Cross Layer Intrusion Detection In MANET'S:A Survey

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

Abstract— **Mobile Ad Hoc Network or MANET is an infrastructure less network which undergoes various security attacks due to the challenges in mobile ad hoc networks which endures dynamic topology, mobility of nodes, congestion. Conventional Single layer attack detection mechanism lack the accurate detection of attacks. In order to overcome those vulnerabilities cross layer intrusion detection methodology is adapted. In this paper, we surveyed various cross layer intrusion detection algorithm and those algorithms compared with respect to various parameters in the network. Finally, conclusion and the future work is suggested**

Index Terms— **Attacks, Cross Layer, Intrusion, MANET**

I. INTRODUCTION

A mobile ad hoc network (MANETs) is diverse from infrastructure network and lack of firm base stations. MANET altogether utilized in various emergency applications, Mobile Ad hoc Networks present most significant merits and have been incorporated in a varied range of applications such as disaster assistance [1] ,monitoring of environment [2] and vehicular networks [3]. MANETs 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.

MANET comprises 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, so it is prone to variety of attacks such as routing, packet modifications, eavesdropping and protecting a MANET under such environments is difficult [4] 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 [4]. Mobile ad hoc network uses various routing protocols like proactive and reactive protocols. MANETs routing protocols classified as either proactive or reactive. Proactive routing protocols were FSR [21], OSLR [21] whereas reactive protocols includes AODV [21], DSR [21], 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 [4]

An Intrusion Detection System (IDS) [5] 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, 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 [6] [7]. 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 [6].

This paper discusses the survey of the Previous cross layer intrusion detection algorithms and their approach towards the malicious attacks caused due to its infrastructure less and dynamic nature. In order to defend those attacks various cross intrusion detection system algorithms have been deployed in various mobile ad hoc nodes to overwhelm the malicious attacks. The IDS algorithm tends to detect the malicious attack and isolate the nodes and also the comparison and suggested work of those algorithm presented

The rest of the paper is ordered as, section 2 depicts the background of mobile ad hoc network, the intrusion detection system, cross layer attacks; section 3 comprises the survey of previous work which incorporates cross layer IDS in mobile ad hoc networks and comparison of algorithm; and finally section 4 comprises the conclusion and future work.

II. BACKGROUND

This section presents the basic information about mobile ad hoc networks, Routing Protocols, Types of Attacks and IDS that are required for the proposed work.

A.MANET

Mobile ad hoc network is a self- assembling system of mobile nodes that communicate with each other through wireless links without fixed infrastructure. 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 [4].

B. IDS

The IDS 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 [4]. 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 [4].

C. Cross Layer Attack

ISSN: 2278 – 1323

Similar to other wireless network, mobile ad hoc network tends to passive and active attacks, Table –I depicts the various attack in different layer.

Table I- Cross layer Attacks [17]

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

Physical Layer Attacks

Eavesdropping - The intruder tries to overhears the hidden information during the transmission in the network.

Jamming - Jamming attack is deployed which interrupts the communication due to the jamming of the signals.

Data Link Attacks

DOS - DOS is the denial of service attack which prohibit the authorized access of resources to the permissible users.

Malicious Behavior Nodes - The significant function of malicious node is to disturb the typical operation of the routing protocol this attacks vastly takes place due to the transmission between the neighbor node

Network Layer Attacks

Black hole attack- Black hole attack is the one which provokes the other node by advertising that it has shortest path to the destination if this reply reaches before the actual reply ,the fake route is formed inclusive of the malicious node, hence the malicious node will cause the denial of service , man in the middle attack.

Gray Hole attack - Gray hole attack is similar to the black hole attack but it drops the packet from only selective nodes hence it is hard to find those attacks.

Wormhole Attack - Wormhole Attack mostly occur due to the coordination between two malicious node they tunnel the packet between them so it makes the control of the network

Rushing Attack - The malicious node rapidly sends the route request to target nodes hence the target node tends to omit the legal nodes route request [20]

Sleep Deprivation - Sleep Deprivation attack continuously uses the legitimate nodes resource which leads the drained battery power.

