E^{2}AACK—A Secure Intrusion Detection System for Wireless Network

Mr.M.Saravanan[1], Mr.A.ThomasPaulRoy[2], Dr.N.Balasubadara[3]

[1].PG Scholar,PSNA college of Engg&Tech,
Dindigul,Tamilnadu,INDIA.
[1]Kmc.saravanan@gmail.com
[2].Associate professor,PSNA college of Engg&Tech,
Dindigul,Tamilnadu,INDIA.
[2]Pauli.dgl@gmail.com
[3].Head of the Department in IT, RMD college of Engg&Tech,
Kavaraipettai,Chennai,Tamilnadu,INDIA.
[3]balasubadra@yahoo.com

Abstract—**The exodus to Wireless networks from wired network is a growing field in the past few decades. Various wireless applications are made up of mobility and scalability based nodes. Among all the wireless networks Mobile Ad-Hoc network is one of the most significant and distinctive applications today. All the nodes are self employed, not fixed on a fixed network infrastructure, and it can act as sender as well as receiver, and directly communicate to the other nodes in the network within the communication range of the network. Also the nodes in the Wireless network can act as relay nodes to their neighbors to relay messages. Since the nodes in the Wireless Network having the ability to self-configuring by them, they are deployed in critical mission based applications like military usage or any kind of emergency recovery. Since the open medium and wide distribution of nodes make the network vulnerable to malicious attackers. In such situations, it is necessary to deploy an effective IDS mechanism to prevent or protect the Network from attacks. In the existing system EAACK – [Enhanced Adaptive Acknowledgement] is proposed as an IDS and it especially designed for MANET. In this paper a combined IP-trace back with E2AACK – [End-to-End Adaptive ACKnowledgement] mechanism is proposed to detect and prevent the malicious nodes in the network. The malicious node activity can be detected by IP-trace back and prevented by getting acknowledgement from both end nodes. The simulation result shows that the E2AACK approach provides higher detection rate and prevention which greatly affect the network performance in terms of throughput and delay**

Keywords: Wireless Networks; Intrusion Detection System; E2AACK; Malicious Nodes; Throughput, Delay.

I. INTRODUCTION

Mobile adhoc network is a collection of wireless sensor nodes can communicate with each other via wireless links and the nodes are self-organized they can accommodate by itself to the existing infrastructure, where the sensor node are not depending on the existing infrastructure. The nodes are random and dynamic, so the topology may change rapidly and unpredictably. The data packet sending and receiving is to be executed by the nodes themselves by individually or by collectively. Depending on the application and the area of the network the resource consumption gets vary. security in Mobile adhoc network is a critical tasks because maintain the confidentially ,reliability and supports the QOS.In this paper propose a combined **IP-trace** back with **E2AACK** – [**E**nd-to-**E**nd **A**daptive **ACK**nowledgement] mechanism is to detect and prevent the malicious nodes in the network. Trace the malicious node location is a complex tasks because malicious node uses the ip spoofing mechanism. so that in this mechanism can be detect the malicious node activity by IP-trace back and prevented by getting acknowledgement from both end nodes.

II. SYSTEM ANALYSIS

A.Related works

In paper [1] defines the two different techniques one is DLLT another one is PPPM. Generally DDOS attackers uses the source address spoofing so that easy to trace the attackers locations but this technique sleuth to trace attackers locations and this implementation doing there Hybrid Networks. On [2] describes the IP trace back DFM, it consist of PPM, DPM IP Trace back schemes. In this techniques are concentrate to the NAT based intrusion detection because attacks are originated to the behind the ip address scheme. The main objective is securing the network infrastructure even to guarantee the secure communication.[3] refers to the trace malicious packet origin ,but it's not a easy task because attackers are using the address spoofing and dynamically change the locations at DDOS attack time. So that In this paper describes the two IP Trace back techniques packet marking and logging so that this techniques are helps to trace the malicious packet transmission origin and disable that node activities, it uses the storage space and record the packet transmission information and trace locations.[4] represents the FDPM, this technique ability to find the real attack sources in a developing network. Even though it consists of flexible mark length strategy to make it compatible to different network environments; it also effectively manages the network flow based on a flexible flow-based marking scheme.

On [5] trace the large scale network based DDOS attacks and their source victim. In this paper presents the dynamic marking and mark based detection scheme, its reliable to increase the possibilities of trace the master attacker locations with minimum no of packet transmissions. When this technique implements only the source routers because marking packets are delayed it discards the transmissions. On [6] to overcome the Hybrid IP trace back techniques limitations and propose the novel approach for minimize the memory use ,increasing the detection rate and also reduces the packet calculation rate.

