*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834, p-ISSN: 2278-8735*
*PP 18-23*
*www.iosrjournals.org*

# Acknowledgement based Security for Manets Against DDOS attacks

Joglekar C.M.[1] & Naoghare M.M.[2]
[1,2](Comp. Engg. Dept., SVIT Chincholi, SPP Univ., Pune(MS), India)

***Abstract :*** *Wireless MANET Mobile AD-HOC Network is an emerging technology and have great strength to be applied in critical situations such as military applications, battlefields commercial and most important and critical applications. Every node in MANET has its own routing capability and free to move in any direction as it does not have centralized infrastructure. However, the open medium and wide distribution of nodes in MANET faces security. Chances of attack on MANET increases as wireless sensor nodes are in unattended environment; there are many types of attacks for example wormhole denial of service, black hole etc.; the DDOS is one of them. DDOS affects network by increasing routing load, end to end delay, packet drop and many other parameters. So it is very important to design and develop effective intrusion-detection system to protect MANET from DDOS attacks. In this paper, we discuss DDOS attack on MANET, and propose and implement a enhanced intrusion-detection system to detect DDOS type of attack and provide security against it using hybrid cryptology for acknowledged packets.*

***Keywords :****Acknowledgment (ACK), Mobile Ad hoc Network (MANET), Distributed Denial of Service (DDOS).*

## 1. INTRODUCTION

Mobile nodes which communicate with each other without centralized infrastructure is Mobile Adhoc Network MANET. Communication between each node is bidirectional however these nodes cannot communicate with each other if distance between them is beyond the range; So Manet is divided in two types of network single hop and multihop to relay data transmission. In a single-hop network, all nodes within the same radio range communicate directly with each other and in multi hop nodes depend on other intermediate nodes to transmit if the destination node is out of their radio range due to this it is vulnerable to attacks. So traditional based IDS are no more feasible .So secure intrusion detection system is to be build for MANET. One of the most powerful attack is DDOS where huge amount of packets are sent to target all over the network this uses large amount of bandwidth thereby dropping important packets to reach the target and as MANET is used in military applications it is important to build the secure IDS for MANET.

## 2. BACKGROUND

*IDS in MANETs*

In this section we describe three approaches of IDS based on acknowledgement and also discuss some possible types of attack on MANET. Three existing approaches are: Watchdog [4], TWOACK [2], Adaptive Acknowledgment (AACK) [5], and EAACK [1]

1) Watchdog*:* Marti et al. [4] proposed a scheme named Watchdog. Watchdog serves as IDS for Manets by detecting malicious node that misbehaves in the network. It detects malicious node by listening to the next hop in transmission, if watchdog finds that next node fails to transmit the packet within period of time then it increases the its failure counter and if it reaches its threshold then it reports the node as malicious. Advantages has made watchdog popular but has disadvantages too. It fails to detect malicious behavior with following:

1) Ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report;5) collusion; and 6) partial dropping.

2) TWOACK: TWOACK proposed by Liu et al. [3] is one of the most important approaches among them. It detects the misbehaving by acknowledgement from every three consecutive nodes from source to destination; each node has to send the acknowledgement upon retrival of packet to the node two hops away down the route. If packet is not received in predefined time then both nodes are reported as malicious. It works on DSR .Twoack solves the problems such as receiver collision and limited power transmission but increases the unwanted network overhead by acknowledge process required by the packets in transmission.

