An Enhanced Cross layer intrusion detection and adaptive response mechanism for MANETs

I. Meenatchi[1] , K. Palanivel[2]

Abstract— **Mobile ad hoc networks are exposed to a multifariousness of various layer attacks such as session hijacking, DOS, rushing attacks, black hole, gray hole, sleep deprivation etc. In this paper we proposed the ECLIDAR methodology for cross layer intrusion detections which identify those attacks in the MANET. Simulation results exhibit the potent of the Intrusion detection and response method in diverse attack layouts, the proposed system improves the energy consumption, packet delivery ratio ,end to end delay. Our simulations show that our scheme is more effective and accurate than those based on isolated observations from any single layer.**

Index Terms— Attacks, Cross Layer, Intrusion, MANET

I. Introduction

A mobile ad hoc network is miscellaneous accordance to the infrastructure network which have deprived base stations. MANET altogether utilized in various emergency applications, Mobile Ad hoc Networks (MANETs) present most significant merits and have been incorporated in a varied range of applications such as disaster assistance [3], monitoring of environment [4] and vehicular networks [5]. Mobile ad hoc network also includes the wide space of vulnerabilities due to their challenges, which impacts the degradation of the network, hence assured communication in mobile ad hoc network is difficult[16].

Challenges in mobile ad hoc network comprises the omission of reliability towards the nodes withstand in accordance to its mobility and dynamism in the topology rapidly, so provoked to diverse malicious attacks. Inadequacy of security in network provokes the intruder to scatter the flow of data paves the way for the loss in data. Quality of service is reduced due to the dynamic nature of the network. Routing in mobile ad hoc network is the major challenge due to the frequent diverse nature of mobile ad hoc network.

Authentication and encryption would be used as the primary defense, Nevertheless those techniques lacks the well-organized defense to the attack[2], hence to overwhelm this attacks and challenges in MANET intrusion detection systems have been deployed in ad hoc network.

An IDS [6] is a software that facilitates the intrusion detection process, initial responsibility of IDS is to detect undesirable and intruder activities. It is the defensive mechanism in the mobile ad hoc network which provides the secured communication in between the nodes. In fixed networks, intrusion detection and system (IDS) acts as a second layer of defense beyond a firewall; whereas in MANETs IDS becomes the front line of defense to protect nodes from attackers [7] [8]. Unlike the fixed infrastructure the mobile ad hoc network lacks the access point and routers hence the IDS is located in each nodes of the mobile ad hoc network in spite of absence of centralized control. Many existing intrusion detection algorithm don’t indulge in punishment which makes the intruder nodes behavior normal[7].

This paper discusses the proposed methodology where the information from the cross layers is used instead of single layer which detects the attacks from all layers and makes the mobile ad hoc network reliable and also the simulation results discussed.

The rest of the paper is ordered as, Section 2 depicts the background of mobile ad hoc networks, cross layer, intrusion detection system section 3 comprises the mechanism of proposed system section 4 depicts the simulation results section 5 depicts the conclusion.

II. Background

A. MANET

A mobile ad hoc network is a self- organizing system of mobile nodes that communicate with each other through wireless links without fixed infrastructure. It includes the characteristics of mobility of nodes, vulnerability of nodes which leads capturing of nodes by attacker, frequently changing topology, More energy consumption, lack of security hence tends to diverse of attacks such as routing, packet modifications, eavesdropping and protecting a MANET under such environments is troublesome[16] MANET have no access points to transfer data towards nodes, it is done through multiple hops. Mobile node exhibits itself as both host and router to create a route[16].

B. Routing Protocols

MANETs routing protocols classified as either proactive or reactive. Proactive routing protocols were FSR, OSLR whereas reactive protocols includes AODV, DSR, etc. Proactive protocol not much productive as reactive protocols because of their overhead hence reactive routing protocols such as AODV and DSR mostly used in MANETs. In a proactive routing protocol [1] each node proactively looks for routes to further nodes, which regularly interchange routing messages, in order to maintain routing table up-to-date and error-free., the node will be maintaining one or more tables to save the information of the routes used for transmission of packets .