In existing technique are does not supports the packet marking and logging information refreshments but this approach supports the all things. [7] it focus on node security, low overhead, path and memory management. DDOS attack detection is very complicated task because attackers wear the fake IP address mask so that find the original ip address is a complex process. But these papers propose the novel technique for trace the attacker's original source within a minimum no of packer transmissions at a same improves performance. In[8] to describes packet marking and logging is a logical treatment for ip trace back technique but is to be use the maximum memory space during the packet inspection so that this paper propose the novel technique for reduces the memory usage and increases the possibilities for attacker location detections. In [9] describes the entropy based attacker detection scheme that is variations between the normal and DDOS attack entropy values so that it implements the packet marking in entropy base ip trace back technique because reduces the refreshment time during the packet inspection.

On [10] describes the numerous analysis schemes for IP trace back technique and it overcomes the packet marking memory utilization problems even it gives the accurate outcome for entire system. In [11] present a hash-based technique for IP trace back that generates the traffic detection report for the Wireless network, and it can easily trace the source of a single IP packet delivered node by the network .it demonstrate the system and space-efficiency.This approach requiring approximately 0.5% of the link capacity per unit time in storage, and this implementation must be doing in current or next-generation routing hardware. On [12] propose the log based IP trace back approach for reducing the overhead on routers. it can use mathematical analysis and simulations to evaluate this approach,namely this log based called as Source Path Isolation Engine (SPIE), This approach maintains the ability to trace a single IP packet while reducing the storage overhead by half and the access time overhead by a factor of the number of neighboring routers. In [13] present a novel IP trace back system is called Deterministic Packet Marking and with packet logging . this approach ability to provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. It describes the new hybrid IP trace back scheme with efficient packet logging. It have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve low false positive rates and negative rates in attack-path reconstruction.it overcomes the packet marking memory utilization problems even it gives the accurate outcome for entire system. In [11] present a hash-based technique for IP trace back that generates audit trails for traffic within the network, and it can trace the origin of a single IP packet delivered by the network .it demonstrate the system effectiveness, space-efficient (requiring approximately 0.5% of the link capacity per unit time in storage), and implementable in current or next-generation routing hardware.

On [12] propose the log based IP trace back approach for reducing the overhead on routers. it can use mathematical analysis and simulations to evaluate this approach. It compared to the state-of-the-art log-based approach called Source Path Isolation Engine (SPIE), This approach maintains the ability to trace a single IP packet while reducing the storage overhead by half and the access time overhead by a factor of the number of neighboring routers. In [13] present an IP trace back system called Deterministic Packet Marking and with packet logging which provides a defense system with the ability to find out the real sources of attacking packets that traverse through the network. It describes the new hybrid IP trace back scheme with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction.

B.EAACK

In EAACK, the RSA-[Digital signature with message recovery], DSA-[Digital signature with appendix] based secured data communication was proposed. Since in the existing system the acknowledgement is received from neighbor nodes commonly while route discovery, there may be a forged acknowledgment attacks can happen. To overcome this problem and reduce the system complexity in terms of time and memory usage, E^2AACK is proposed.

C.E^2AACK

A network G consists of N number of nodes, where the entire network is divided into several regions. Entire communication world contains various kinds of wireless networks, each network, regions has its own unique number termed as ID. In this proposed approach any node can transmit data to any node, where a node s considered as source node and node D is considered as Destination node. Where, k number of nodes can occur in the route as intermediate nodes and those can be verified as malicious nodes or not by ACK method and trace the IP address of the nodes. In this network all the nodes are assigned by a key and the key is created in such a manner:

$$Key(nodei) = \text{"Node-ID"} + " \ Region - ID" + \text{"}Network - ID\text{"}$$

Example,

$$Key\ (node - 4) = \ "4" + "3" + "7" \ = \ 437$$

In this network, from source node to destination node, a secure route is discovered, then verifies the intermediate nodes and transmits the data in the same route. Initially, the

source node broadcasts a REQ packet for neighbor request and receives ACK from several nodes. The ACK packets are verified and best nodes are selected according to the TIME, KEY, and Distance and trace the IP address of the node simultaneously. Once the neighbor is elected, the neighbor detail is recorded for future verification. The same procedure is repeated until a route discover up to Destination node from the source node.

