Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

INTRUSION DETECTION SYSTEM IN MOBILE ADHOC NETWORK USING CLUSTERING TECHNIQUES WITH ASACK: AN ADVANCED SAFE ACKNOWLEDGEMENT SCHEME

Bharathisindhu.p [1],Dr S.Selva Brunda[2]

[1]*Ph.D Scholar, Bharathiar University*
[2]*Head of the Department,Cheran College of Engineering*

ABSTRACT: *The challenges of new innovation accompanies with the wireless technology. The technology is improved day to day to accompany the challenges of new innovation. MANET is self configured and connect with devices without wire. All devices in MANET act independently in all direction. The networks are protected with various firewalls for preventing the intrusion and to monitor the networks and able to prevent the network from intrusions. The limitation and lack of mid monitoring, the attacks such as passive and active can be easily following the MANETs. The proposed ASACK model with supervisor table helps to increase the efficiency and speed of the networks. The supervisor table proposal also helps the packets to reach the destination with minimum number of delays, minimum cost, and minimum packet loss when compared with existing schemes.*

Keywords*: MANET, Intrusion Detection System, ASACK*

I. INTRODUCTION

The configuration of the Mobile Adhoc Networks (MANETs) is centralized which is self configured and connected by the links without wires. It is wireless network without any infrastructure. Efficient routing protocols make the MANET reliable. MANET facing various security issues, though they are self configured. The characteristics of MANET are used in military and disaster management applications [1]. The various challenges faced by the MANET are peer to peer applications [2], security [3], and maintaining network topology [4]. The MANET works with open boundary. The traditional security mechanisms are impossible to prevent the intrusions. MANET provides an ease method for communication establishment and rapidly deployable communications [5]. The proposed schemes helps go prevent the misbehaving node over the Adhoc network and to control the damage by those misbehavior nodes. The proposed model helps to increase the efficiency of the overall network.

Routing protocols helps to discover network topology and built a route to forward the data packets and maintains the route between the communications. The classification of routing protocols are proactive, reactive and hybrid protocols. The proactive types of protocols are table driven; the routing table maintains all the information. The proactive types were constant and keep informed regularly. Some of the proactive protocols are DSDV (Destination Sequence Distance Vector), OLSR (Optimized Link State Routing), and HSR (Hierarchical State Routing). The reactive protocols are called On Demand routing protocol. Some of the reactive protocols are DSR (Dynamic Source Routing), AODV (Adhoc On demand Distance Vector). The hybrid protocols are the combination of both proactive and reactive. The hybrid protocols are ZRP (Zone Routing Protocol), TORA (Temporally Ordered Routing Algorithm).

The adhoc network and their related research were found in [6][7].Adhoc networks were addressed by many researchers over the years. MANET used generally and apprehensive with security issue. The major disadvantage of the MANET is that it assumes every node in network as mutual and is not malicious. The classification of dropping packets in MANET into two types: intended misbehavior and unintended misbehavior [9].

II. RELATED WORK

The basic of many intrusion detection techniques is Watchdog system and it was proposed by Sergio Marti et al [10].In the Watchdog system, it identifies the misbehavior node and failed to agree the forward packets in MANET. Due to the ambiguous collision, receiver collision, limited transmission power, false misbehavior reporting and partial dropping the Watch Dog might failed to detect the presence of Malicious Node. Next to Watchdog, Path rater was proposed and it helped the routing protocol to help to avoid the misbehavior node. The Enhanced Watchdog (ExWatchdog) focused on the weakness of the Watchdog mechanism [11]. In ExWatchdog it maintains a table for each node that holds the count of packet sent, packet received respectively. Then Novel intrusion detection and response system called Route guard. This Route guard technique combines both Watchdog and Path rater [12]. The enhancement of Watchdog technique is

proposed by Parker et al in [13]. Here two response mechanism where proposed such as passive response mode and active response mode. Another mechanism called CONFIDENT which stands for Cooperation of Nodes Fairness in Dynamic Adhoc Networks [14] was proposed by Sonja Buchegger et al. In each and every node in CONFIDENT maintains four main components namely a monitor, reputation system, a path manager and a trust manager. A 'CineMA' stand for Cooperation Enhancement in MANET is proposed for maintaining the misbehaving node by limiting the number of packets forwarded shown in [15].

The watch dog methods are simpler and base for the all other methods. The TWOACK is proposed by Balakrishnan et al [16] that replaces Watchdog and solves the problem of the receiver collision and limited transmission power. This scheme is used in source routing protocol. In TWOACK each forwarded packet has to be acknowledged. The AACK is considered as Enhanced TWOACK aims to improve the performance of TWOACK proposed by Shakshuki et al [17]. To detect the selfish Gunasekaren et al[18]as AAS(Authenticated Acknowledgement Scheme).Those selfish nodes were eliminated and networks is free from intrusions. Selfish node only send the packets to destination that could not focussed on the neighbour node.

