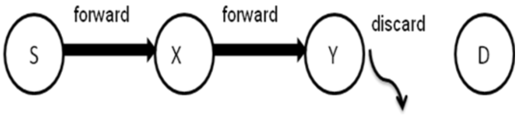

Fig 7: Collusion

D. Receiver collision

In the receiver collision problem, node A can only know whether B forwards the packet to C or not, but it cannot tell if C receives it. Due to the collision occurs at C between packet 1 and packet 2, the packet can get lost. This is termed as receiver collision.

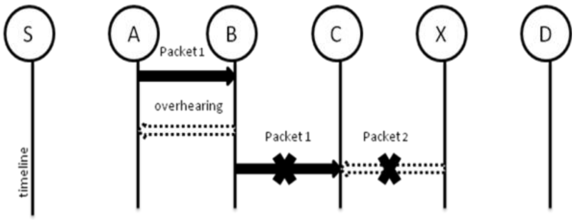

Fig 8: Receiver collision

IV. SCHEME DESCRIPTION

In our proposed scheme we have classified the Association among the nodes and their neighboring nodes in to three types as shown below. In an ad hoc network the Association between any source node and destination node will be determined as follows.

A. Trust Identification

In this module, we calculate the trust between the nodes. Where the nodes are classified as Unknown, and Known. Trust classification and calculation is made on demand based on the data transfer route request.

Desolate

- The source node have not sent/received any messages to/from destination node
- Trust levels between them are very low.
- Probability of malicious behavior is very high.
- Newly arrived nodes are grouped in to this category.

Distrusted

- Source node has sent/received some messages to/from destination node.
- Trust levels between them are neither low nor too high.
- Probability of malicious behavior is to be observed.

Trusted

- Source node has sent/received plenty of messages to/from destination node.
- Trust levels between them are very high.
- Probability of malicious behavior is very less.

B. Trust Aware Routing

Based on the results of the previous module, we propose a module called trust aware routing, where the problem of packet dropping is avoided by making the transmission in the trust aware routing nodes.

V. PERFORMANCE EVALUATION

In this section, we describe the simulation environment and methodology as well as comparing performances through simulation result comparison with EAACK and proposed Improved Adaptive Acknowledgment schemes.

A. Simulation Methodologies

To investigate the performance of our scheme under different types of attacks, we propose three scenario settings to simulate different types of misbehaviors or attacks.

Scenario 1: This scenario represents the simulation of packet dropping attack. In this the malicious nodes will simply drop all the packets that are received by those nodes. This scenario is simulated in order to test the IDS's of the weaknesses to watchdog namely receiver collision and limited power transmission.

Scenario 2: This scenario represents the design to test the performances against false misbehavior report. Here malicious nodes always drop the packets that are received and it sends back a false misbehavior report whenever possible.

Scenario 3: This scenario evaluates the IDSs' when the attackers are wise enough to forge acknowledgment packets and claiming positive result which is actually negative.

B. Simulation Configurations

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with Microsoft windows XP Professional**.** The system is running on a laptop with Intel(R) Core™ i5-2430M CPU and 2.40 GHz 2.38 GHz 512 MB of RAM. We adopted the default scenario settings in NS 2.28 The intention is to provide more general results and make it easier for us to compare the results. In NS 2.28, the default configuration specifies 100 nodes in a flat space. The maximum hops allowed in this configuration setting are six. The moving speed of mobile node is limited to 20 m/s and a pause time of 1000 s. the parameters are given in TABLE I as follows. User Datagram Protocol traffic with constant bit rate. For each scheme, we calculated the average performance.

TABLE I. PARAMETER

PARAMETERS	**RANGE / TYPE**
CHANNEL TYPE	WIRELESS
MAC LAYER TYPE	MAC 802_11
ANTENNA MODEL	OMNI ANTENNA
MAX PACKET IN IFQ	50
NO OF MOBILE NODES	100
ROUTING PROTOCOL	AODV
TIME OF SIMULATION END	50
X DIMENSION	1216
Y DIMENSION	743

In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics.

1) *Packet delivery ratio (PDR):* PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

$$PDR = \frac{\sum \text{Number of packets received}}{\sum \text{ Number of packets sends}} \qquad (1)$$

2) *Routing overhead (RO):* RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

$$ROH= \frac{\sum \text{Routing Transmissions}}{\sum \text{Routing transmissions} + \sum \text{Data Transmissions}} \qquad (2)$$

C. Performance Evaluation

1) Simulation Results—Scenario 1: In scenario 1, malicious nodes drop all the packets that pass through it. Fig. 9 shows the simulation results that are based on PDR.

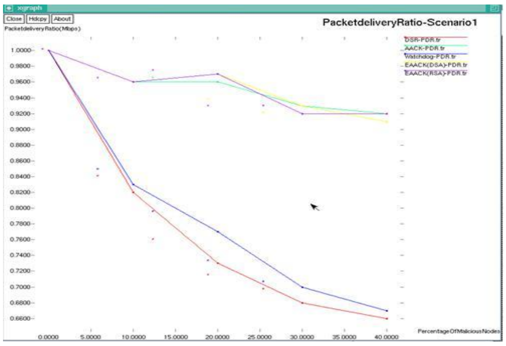

Fig 9: Simulation results for scenario 1—PDR.