Once route discovered, the source node start sending data packet to the next neighbor, and the next neighbor pass the data packet to the next neighbor and this process gets repeateduntil reaches the destination node. Iff, the key of the node matches with the Node-ID, Region-ID, network-ID and the IP address of the neighbor node the data packet will be passed to that neighbor node, else, the packet transmission is stopped and that neighbor is intimated as Malicious node and eliminated. The overall process of the E2AACK approach is given in the algorithm to verify its performance in any language or in simulation tools.

```
E2AACK_ Algorithm ( )
    {
Let G be a network with N number for node where N =
➢ {n1,n2,n3,…..nk }
➢ Let S – is source node, D – is Destination node,
➢ Route_Discovery(S,D,G)
➢ For I = S to D
    If [Node(i + 1).Key.valid ==
➢ true] &&
            [Node(i+1).IP.Valid == true]]
      Node(i+ 1).Data =
➢ Node(i).Data
➢     Node(i).ACK = Node(i+1).ACK
➢   Else
➢     Eliminate(Node(i+1))
➢     Look for next node
➢   End if
➢ End for
    }
    Route_Discovery(S,D,G)
    {
➢
➢ For I = S to D step 1
    If [Node(i).Key.valid ==
➢ true] && [TraceIP(Node(i)] then
      routeTable =
    append[routeTable[ [Node(i),…]]
➢ Else
➢     Discard the node
➢ End if
➢ End for
    }
```

D.Simulation Settings

Using Network Simulator-2, the E2AACK algorithm is implemented in C++ code where the network topology is created in NS2-TCL code and the performance of the algorithm is evaluated and the corresponding results are produced below. To simulate the approach some of the parameters should be set in the Ns2 simulation tool and it shown in Table-1.

[1] Parameters	[2] Value
[3] Area	[4] 1200 x 1200
[5] Routing protocol	[6] AODV
[7] Mac	[8] 802.11
[9] Propagation Model	[10] Radio Model
[11] Number of Nodes	[12] 20, 40

Table-1: Simulation Settings

Using the above configuration the algorithm is written in C++ with TCL coding and the number of malicious node detected, throughput due to the algorithm is verified and evaluated.

The following figure shows the performance of the proposed approach.

III.RESULTS AND DISCUSSION

The numbers of malicious node activity occur in the network in the existing and proposed is compared by changing the number of nodes deployed in the simulation as 20, 40 and the obtained throughput is shown in the Figure-1.

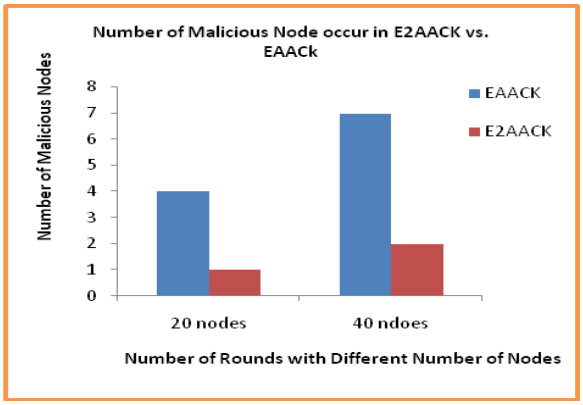

Figure-1: E2AACK Vs. EAACK Number of Malicious Node Occur

The throughput of the existing and proposed is compared by changing the number of nodes deployed in the simulation as 20, 40 and the obtained throughput is shown in the Figure-2.

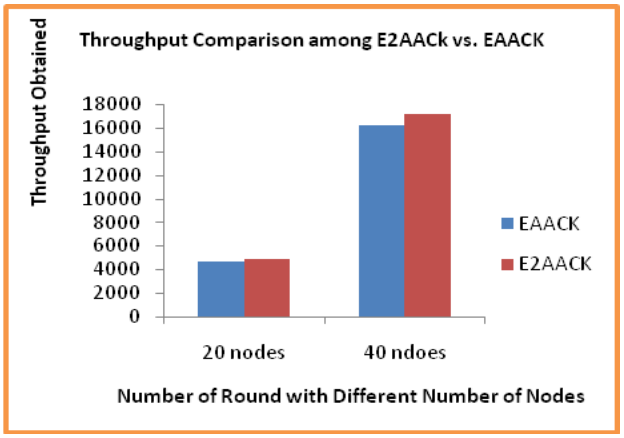

Figure-2: E2AACK Vs. EAACK Throughput

The delay of the existing and proposed is compared by changing the number of nodes deployed in the simulation as 20, 40 and the obtained throughput is shown in the Figure-3. The delay of the existing and proposed is compared by changing the number of nodes deployed in the simulation as 20, 40 and the obtained throughput is shown in the Figure-4.

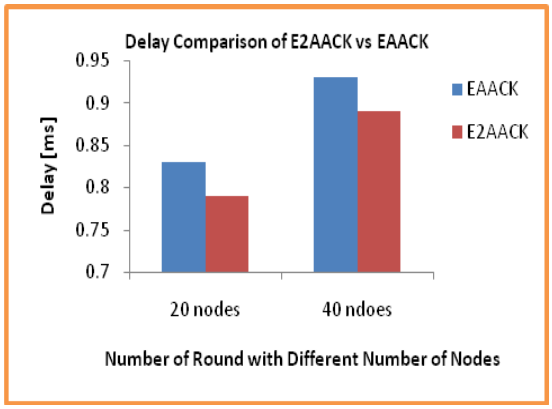

Figure-3: E2AACK vs. EAACK Delay

The remaining energy of the existing and proposed is compared by changing the number of nodes deployed in the simulation as 20, 40 and the obtained throughput is shown in the Figure-4.