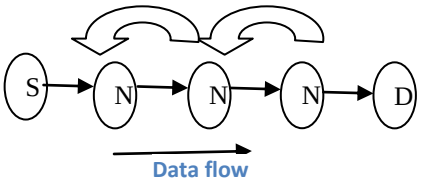


Figure-1 Operation of AAS

The EAACK (Enhanced Adaptive Acknowledgement) was proposed by Nankang et al [19] are bidirectional. The EAACK scheme mainly classified into 1.ACK 2.SACK 3. MRA.

Packet Flag	Packet Type
01	ACK
10	S-ACK
11	MRA

Table 1: EAACK Scheme

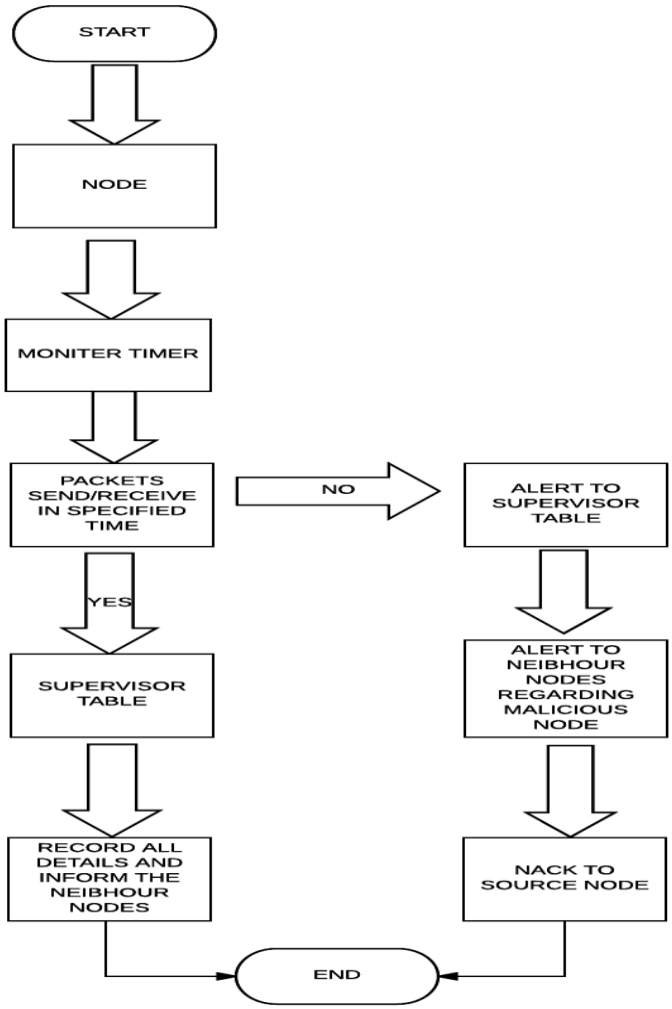
The EAACK can detect the malicious node with the fake misbehaving report. Also it sends the Acknowledgement (ACK) and No acknowledgement (Nack) to previous nodes whenever the packets reaches the destination. Along with that it has both S-Ack and MRA to send the report of the node status.

III. MOTIVATION

IDS help as a defence layer for MANET to detect and prevent various attacks such as black hole, gray hole. Worm hole, denial of service, distributed denial of service attacks. To improve the efficiency of the MANET and detection accuracy.

IV. PROPOSED MODEL

We propose a scheme called ASACK (Advance Safe Acknowledgement Scheme) with the monitoring timer and supervisor table on each and every node in the MANET. The monitoring table helps to maintain the timings of send and receive packets of the node. Also it helps to monitor the node whether it receiving the packets from the promising node or malicious node.



Flow Chart 1: ASACK Scheme

The supervisor node helps to maintain the information about the node and packets whether it receives from the promiscuous node or malicious node. Once the node receives the packets from the neighbour node it check with the supervisor table and verifies that the neighbour node is original or malicious. If it is original node it again forward the packet and saves that node is not malicious. If it is malicious and doesn't match with the monitoring timer the packets from the neighbour sends the NACK back and send the suspect alert to its neighbour. Mean while every node in the network get the alert that the node is malicious and the packet receive from the node is malicious. The mean, standard deviation results are estimated to find the difference with actual and estimated values.
The actual and the expected value help to find the difference value of the node.

1. Mean= $\frac{s1+s2+s3+s4+s5}{5}$

2. Standard deviation = $\frac{1}{n}\sqrt{\sum_{i=1}^{n}(X_i - mean)^2}$

3. Variance = $(S.D)^2$
4. Expected value= (mean+ variance)

The difference value is upper than the threshold value it is fount the node as the malicious else it is safer node.

V. PROBABILTY BASED CLUSTERING

We use probability based clustering identified the relationship between the values. By comparing the values with threshold value we can find the malicious node. The relationship is estimated with three parameters Mean, Standard

deviation and sampling probability. The mean is defined with μA and standard deviation is defined with σA. Samples are chosen with the probability of A. We can apply the three parameters and the probability of the instance x,

$$P(A/x) = p(x/A)\, p(A) / p(x)$$

We can normalize the result with their sum. The normalized value with the expected value is upper bound then it is said to be malicious node. The efficiency of network will increase when number of nodes compare at a single time.