Transport layer attack

Session Hijacking - In this attack the session is hijacked by the attacker, here attacker launches the variety of attacks by utilizing the internet protocol spoofs number

D. Cross Layer Based Methodology

In order to overwhelm the above introduced attacks it issues a cross layer based methodology which exceeds the inclusive performance of the network which recognize the multi layered attacks . More harmful attacks like packet dropping, routing disruption, jamming attacks or other forms of Denial-of-Service (DOS) at any of the networking layers can severely disrupt MANET communications[19]. The basic purpose of cross layer design is to use multi layer parameters from OSI stack to increase the efficiency and performance of MANET[8][9].

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[10].

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[11]. A Cross Layered Architecture for the Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks is also proposed [18]

III. OVERVIEW OF VARIOUS CROSS LAYER ALGORITHM

Various Cross layer Intrusion detection algorithm have been discussed.

A. Cross Layer Intrusion Algorithm

Algorithm 1: layer based adaptive real-time routing attack detection system for MANET'S [12]

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 .The above process is done by the following phases, [12]

In data collection phase the CARRADS responsible for monitoring neighborhood nodes and they collects information from protocol layers based on parameters such as traffic, dynamic topology and they store the routing behavior. Hybrid method is used where standard and malicious behavior used for training audit data's. Next module is behavior identification module where monitoring, identifying and classifying a new pattern observed in the neighborhood is addressed.

Third module is incorporated to lessen the computational overhead this module aims to reduce the dataset size, without affecting its information content. Association comprises the cross layer properties to make a diminished set of derived features. Filtering is a process used for removal of redundant and useless information content. The final module is the learning phase where the valid decision is applied based on the patterns [12].

Merits and Demerits: The Computational overhead is reduced in the real time intrusion detection in mobile ad hoc network The Energy consumption would be more due to the

ISSN: 2278 – 1323

more steps involved in the detection of malicious node in the network

Algorithm 2: Cross Layer Based Detection and Authentication in Secure Routing in MANET [13]

Initially the path is established between the source and destination which is checked by using the authentication method 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 [13] .The next step is the detection method where the neighbor forward rate is calculated and the compared with the threshold value of each node ,if the threshold value greater than neighbor node forward count then the node is prone to the black hole or grey hole attack[13].

Merits and Demerits: It reduces the packet drop due to the malicious activity of node and also reduces the link failure in the network. The Authentication method is used hence only known attacks is addressed.

Algorithm 3: A Novel Cross Layer Intrusion Detection System in MANET[15]

Initially in the association module the training data's are obtained from association regulations, which is converted into rule set. The sets consists of routing control packet and data packet, this set is further reduced by associating the characteristics from different layers hence the overhead of the pursuing phase reduced. Traffic characteristics is collected using the association algorithms which is followed by the clustering algorithm[14][15].

The next module is intrusion detection in which local data collection is employed where attack traces from physical, MAC and network layers is collected through the association module. It is followed by the detection module where anomaly detection technique compares the current test profile with normal profiles if there is any deviation and higher threshold value then the network is under which initiates alert. If the confidence level is low and the evidence not clear to make decisions then the Cooperative Detection is employed to gather data's from other nodes The last module is the alert method it is provided information from the previous steps and finally detect the intrusion in the system.[14][15].

Merits and Demerits: It reduced traffic in the network. The Lack of resilient and smart intrusion detection system.

Algorithm 4 :A distributed cross-layer intrusion detection system for* ad hoc *networks [16]

Node related distributed method is used since ad hoc networks prone to absence of central monitoring methodology. The primary step in this algorithm is to collect the audit data's based on the featured set from the networks involved. In the profile module uses two subsystem ,first is the pre processor which converts audit data into profile based process, the next step in the sub system is profiler where the associate patterns is proposed ,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. Based on the above module in the decision phase global and local alert is triggered [16].

Merits and Demerits: The Unknown attacks could be detected due to the novel collaboration approach. It detects attacks within the radio range transmission hence one hop perimeter is detected

Algorithm 5: Cross-layer Analysis for Detecting Wireless Misbehavior[19]

Intrusion Detection System mostly experience false positives due to presence of congestion, dynamism of the nodes and interference in ad hoc networks, hence proximity and congestion can be deployed. In this algorithm intrusion detection method used which uses the heuristics method to differentiate intrusion by deploying the detected behavior from different layers of the protocol. This method detects more vulnerable attacks that target the multiple layers in the network it engages cross layer communication depend on surveillance at various networking layers to deuce the occurrence of false positives in the network[19]

Merits and Demerits: Reduces the false positive in the attack identification due to use of novel methodology. Sometimes intruder utilizes many vulnerabilities in the different layers attack detection method so the intruder may not suit any one of the observed attack signatures hence left unrecognized[19]

B. Comparative Analysis of Algorithms

The Comparative analysis of previous proposed algorithms [12] [13] [14] [15] [16][17] have been described in Table 2, comprises the algorithm proposed, parameters used for the attack detection and response mechanism.