3) AACK*:* Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. AACK reduces network overhead faced by twoack.In this a packet is send from the source node and all intermediate nodes forwards the packet to the destination node, as the packet reaches the destination node has to send the acknowledgement packet to the source node on the same route in reverse order, if this packet is not received the acknowledgement in predefined time then source nodes shifts to twoack node this reduces the network overhead but still fails to detect malicious node due to false report and forged acknowledgement packet.
4) EAACK: It handles three weakness of watchdog such as false misbehavior, limited transmission power, and receiver collision, N. Kang et. al.[1] proposed a system called Enhanced Adaptive Acknowledgement(EAACK) it consist of three parts as.
A. Acknowledgement mode: It is basically the end-to end acknowledgement in predefined time else switches to S-ack mode.
*B.Secure-Acknowledgement mode:* This part is basically to determine misbehaving nodes in the route. Every two consecutive nodes should send acknowledgement to source node in reverse path,so misbehaving node will be detected if acknowledgement not received in predefined time and then shifts to MRA –mode. to confirm misbehavior report.
C. Misbehavior reporting acknowledgement mode: This is designed to detect whether the destination node has received the missing packet through different route. to detect the misbehaving node with presence of false misbehavior report because this report can be generated by malicious attacker to report innocent nodes as malicious. this attack can be harm for entire network. If reported packet was received, if already received then it concludes that this is a false misbehavior report and whoever has generated this report is declared as malicious. Otherwise report is trusted.
EAACK fails to detect is source get attacked and also increases the overhead and time required to deliver the packet.
5) TYPES OF ATTACK:
a. Denial of service: it completely disrupts the routing information by creating the bogus route information thereby disrupting the the establishment of routes and to use resources of the participating nodes and consumes batteries by keeping the nodes engage in finding the routes which leads to overflow of the routing table.[7]
b. Distributed denial of service: In denial of service only one node participates in the attack whereas in DDOS many nodes participate in the attack thereby disrupting routing information. All nodes at a time attack on victim node by sending huge amount of packets which will consume bandwidth and victim will not be able to receive important packet [7].

## 3. PROBLEM DEFINITION

Three weakness of watchdog such as false misbehavior, limited transmission power, and receiver collision along with to detect if source gets attacked and to reduce overhead and increase packet delivery ratio are handled by our [proposed system. The three problems in detail:
1. Receiver collisions: for example node A sends packet 1 to node B it overhears that whether node B has forwarded the packet to node C at the same time node X is sending packet 2 to node C, node A overhears that node B has successfully forwarded the packet to node C but failed to notice that node C has not received the packet 1 due to collision between node 1and node 2.
2. Limited Transmission power: In order to preserve own transmission power node B limits its power such that it is strong enough to be overhear by node A but not strong enough to be received by node C
3. A False Misbehavior Report: node A successfully overhears that node B has forwarded packet to node C, still node A reports as node B misbehaving.
So in our propose IDS we use improved EAACK with additional node as IDS node which will routing protocol [9].As the system is completely based on acknowledgement packets it needs security so we extend the research by adding hybrid cryptography by using algorithms such as AES and Blowfish during packet transmission to ensure integrity and authenticity of all acknowledgement packets.

## 4. SCHEME DESCRIPTION

In this section, we describe our proposed scheme in detail each node in the network is bidirectional. Additionally one node is set as attack node and one node source node as IDS node. Hybrid cryptography (AES and blowfish algorithm) is used to prevent acknowledgement packets from attacks. Our system Improved

EAACK consists of major parts of EAACK which are already discussed. and additional part such as attack node, IDS node. To detect DDOS attack.

1. Attack node

In this we create one node as attacker node whose parameters are set such as scan time, scan port, infection rate, attacker node then sends probing packet to all other nodes .Any weak node in the radio range then agrees for communication with attacker node when that probing packet is received by the node is infected then this infected nodes launch DDOS attack and infect next node so on in that case overall network is infected.

2. IDS NODE

In this one node is set as IDS node that watches all the nodes in the range for abnormal behavior in the network. That node creates the normal profile which contains information such as packet type (TCP, UDP, CBR), time of packet (sent, received) and threshold value.

3. Acknowledgement mode

It is basically the end-to end acknowledgement .In this S node sends out the packet to the destination node if all the nodes in the path are cooperative then node D.Successfully receives the packet, then node D has to send the acknowledgement to the node S along the same path in reverse order in predefined threshold time. If node S receives the packet in the time defined then the packet transmission from node S to node D was successful else it switches to S-ACK mode.