The simulation results of RO in scenario 1 are shown in Fig. 10. We can say that DSR and Watchdog scheme achieve the best performance, since they do not require acknowledgment scheme to detect malicious misbehaviors.

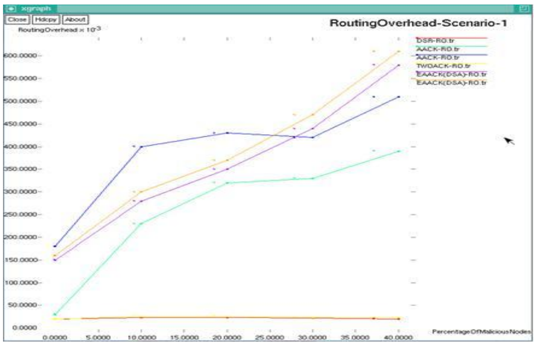

Fig.10. Simulation results for scenario 1—RO

2) Simulation Results—Scenario 2: The second scenario, we have set all the preset malicious nodes to send out false misbehavior report to the source node whenever it is possible. Fig. 11 shows the simulation results that are achieved based on PDR. Improved Adaptive Acknowledgment is capable of detecting false misbehavior report.

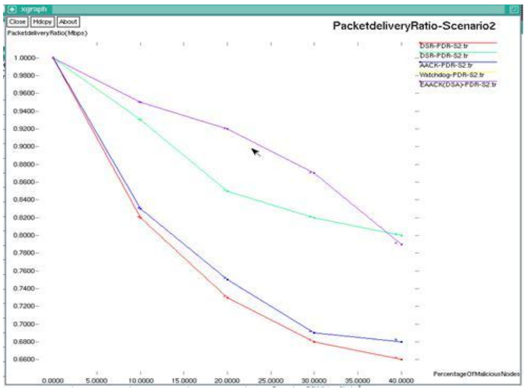

Fig 11: Simulation results for scenario 2—PDR

In terms of RO, owing to the hybrid scheme, it maintains a lower network overhead compared to TWOACK in most cases.

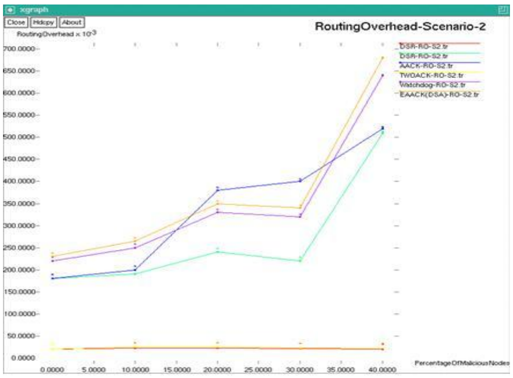

Fig.12. Simulation results for scenario 2—RO.

3) Simulation Results—Scenario 3: In scenario 3, we have provided the malicious nodes the competence to forge acknowledgment packets. By this way, malicious nodes will simply drop all the packets that are received and send back the forged positive acknowledgment packets to its previous node whenever necessary. The PDR performance comparison in scenario 3 is shown in Fig. 13

Fig. 14 shows the achieved RO performance results for each IDS's in scenario 3. We desist that the reason is that digital signature scheme brings in more overhead than the other two schemes.

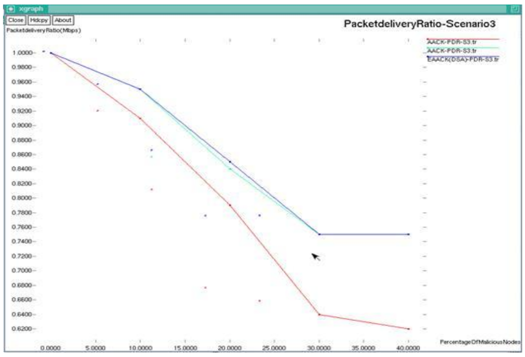

Fig 13: Simulation results for scenario 3—PDR.

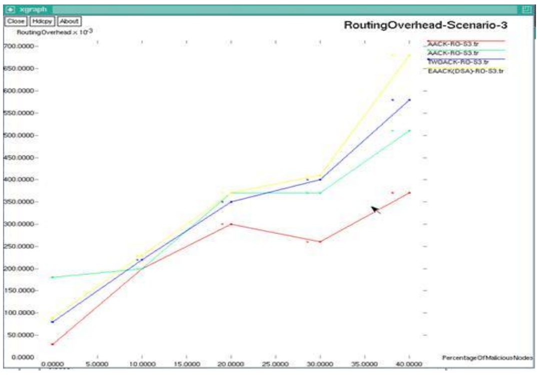

Fig.14. Simulation results for scenario 3—RO

VI. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. Misbehavior of nodes may cause severe damage, even fails whole of the network. In this paper, investigation is done on the misbehavior nodes and a new approach is proposed for detection of misbehaving node. Although it generates more ROs in some cases, it can vastly improve the networks PDR when the attackers are smart enough to forge acknowledgment packets. We implemented RSA scheme in our simulation to avoid forging. So the proposed approach is more advantageous than previous similar scheme.