Many techniques is used to detect the malicious attack in mobile ad hoc network, in the survey work it uses anomaly, used to detect the attack, Parameters such as threshold, security, Overhead and Routing Protocols were considered for comparative analysis of algorithms. The above parameters were considered in order to co relate the existing cross layer intrusion detection algorithms and their performance in the network.

- Overhead is used hence the range is set if the calculated value passes it then the node is mapped as malicious [4]
- Security is the prior concern in mobile ad hoc networks due to its dynamic characteristics hence the algorithms have been proposed to ensure the secure transmission of packets during routing,
- Overhead includes the usage of memory space, bandwidth, amount of resource utilized, so the overhead should be taken into primary consideration in order to make the network reliable in packet transmission,
- Routing protocols also taken into consideration for comparing the surveyed algorithm in order to gain significant features of them[4]

Table II- Comparison Of Algorithm

ISSN: 2278 – 1323

Existing Algorithm	Comparison Slots			
	Technique used	**Routing protocol**	**Overhead**	**Qos**
Cross layer based adaptive real-time routing attack detection system for MANETS[12]	SVM	AODV	Yes	No
Cross Layer Based Detection and Authentication in Secure Routing in MANET[13]	Threshold	AODV	Yes	No
A Novel Cross Layer Intrusion Detection System in MANET[15]	Anomaly	AODV	Yes	No
A distributed cross-layer intrusion detection system for ad hoc networks[16]	Anomaly	AODV	Yes	No
Cross-layer Analysis for Detecting Wireless Misbehavior[19]	Threshold	AODV	Yes	No

The Existing algorithm lacks the response mechanism ,if the node is termed as malicious it is difficult to further isolate from the network since many routing paths involved in the routing. And also the existing algorithms prone to increase in the overhead ,packet delivery ratio and end to end delay which drastically affects network performance and also the quality of service becomes more challenging.

In order to overcome those demerits the response action should be included in the proposed algorithm ,the adaptive response action should be provided for the nodes which is classified as intruder in the network ,comparing to the previous algorithm our proposed methodology improves the further packet delivery ratio, end to end delay and energy consumption, hence there will be increased quality of service in the network .

IV CONCLUSION

Mobile Ad Hoc Network prone to many security issues due to dynamic nature of mobile ad hoc networks ,providing security to mobile ad hoc network tends to be the risky task. Many single layer intrusion detection algorithm had been proposed it doesn't provide any accuracy in the detection of malicious nodes ,in order to overcome those demerits various cross layer intrusion detection mechanism is discussed.

Initially the concept of mobile ad hoc networks and its challenge discussed ,Further Intrusion detection system, Cross layer concepts depicted. We then survey the various cross layer intrusion detection methodology and the comparison work is described. In future the adaptive response action should be provided for the nodes which is classified as intruder in the network which improves the further packet delivery ratio, end to end delay and energy consumption.

REFERENCES

[1] 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

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

[3] 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.

[4] 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

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

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

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

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

[9] 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

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

[11] 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)

ISSN: 2278 – 1323

[12] 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

[13] 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

[14] V. Anjana Devi1 and R. S. Bhuvaneswaran2,adaptive association rule mining based cross layer intrusion detection system for manet, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[15] 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

[16] 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

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

[18] K.P.Manikandan,1R.Satyaprasad2 K.Rajasekhararao3,"A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks",IJCSIT, 2011

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

[20] S.marti. T.Giuli, K. Lai, and M.Baker, Mitigating routing misbehavior in mobile ad-hoc networks. in proc. Of MOBICOM, 2000

[21] Ms. Amruta Kodole1 , Prof. P. M. Agarkar2 ,A survey of routing protocols in mobile ad hoc networks, Multidisciplinary Journal of Research in Engineering and Technology, Volume 2, Issue 1.

ISSN: 2278 – 1323