Due to limited constraints of energy consumption and bandwidth of MANET nodes, periodic transmission of routing messages would lead to the congestion of the network. In a reactive routing protocol [1] a route is analyzed and formed when two nodes decides to forward the data, if the source needs the route to a destination it will establish a route by route discovery procedure.

C.IDS

The Intrusion detection system is a method for detecting the attacks by analyzing and continuously monitoring network functions. Intrusion detection arises as a crucial defensive mechanism in mobile ad hoc networks. Intrusion detection systems would be deployed in each mobile node to monitor local traffic and to detect occurrence of local intrusions. These nodes can forward the intrusion information to neighbors when needed. Another technique in the IDS is to deploy intrusion detection system for self and neighbor nodes to check for malicious neighbor nodes present[16]The global intrusion detection system can be deployed for clusters of mobile nodes where cluster head node is responsible for global intrusion detection for its cluster [13].Three significant components of IDS include data collection, detection, and response [14]. The data collection is responsible for transferring data to a common format, data storage and sending data to the detection module [14].

The intrusion detection system gathers the audit data and cross check the data in order to find any attack in the network, with the established data used for auditing the IDS could be classified ad host and network based [6].A network based generally present in the gateway of the network and examines the packet whereas the host based system uses the operating system data to examine the attacks in the network. IDS classifications is of various types primarily includes Active and passive IDS, The active attack is set for automatic blocking of suspecting attacks which provides real-time remedial action for respective detecting attacks. A passive IDS is a system which is deployed to for monitoring and analyzing network traffic activity and provide caution to the nodes regarding vulnerabilities and attacks[16].

A knowledge-based Intrusion Detection Systems which consists of the database of previous attacks signatures and known system vulnerabilities for taking responsive actions. Anomaly-based Intrusion Detection Systems is the process of collecting data related to the performance of authorized nodes over a span of time which followed by examination applied to noticed behavior to determine with a highest degree of confidence that the behavior of intruder nodes not authorized. Even though false alarm rates is a primary problem for developing the intrusion detection system especially the anomaly based intrusion detection system, yet the system has fully met the desired objectives compared to the signature based system[15] Specification-based intrusion detection which frames specifications that capture authorized nodes behavior any variation from the framed specification marked as an attack.

D. Cross layer

Majority of intrusion detection system have been done for single layer attacks, they should be apply for different layers of the protocol. Since Distinctive identity of mobile ad hoc networks such as the dynamic nature of the channel ,lower signal strength, mobility of the nodes and optimum path selection using the network layer requires some scale of cooperation in the midst of various layers to enhance the whole network execution ,in order to overwhelm the above introduced issues a cross layer based methodology is used which exceeds the inclusive performance of the network which recognize the multi layered attacks .The basic purpose of cross layer design is to use multi layer parameters from OSI stack to increase the efficiency and performance of MANET[9][10]. The objective of applying a cross layer technique for routing procedure is to obtain valid path that are reliable and productive, different layers to collaborate and share network status information[11]. Various attacks emerges from flow in the protocols, and also due to the shortage of typical identification and authentication method, hence makes the network vulnerable, so the intruder nodes can utilize these vulnerabilities tends to the networking layers for malicious behavior hence dreadful attacks like packet dropping, routing disruption, jamming attacks or other forms of Denial-of-Service adversely affects the mobile ad hoc network communications[12].Below table lists the various cross layer

Table I- Cross layer Attacks[23]

Layers	**Attacks**
Physical	Jamming, Eavesdropping
Data Link	DOS, Malicious Behavior Nodes
Network	Black hole,grey Hole, worm Hole, Sleep Deprivation, Rushing Attacks
Transport	Session Hijacking,SYN Flooding

Many Cross layer intrusion detection algorithms had been deployed . In the adaptive real time routing algorithm detects the occurrence of new patterns of the routing traffic ,prioritize them based on their information content, next step is to adapt it with incremental update of the detection model for the reduced overhead using the new patterns[18].The authentication mechanism with symmetric key used for security of the network and the neighbor node value is calculated and based on the threshold value ,the attack in the node is detected[19].The novel cross layer intrusion is proposed where the association and clustering algorithm is used for attack detection[20].The distributed cross layer algorithm is used in which [21] the patterns and confidence value used for detection of the attacks in the network .Cross layer intrusion detection algorithm for reducing the false positive in attack detection also proposed[22].