4. Secure-Acknowledgement mode

This part is basically to determine misbehaving nodes in the route. IDS node here compares the normal profile with each new trace value, then to find the attacker scheme proposed by Liu *et al.* [3] is applied every third consecutive node needs to send S-ACK acknowledgement packet to the first node, if first node does not receive this packet in the predefined time then both nodes are declared as misbehaving nodes. Then are scheme moves to MRA mode to confirm misbehavior report.

5. Misbehavior reporting acknowledgement mode

This is designed to detect whether the destination node has received the missing packet through different route. It solves the weakness of watchdog when it fails to detect the misbehaving node with presence of false misbehavior report because this report can be generated by malicious attacker to report innocent nodes as malicious. This attack can be harm for entire network. To start MRA mode the source node searches for alternative route and sends packet to destination node by diverting the misbehavior reporter node. When destination receives MRA packet taking the help of ids node it compares if reported packet was received, if already received then it concludes that this is a false misbehavior report and whoever has generated this report is declared as malicious. Otherwise report is trusted.

In our proposed system as the IDS node is introduced which maintains the profile along with the information of affected node .So when in MRA mode it is searching for alternate path it will select the path comparing it with profile & log as it will not select the affected node in it will increase the throughput of the system and by acknowledgement we will get sure that the packet has reached the destination.

```
Algorithm
Create node =ids;
If ((node in radio range) && (next hop! =Null)
{
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
{pkt_type; //  TCP, CBR, UDP
Time;
Tsend, trecv, tdrop, rrep, rreq
}
Threshold_parameter ()
If((load<=max_limit)&& (new_profile<=max_threshold) &&(new_profile>=min_threshold))
{
Not DDOS attack;
```

```
        Shift to ACK mode()//send acknowledgement to the source node
        }
        Else {
        Attack in network;
        Find_attack_info (); // by IDS Node
        Shift to S-ack mode()
    }
      Else {
        "Node out of range or destination unreachable"
        Find_attack_info ()
        {
        Compare normal_profile into each trace value
        If (normal_profile! = new trace_value)
        {
        S-ack mode generates Node misbehavior Report
         shift to MRA ();
        }
```

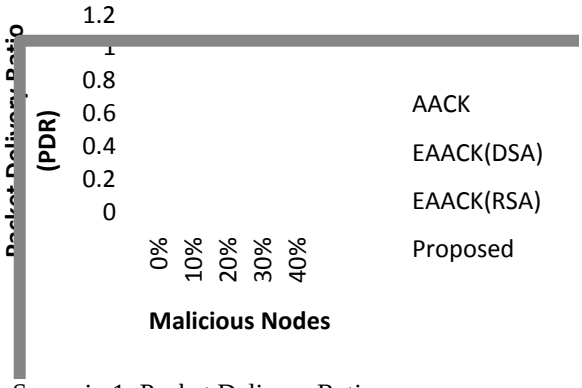
As in our proposed system we rely on acknowledgement packets to detect misbehaving in the network; we need to secure acknowledgement packets to maintain integrity so hybrid cryptography a combination of AES and Blow fish is used for encryption and decryption to safeguard the data. Blowfish t uses symmetric block cipher variable key length from 32 bits to 448 bits for securing data it uses Feistel Network iterating simple encryption function 16 times with block size 64 bits. AES with block size of 128 bits 196 bits and 256 bits works on substitution principle and encrypts data in one pass. The plaintext is the input to blowfish then output cipher text of blowfish is the input to AES and the output of AES is the double encrypted cipher text which is the strongest cipher text we receive .This provides high security as we need that to use in applications such as military.