VI. SIMULATION METHOD

The simulation is dome with Network Simulator (NS2). The default scenario is taken as the simulation configuration file. Our simulation consists of 100 nodes in the flat space with the size of 1000*1000m. The maximum hop allowed for this scenario is 100 nodes and the transmission range of coverage is 250m. Te 802.11 MAC layer and the antenna model is Omni-directional. The interval time for generating the packet is 0.1 sec and the size of the packet is 1000b.

The performance metrics are used

1. Packet delivery Rate It stands for the ratio of number of received packets by the receiving node and the number of sent packets by the sending node.
2. Transmission rate The average rate of transmission, effective speed of transmission.
3. Dropping Ratio It is measured as a percentage of packets lost with respect to packets send.
4. Time delay The waiting time taken by the sent packet and received packet.

CONCLUSION

The performance of the MANET may decrease when misbehavior node occurs and it leads to route failure. The Intrusion Detection System with Probability based clustering is proposed for identifying the malicious node. This scheme will helps to increase the speed of detecting the malicious node and packet delivery may increase without overhead. Network Simulator helps to show the result and able to view the graph. The network performance is increased when compared with existing schemes.

BIBLIOGRAPHY

[1] Security challenges in Mobile ADHOC Networks: A Survey. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

[2] A.Gantes and J.Stucky, “A flatform on a Mobile Adhoc Network Challenging Collaborative gaming” International Symposium on Collabrative technologies and system,2008

[3] K.U.R.Khan ,R.U.Zaman and A.V.G.Reddy, “ Ingrating Mobile Adhoc Networks and the Internet Challenges and the review of Challenges”, presented at the 3 rd International conference on communication systems software and Middleware and Workshops,COMSWARE,2008

[4] M.Suguna and P.subathra “Establishment of stable Certificate Chains for Authentication in Mobile Adhoc Networks”,presented at the International conference on Recent Trends in Information Technology (ICRTTT),2011

[5]Nishu Garg and R.P.Mahapatra “MANET Security Issues”, International Journal of Computer Science and Network Security, Vol.9 No.8,August 2009

[6] C.E.Perkins, Adhoc Networking,Addision Werley Professionals, December 2000

[7] M.Ilyas.,ed., The Handbook of Adhoc Wireless Networks.CRC press,December 2002

[8] Y.Zhang,W.Lee and Y.Huang, “ Intrusion Detection Techniques for Mobile Networks”(ACM WINET), Vol.9,No.5,September 2008

[9] A.Roubaiey,T.Sheltami,A.Mahmoud “AACK:Adaptive Acknowledgement Intrusion Detection for MANET with Node Detection Enhancement” IEEE Computer Society,2010

[10] S.Marti,T.J.Giuli,K.Lai and M.Barker, “Mitigating Routing Misbehaviour in Mobile Adhoc Networks” Proceedings of the 6th Annual Internataional Conference ono Mobile Computing and Networking(Mobicom ’00),pp.255-265,August 2000

[11] Nasser. N,Chen.Y, “ Enhanced Intrusion Detection System for Discovering Malicious Node in Mobile Adhoc Networks” Communications,2007. ICC’07.IEEE International Conference on, Vol.10, pp.1154-1159, 24-28, June 2007

[12] Hasswa.A,Zulkernine.M,Hassanein.H, “ Routeguard, :An Intrusion Detection and response system for mobile adhoc networks” wireless and mobile computing,networking and communication,2005.(WiMob ‘2005), IEEE International Conference on, Vol 3,pp. 336-343,August 2005

[13] Parker.J,Undercoffer.J,Pinkston.J,Joshu.A, “On Intrusion Detection and Response for mobile Adhoc Networks”, performance,computing and communications,2004 IEEE International Conference, pp.747-752,2004

[14] S.Buchegger,J.Y.L.Boudec, “Performance Analysis of the Confident Protocol(cooperation of Nodes: Fairness in Dynamic Adhoc Networks)”, in MOBIHOC ’02,2002

[15] M.Frank,P.Martini,M.Plaggemeier, “ Cinema: Cooperation enhancement in MANETS”, in proceedings of the 29th Annual IEEE International Conference on Local computers Networks LCN’02,2004

[16] Balakrishnan.K,Jing Deng,Varshney.V.K, " TWOACK: Preventing Selfishness in mobile adhoc Networks", Wireless Communications and Networking Conference,2005 IEEE,Vol.4,2137-2142, Vol.4,13-17 March 2005

[17] A.Roubaiey,T.Sheltami,A.Mahmoud,E.Shakshuki,H.Mouftah, " AACK:Adaptive Acknowledgement Intrusion Detection for MANET with node Detection Enhancement", IEEE 24th International conference on Advanced Information Networking and Applicaitons,2010

[18] M.Gunasekaran,P.Sampath,B.Gopoalakrishnan, "AAS: An Authenticated Acknowledgement Based Scheme for preventing selfishnodes in mobile adhoc Networks",International Journal of Recent Trends in Engineering,Vol 1,No.1,May 2009

[19] Nan Kang,Elhadi M.Shakshuki,Tarek R.Sheltani, " Detecting Misbehaving Nodes in MANETS",Security Issues,iiWAS2010 Proceeding 2010