III. RELATED WORK

In [24] Cross layer based adaptive real-time routing attack detection system for MANETS is proposed where the primary step is to detect the occurrence of new patterns of the routing traffic ,prioritize them based on their information content, next step is to adapt it with incremental update of the detection model for the reduced overhead using the new patterns. In[19] CLDASR the authentication method is used, where the source wants to send a route request packet it generates a hash value also encrypts the hash with the path using the shared symmetric key with the destination, if the threshold value greater than neighbor node forward count then the node is prone to the black hole or grey hole attack. Routing protocols have many downsides hence the intruders can compromise the node and launch the attack. In[21] the distributed cross-layer intrusion detection system for ad hoc networks collect the audit data followed by detection module where the anomaly detection is used for detecting deviation from the normal profile, if the node have more confidence value it is marked as anomaly. In[25]the approached intrusion detection method uses the heuristics method that detects more vulnerable attacks that target the multiple layers in the network .In[26] An Intrusion detection and adaptive response mechanism is provided for the nodes with network layer attacks.

IV. PROPOSED SYSTEM

Fundamental aim of the cross layer methodology is to use the parameters from the multiple layers and to elevate the methodical and performance of the mobile ad hoc networks. It utilizes the data's from various layers and improves the accurate detection, hence this implements the all-encompassing methodology that detects the attacks budding from any layer in the network. Each layers are inclined to different attacks hence subsequently considering the information from those layers is indispensable hence we proposed the algorithm enhanced cross layer intrusion detection and adaptive response (ECLIDAR).

The proposed system uses the Clustered[2] mobile ad hoc network organization, the efficient node which has maximum processing capability selected as cluster head and the manager node is deployed for the control of the clustered nodes. The MANET mining[4]algorithm is used to detect frequent item sets which is the repeated nodes of divergent paths and based on it association rule is derived .The proposed IDS architecture is shown in fig. 1 and their module is described below .In the syndicate module, association algorithm[5][4] is used for collecting data's from each layers based on it the audit data traces is obtained, with behavioral information consisting of layer specific information.

Anomaly detection uses clustering algorithm for intrusion detection which detects both known and unknown attacks, it consists of training and testing phase, in training phase based on the traces the initial training profile is generated, they exhibit the usual behavior features of the nodes in the mobile ad hoc network. The testing module consists of learning and novelty phase. If any node deviate beyond a threshold interval then the node prone to attack, for the known attacks the intrusion response action is provided ,when the attack is not known then the novelty phase is invoked which updates the attack trace and further response is provided.

Algorithm1 illustrates the overview of ECLIDAR which exhibits the overview of the steps involved in intrusion detection and its respective response. Algorithm 2 illustrates the Apriori[5] which collects the audit data traces from multiple layers using the traffic in the network. Algorithm 3 provides the anomaly method which uses clustering algorithm for detection of known and unknown attacks, based on the severity of the attack the intrusion response action is provided.