## 5. RESULT

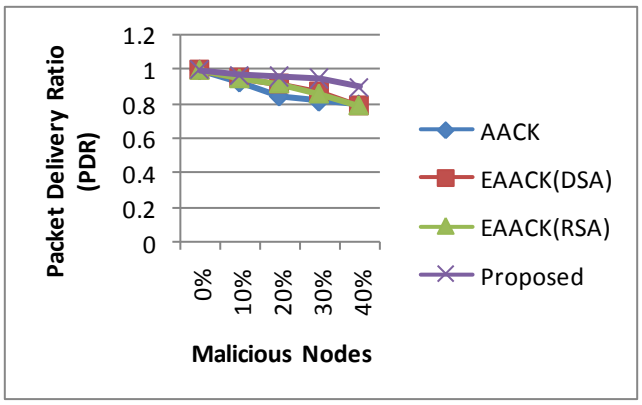
We implemented the system in real time to compare the performances one of the parameter performance parameter PDR was used.Packet Delivery ratio(PDR): defines the ratio of number of packets received by the destination to the number of packets sent by source node.

The graph shows the results with three scenarios:

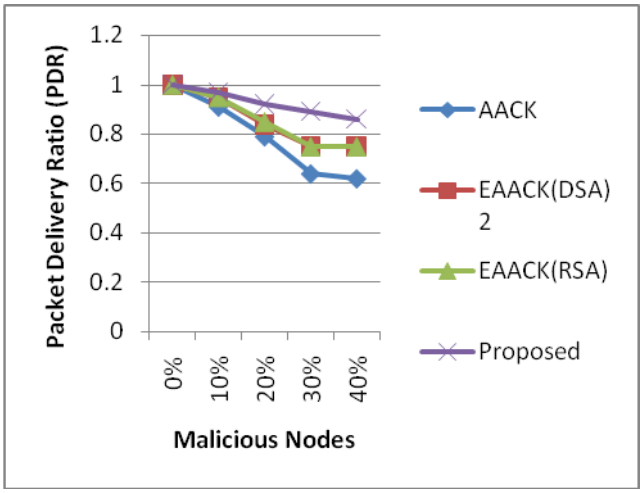
1. Scenario1: Malicious nodes drop all the packets that pass through the network. Table shows that EAACK's performance drops due to MRA but proposed system increases it as it receives MRA acknowledgement fast.
2. Scenario2:In this we set all the malicious node to sent false misbehavior report in this our proposed system works more than 90% due to MRA mode with IDS node as it finds the alternate route faster. To detect misbehavior node.
3. Scenario3: In this we set malicious node with ability to forged acknowledgement packets. In this our system shows the improved results.




Scenario 1: Packet Delivery Ratio




**Scenario 2: Packet Delivery Ratio**




Scenario 3: Packet Delivery Ratio

## 6. CONCLUSION

With our proposed system it not only helps us to detect the DDOS type attacks but also increases the PDR as shown in our results as DDOS attack is the dangerous and it affects network load. This type of attack also ditrupts the routing information but as we maintain the IDS Node with profile by comparing we get the results fast as to which node is affected or may be affected and find the alternate route faster. Hydrid

crytopgraphy (AES & Blowfish) provides double encryption nad is faster.. In future we can use the system with other protocols to find the different types of attacks.

## REFERENCES

[1] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE "EAACK—A Secure Intrusion-Detection System for MANETs" IEEE Transactions on Industrail Electronics, VOL. 60, NO. 3, March 2013
[2] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviourin MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5,pp. 536–550, May 2007.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviourin mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. MobileComput. Netw., Boston, MA, 2000, pp. 255–265.
[4] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Videotransmission enhancement in presence ofmisbehaving nodes inMANETs,"Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.[26]
[5] K. Al Agha, 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.
[6] Prajeet Sharma, Niresh Sharma, Rajdeep Singh" A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network" International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012
[7] A.Anna lakshmi and Dr.K.R.Valluvan " A Survey of Algorithms for Defending MANETs against the DDoS Attacks;" Volume 2, Issue 9, September 2012 ISSN: 2277 128X
[8] 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
[9] 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.
[10] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged Acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.