ACKNOWLEDGMENT

We would like to take this opportunity to express our deepest gratitude to *Mr. P. RAJA, Head of the Department, Electronics and Communication Engineering*, for giving us suggestions then and there. He has always been a source of inspiration and encouragement towards the paper. We would like to take this opportunity to thank our respected *Director*, **Dr. V. S. K. VENKATACHALAPATHY** and our *Management*, for providing us with a good environment and facilities to complete this paper. Finally an honorable mention goes to our families and friends for their encouragements and supports on us in completing this paper.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs". *Ieee transactions on industrial electronics,* vol. 60, no. 3 march 2013.

[2] N. Bhalaji, Sinchan banerjee and A.Shanmugam,"A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks". *Journal of Computer Science 4 (7): 538-544, 2008, ISSN 1549-3636, © 2008 Science Publications.*

[3] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar." A Survey of Intrusion Detection Systems in Wireless Sensor Networks". *IEEE communications surveys & tutorials, accepted for publication.*

[4] Aishwarya Sagar Anand Ukey, Meenu Chawla, Maulana Azad "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET". *IJCSI International Journal of Computer Science Issues*, Vol. 7, Issue 4, No 1, July 2010.

[5] Vinay P.Virada, "Intrusion Detection System (IDS) for Secure MANETs: A Study". *International Journal of Computational Engineering Research* (ijceronline.com) Vol. 2 Issue. 6.

[6] Swapna Taksande, Prof. Rajani Bhoomarker, Prof. Sameena Jafar, "review paper on response based approaches for detection of misbehaving nodes in manets". Swapna Taksande *et al*, *International Journal of Computer Science and Mobile Computing,* Vol.3 Issue.1, January- 2014, pg. 385-392 © ***2014.***

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

[8] Kashyap Balakrishnan, Jing Deng, and Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile AdHoc Networks," in *Lecture Notes in Electrical Engineering, vol. 127.* New York: Springer-Verlag, 2012, pp. 659–666.

[9] A. Tabesh and L. G. Frechette, "Security issues in MANET: A survey on attacks and defense mechanisms," *IEEE Trans. Ind. Electron.,* vol. 57, no. 3, pp. 840–849, Mar. 2010.

[10] T.V.P.Sundararajan, Dr.A.Shanmugam, " Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks," *ICGST-CNIR Journal, Volume 9, Issue 1, July 2009*

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

[12] A.Al-Roubaiey, T. Sheltami, A. Mahumad, E. Shakshuki, H. Mouftah, " AACK: Adaptive Acknowledgement Intrusion Detection for MANET with Detection Enhancement", The 24th International Conference on Advanced Information Networking and Applications (AINA), IEEE Computer Society.

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

[14] D.B. Johnson, D.A. Maltz, and Y. Hu, "The Dynamic Source Routing Protocol for Mobile ad-hoc Networks (DSR)", IETF Internet Draft, July 2004.

[15] C. E. Perkins and P. Bhagwat "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers" In Proc. Of ACM Special Interest Group on Data Comm. (SIGCOMM '94), pp. 234-244.

[16] Sanzgiri, K., Dahill, B., Levine, B-N., Shields, C. and Belding-Royer, E-M. 1999," A review of current routing protocols for ad-hoc mobile wireless networks" Personal Communications Magazine.

[17] C. E. Perkins, E. M. Royer, S. R. Das, " Ad Hoc On-Demand Distance Vector (AODV) Routing", Internet Draft, draft-ietfmanet-aodv-10.txt.

[18] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626

[19] S. Marti, T. J. Giuli, K. Lai, and M. Baker " Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), PP. 255-265

[20] S. K. Sarkar, T. G. Basavaraju, C. Puttamadappa, "Ad Hoc Mobile Wireless Networks" Auerbach Publications.

[21] Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE Communications Surveys & Tutorials, Vol 13, No.4, pp 658-672.

[22] Balakrishnan, K.; Jing Deng; Varshney, V.K., "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)

[23] K. Sangeetha., "Secure data transmission in MANETS using AODV ", In Proceedings of International Journal Of Informative & Futuristic Research,Volume -1 Issue -5, January 2014

[24] Ramya K, Beaulah David and Shaheen H, "Hybrid Cryptography Algorithms for Enhanced Adaptive Acknowledgment Secure in MANET ", In Proceedings of IOSR Journal of Computer Engineering (IOSR-JCE) ,Volume 16, Issue 1, (Feb. 2014), PP 32-36