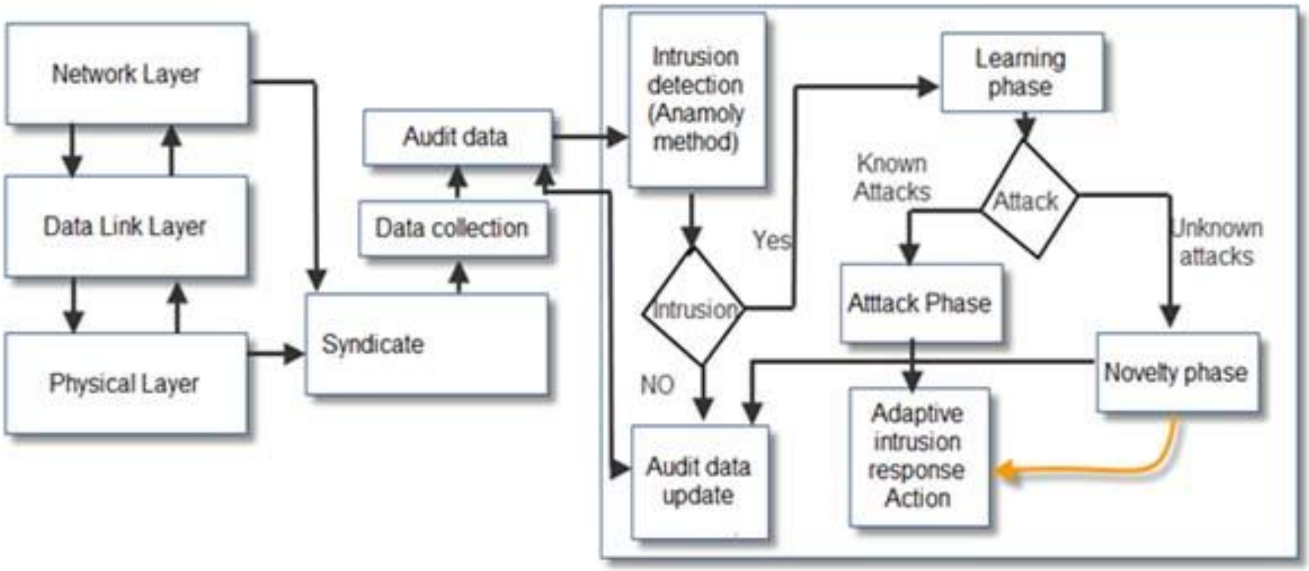


Fig 1: Enhanced cross layer intrusion detection and adaptive response mechanism architecture

Algorithm 1:Procedure ECLIDAR

```
Step1: BEGIN
Step2: Apply Apriori Algorithm based on manet mining
         Set audit data
Step3: Invoke clustering Algorithm for intrusion detection
         if feature set is built
         then compare ,detection pattern > threshold
         set node as malicious
Step 5: Apply adaptive intrusion response action
Step 6: END
```

Algorithm 2: Apriori

```
Step :1
        IN = frequent item sets 1
        N is the permission number
        while (IN-1 != null set) do begin
        CN =New contender of size N
        For all traffic  E Є T do begin
        Increment the count of all contenders in CN that are contained in E.
        k := k+1;
Step 2:
        contender  generation
Insert into CN
        M.itemN-1 < N.itemN-1 ensures that no duplicates
        In Pare step, remove unlikely set
        if s is not in IN-1
        Delete c from CN
Step 3:
        Generate rules for every frequent item set i
        For every subset v, we output a rule set of the form v⇒ (i-v)
        All subsets of v are considered to generate rules with multiple consequents
```

Algorithm 3:Procedure anomaly detection and response

```
Train the audit data
Let sample be pi
cluster value is zero, where cluster=c
If c=0
then Make new cluster with respect to centroid from pi
C=C+1
else
find nearer cluster  to pi
If distance to nearest cluster Distance(pi )<w
add and update centroid
else
make new cluster of the centroid
Cluster<threshold  then
set  as anomalous
#unknown attack
If  the rule trace is empty
Store Detected Rule Trace = Rule Trace
Else If (Rule Trace == Detected Rule Trace)
New attack rule trace
structure the rule for New attack
Append New attack Rule
Else
Label  as normal
```

V.SIMULATION RESULTS

The simulation results of the proposed system is discussed in this section where the parameters such as end to end delay, packet delivery ratio, Energy consumption is considered for evaluating the performance of the proposed system. End to end delay and energy consumption should be affordable in the network ,where as the packet delivery ratio should b higher for the reliable network.

We use network simulator version 2 has simulation environment, where the simulation parameters assigned .The number of nodes considered as 100,AODV as routing protocol, simulation time considered to be 250 s, MAC type to be 802.11,The traffic source considered to be constant bit rate once the parameters are assigned thee simulation is derived for the qos metrics.

Table II- Simulation Parameter

Parameter	**value**
Number Of nodes	100
MAC TYPE	802.11
Traffic Source	CBR
Antenna model	Omni Antenna
Simulation time	250 m/s
Routing Protocol	AODV

In Figure 2 the energy consumption graph is simulated which compares the number of nodes with the energy the proposed system only absorbs sixty percentage of energy since the energy constraints which is essential for mobile ad hoc network for further transmission is conserved.