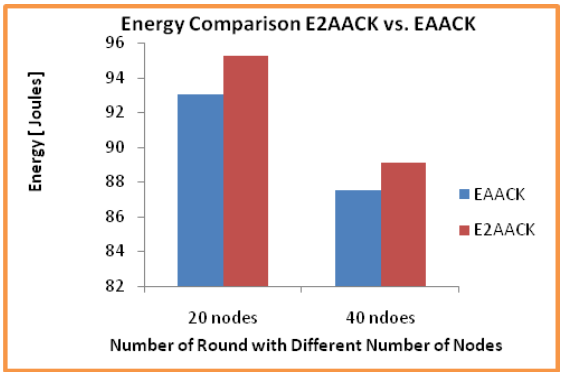

Figure-4: E2AACK Vs. EAACK Energy Saving

IV.FINDINGS AND SUGGESTION

From the Figure-1, Figure-2, Figure-3, it is clear that the E2AACK is efficient than the EAACK the number of malicious activity is reduced from 4 into 1 and 7 into 2 for 20 nodes, 40 nodes deployed in the network respectively. The throughput is increased from 4678 into 4876, 16234 into 17122 for 20 nodes, 40 nodes respectively. In terms of delay the proposed approach takes less time than the existing approach where it reduces the time from 0.83% into 0.79% and 0.93% into 0.89% for 20 nodes and 40 nodes respectively. In terms of Energy saving, the proposed approach saves energy from 93 to 95.23 and 87.54 into 89.12 joules for 20 nodes and 40 nodes respectively. Since, the E2AACK approach is considered and proved as an efficient approach than the EAACK approach.

V.CONCLUSION

From the results and Discussion section and from Figure1, 2, 3, and Figure 4, it is clear and proved that the E2AACK approach provides security for Wireless network than the existing approaches and it improves the QOS of the network in terms of throughput, delay, energy and detection rate, prevention rate of the malicious nodes. In future, this proposed approach is applied for huge size network with multiple regions and compared with current security approaches to prove the efficiency**.**

REFERENCES

[1] Durgarani Basireddy1, Sreekanth.K2 “Establishing Source of Spoofing Attack Using IP Hybrid Trace back Scheme IP trace back through (authenticated)” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013

[2] Vahid Aghaei-Foroushani* and A Nur Zincir-Heywood “IP trace back through (authenticated) Deterministic flow marking: an empirical Evaluation” Aghaei-Foroushani and Zincir-Heywood EURASIP Journal on Information Security 2013, 2013:5 http://jis.eurasipjournals.com/content/2013/1/5ARCH

[3] Dong yan, yulong wang, sensu and fangchun yang “A Precise and Practical IP Trace back Technique Based on Packet Marking and Logging” journal of information science and engineering 28, 453-470 (2012)

[4] Yang Xiang,Wanlei Zhou,and Minyi Guo,”Flexible deterministic packet marking”An ip traceback system to find The real source of attacks” ieee transactions on parallel and distributed systems, vol. 20, no. 5, may 2009

[5] Reza Shokri,Ali Varshovi,Hossein Mohammadi,Nasser Yazdani,Babak Sadeghian “DDPM: dynamic deterministic packet marking For ip traceback”

[6] N.Srilakshmi,K.Rani”An Improved IP Traceback Mechanism for Network Security” international Journal of research in Engineering and Technology

[7] Andrey Belenky and Nirwan Ansari,"IP Traceback with Deterministic Packet Marking" ieee communications letters, vol. 7, no. 4, april 2003

[8] INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGIES, VOL. 01, ISSUE 03, SEP 2013 "RIHT: a novel hybrid ip traceback scheme" Ms. U prashanthi,Mr. D srikanth

[9] Ezhilarasi.S "Traceback of ddos attacks using entropy variations"

[10] international journal of reviews on recent Electronics and computer science "Hybrid traceback on deterministic ip packet marking Schema" Harish Pabba, K.Sandhya Rani

[11] Alex C. Snoeren,Craig Partridge,Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio,Beverly Schwartz, Stephen T. Kent, and W. Timothy Strayer"Single-Packet IP Traceback" ieee communications letters, vol. 7, no. 5, May 2004

[12] Chao Gong and Kamil Sarac,"A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking" ieee communications letters, vol. 6, no.4, June 2005

[13] C.Vaiyapuri,R.Mohandas "IP Trace Back Scheme for Packet Marking and Packet Logging Using RIHT" International Journal of Computer Science and Mobile Computing