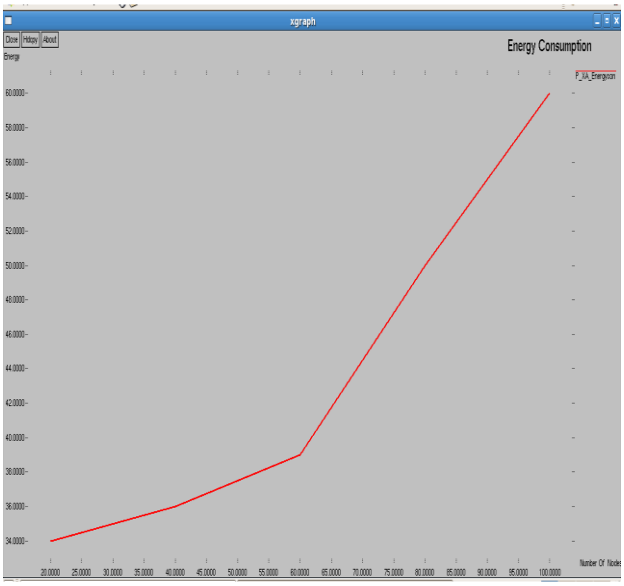


Fig 2:Energy Consumption

In Figure 3 the end to end delay graph is simulated which compares the number of nodes with amount of delay . End-to-End Delay is the average time interval between the generation of a packet in a source node and the successfully delivery of the packet at the destination node .The lower the end-to-end delay the better the proposed performance. The end to end delay is calculated as,

End to End Delay = n_to_n_delay/count;

(where n_to_n_delay = n_to_n_delay + delay[i];)

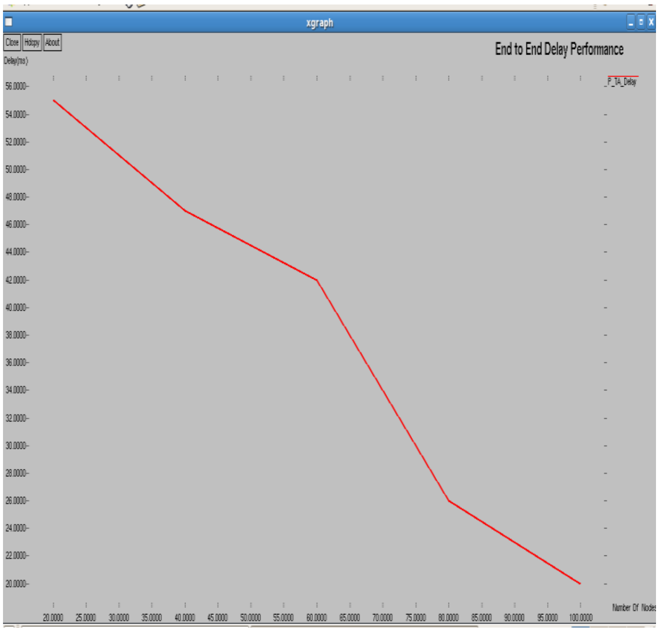


Fig 3:End to End Delay

In Figure 4 the delivery ratio is simulated, packet Delivery ratio is the number of data packets successfully delivered to the destination nodes .The graph exhibits the better delivery ratio as the number of node increases. The delivery ratio is calculated by,

Packet Delivery Ratio = 100*Data Recieved/Data Sent

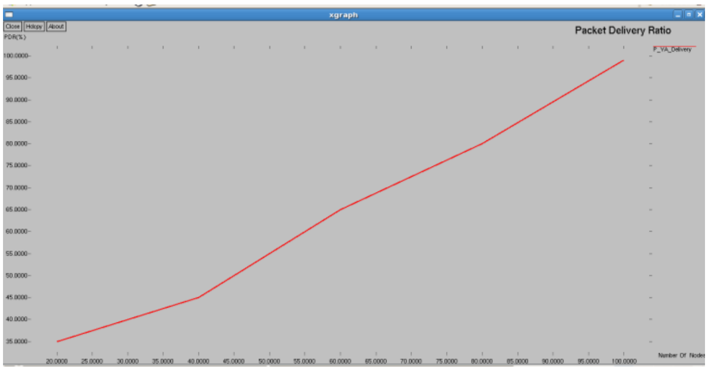
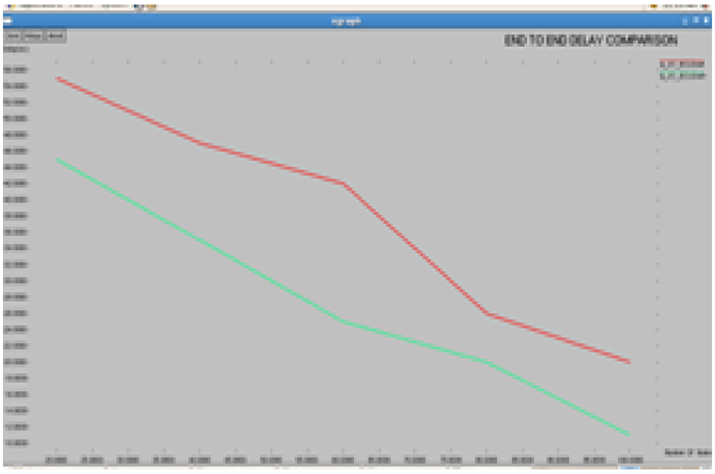


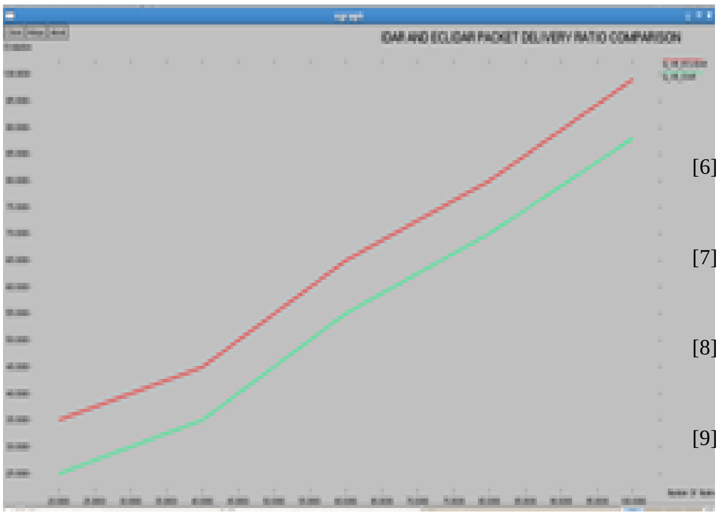
Fig 4:Packet Delivery Ratio

The existing algorithm [26] approaches the single layer method for the detection of attacks only in the network layer, it uses both statistical anomaly and knowledge based intrusion detection methods for the attack identification which increases the end to end delay and energy consumption and reduced packet delivery ratio, in order to overcome those demerits the proposed approach is deployed. The analysis graph is shown below for the comparison between the existing intrusion detection adaptive response and proposed enhanced cross layer intrusion detection and adaptive response algorithm , where the existing system addresses only single layer attack whereas the proposed algorithm addresses the attacks in various layer of the protocol stack.

Fig 5.a depicts the end to end delay for the [26]estimated to be 136.083ms ,whereas our proposed algorithm delay is estimated to be 190.437m. Fig 5.b depicts the packet delivery ratio for the [26]calculated to be 85.71%,whereas the proposed algorithm have the delivery ratio of 99.94%,with respect to the analysis the proposed algorithm improves the packet delivery and end to end delay is affordable since it detects the multiple layer attacks.



(a)



(b)

Fig 5:comparison of IDAR and ECLIDAR (a)end to end delay (b)Packet delivery ratio

VI. Conclusion

Mobile Ad Hoc Network prone to many security issues due to its dynamic nature hence providing security becomes the risky task. Many single layer intrusion detection algorithm had been proposed which doesn't provide any accuracy in the detection of malicious nodes ,in order to overcome those demerits cross layer intrusion detection mechanism is proposed where the data traces is collected from various layers using the association, further the clustering algorithm is used for the intrusion detection which detects both known and unknown attacks, adaptive response action is provided based on the severity of the attack, which improves the packet delivery ratio and reduction in end to end delay, energy consumption.

REFERENCES

[1] M. Abolhasan, T. Wysocki, and E. Dutkiewicz,2004, ―A review of routing protocols for mobile ad hoc networks,‖ Elsevier Journal of Ad Hoc Networks, 1–22.

[2] Mandala, S., Ngadi, M.A., and Abdullah, A.H,2007,: 'A Survey on Manet Intrusion Detection', International Journal of Computer and Science and Security, 2, (1), pp. 1-11

[3] H.C. Jang, Y.N. Lien, T.C. Tsai, Rescue information system for earthquake disasters based on manet emergency communication platform, in: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM, 2009, pp. 623–627

[4] A. Vasiliou, A.A. Economides, MANETs for environmental monitoring, 2006,in: IEEE International Telecommunications Symposium, , pp. 813–818.

[5] B.C. Seet, G. Liu, B.S. Lee, C.H. Foh, K.J. Wong, K.K. Lee, A-STAR: a mobile ad hoc routing strategy for metropolis vehicular communications, in: NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, Springer, 2004, pp. 989–999.

[6] Zhang, Y., & Lee, W. 2000. **"**Intrusion detection in wireless ad hoc networks‖. In Proceeding of 6th ACM MOBICOM.

[7] Huawei Li Das, A.Jianying Zhou, 2005,Theoretical Basis for Intrusion Detection, IEEE Proc, Information Assurance and Security.

[8] B. Sun, ―Intrusion detection in mobile ad hoc networks,2004, Ph.D. dissertation, Texas A&M Univ., College Station, TX.

[9] Amardeep Singh, and Gurjeet Singh, "Security in Multi-hop Wireless Networks", IJCST Vol. , Issue 2, June 2011

[10] Manikandan, K. P., and Satyaprasad2 K. Rajasekhararao. "A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks

[11] Shruti Thacker ,Enhancing Routing With Cross Layer Optimization in MANETs, (IJCSIT, Vol. 5 (3) , 2014, 3708-3710

[12] Parker, J. ; Patwardhan, A. ; Joshi, A.Cross-layer Analysis for Detecting Wireless Misbehavior**,** Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE (Volume:1)

[13] Nish Dang & Poona Mitta, 2012 Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology.

[14] Sen, S., & Clark, J.A., 2008, Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Springer.

[15] Garuba, M., Liu, C. & Fraites, D., 2008, Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE.

[16] I. Meenatchi, K. Palanivel, " Intrusion Detection System in MANETS: A Survey," International Journal of Recent Development in Engineering and Technology, Volume 3, Issue 4, October 2014

[17] Yu Liu, Yang Li, Hong Man" 2006, A distributed cross-layer intrusion detection system for *ad hoc* networks",springer

[18] John Felix Charles Joseph a,*, Amitabha Das b, Bu-Sung Le Boon-Chong Seet c,CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS, Elsevier, Computer Networks 54 (2010) 1126–1141

[19] K.Suresh Babu , K.Chandra Sekharaiah "CLDASR: Cross Layer Based Detection and Authentication in Secure Routing in MANET" IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.4, No2, April 2014

[20] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi, Seung-Jo Han,"A Novel Cross Layer Intrusion Detection System in MANET", 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[21] Yu LIU*, Yang LI*, Hong MAN*,"Distributed cross-layer intrusion detection system for ad hoc networks",springer, Volume 61, Issue 3-4 pp 357-378

[22] Jim Parker, Anand Patwardhan ,Anupam Joshi,"Cross-layer Analysis for Detecting Wireless Misbehavior", Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd ,IEEE volume1.

[23] J. Godwin Ponsam1, Dr. R.Srinivasan2 ,"A Survey on MANET Security Challenges, Attacks and its Countermeasures" ,IJETTCS 2014

[24] John Felix Charles Joseph a,*, Amitabha Das b, Bu-Sung Le Boon-Chong Seet c,CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS, Elsevier, Computer Networks 54 (2010) 1126–1141

[25] Jim Parker, Anand Patwardhan ,Anupam Joshi,"Cross-layer Analysis for Detecting Wireless Misbehavior", Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd ,IEEE volume1.

[26] A. Nadeem, M. Howarth, 2014, An intrusion detection & adaptive response mechanism for MANETs, Elsevier Journal of Ad Hoc Networks, 368-380