IJCTA, 9(10), 2016, pp. 4885-4890

Cross–Layer IDS for Grayhole Attack in Wireless Mesh Networks

***Prabhat Ranjan *Hemraj Saini**

Abstract : Wireless Mesh Networks is one of the promising technology in giving wireless internet connectivity. It has mesh routers and mesh clients, in which mesh routers have less movement and is the base of WMN. They provide network access for both mesh and conventional clients. Since it allows faster, easy and cheaper network deployment hence they are becoming a popular choice. In WMN, security is the main concern. Due to its open medium, dynamic topology and lack of physical security they are vulnerable to various kinds of attacks and intrusions at different layers. Security in WMN is in starting stage as a little focus has been given till now and so lead to vulnerability to various types of attacks. DoS attacks can compromise the availability of WMN as such attacks would hinder giving service to more than one node. Grayhole is one kind of routing disturbing attack and can bring great damage to the network. Intrusion is an unwanted work used to hinder the working of network. Wireless networks are very much vulnerable to different kinds of attacks at different layers. Intrusion detection is a passive defense strategy to inform administrator about attacks on the network. In this paper, we have worked on Cross layer Intrusion Detection System (IDS) which has the capability to accommodate the integrated property of routing protocols with linked information in WMN to detect attacks on multiple layers.

Keyword : Wireless Mesh Networks, Grayhole Attack, Intrusion Detection System and Cross Layer.

1. INTRODUCTION

WMN [1] are having dynamically self organization and self-configuration systems. They are easy to install, cheap and self reliable. It contains Clients and Routers which forwards the packets on the behalf of other nodes to improve communication range and bandwidth. The principle will be to hop data among nodes till it reaches the destination. Due to WMNs open and dynamic topology, it is vulnerable to several types of attacks at different layers. WMNs [2] are vulnerable at routing layer then at Physical and MAC layer. Routing layer consists of two types of attacks *i.e*. data plane and control plane attacks. Control plane attacks disturb the route discovery and maintenance phase of the routing protocols and data plane attack affects the routing by dropping packets. Grayhole attack is one of the data plane attack in routing layer which drops packets in active route. Data plane attacks are also known as DoS attacks as they result in substantial service interruption.

Intrusion Detection System (IDS) [10] act as a second line of defence in contradiction of these attacks. It is the process of network monitoring and checks the security violations. Further, it consists of two types *i.e*. cross layer and single layer IDS. Single layer is created on the information from a single layer whereas the cross layer uses two or more layers for detection. We used multi-layered approach for adversary node detection on AODV protocol with factors like hop count, error rate and packet drop ratio.

2. GRAYHOLE ATTACK

Grayhole attack is an active type attack [8], [9], [18]. Uses of the route discovery process where malicious node makes itself as the best node to the destination. Dynamic routing protocols like AODV/DSR are most

* Department of Computer Science & Engineering Jaypee University of Information Technology, Waknaghat-173234 prabhatrongta@gmail.com, hemraj1977@yahoo.co.in

susceptible to this attack. In this attack, on receiving RREQ message, the adversary node immediately replies with the false route reply message. The false route reply message is to tell the other nodes that the destination node is on the next hop to this malicious node and the malicious node has the best route to that destination node. In this way all the neighbouring nodes makes the next hop as the destination and when this malicious node receives the data packets it may simply drop some of the packets.

In the given figure 1, with S as the source and D as the destination, Grayhole node A sends false RREP message to the network and makes itself as the finest route to the destination and with time A will keep dropping some of the packets coming from S.

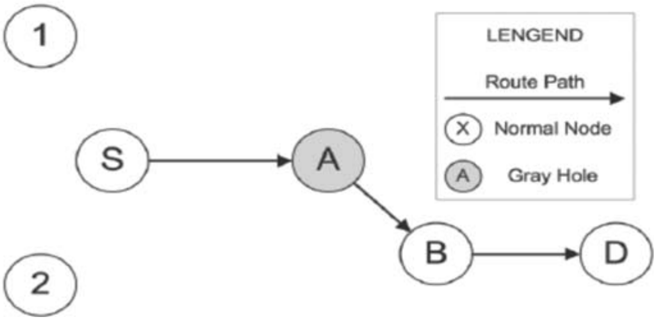

Fig. 1. Grayhole attack

3. RELATED WORK

Grayhole attack will bring damage to the network. We found some of the detection systems on WMN. Sun et al [8] gave an approach for attack detection. They used a neighbourhood technique to perceive the attacker and used a recovery of route protocol to make an improved path to the real destination. They gave a neighbouring node set which is within the range of node. Two kinds of control packets are sent to distribute set of neighbours among the various nodes. One drawback of this scheme is that public key infrastructure is needed, unless it will be prone to attack. P.Yi et al. [9] made a scheme on path, in which a node does not lookout every node in the network but watches the neighbouring hop in the current path. Gao et al. [12], for detecting adversary nodes used a signature algorithm to trace the packets [13], [17] dropped by those nodes. The advantages of this algorithm are reliability, wide application, good security and the overhead of bandwidth is low. Shila et al. [14] came up with the defending grayhole attack in WMN consists of two phases. i) Counter threshold based which uses the threshold to detect threats. ii) Another is query based uses feedback from the neighbouring nodes to detect the location of the attacker. Ping Y YI et al. [15] and [16] came up with a detection approach on distributed intrusion. PingYI [9] made a scheme based on path, in which a node is not watching every node in the neighbour but observing next hop of the current path using a threshold value. It overhears the action of next hop. This protects the resources of the perceiving node by not sending extra control packets. In MAC layer, a report on collision rate is made to develop dynamic detecting threshold. The experimental research shows that cross layer based detection methods are better and active than single layer techniques. Some of the approaches for detection are in the table 1 below.

Table 1. Various Detection Methods.

S.No	*Detecting Method*	*Key Idea*
1.	Neighbourhood-based method[8]	Every node watches its neighbours to detect any malicious node.
2.	Path based scheme[9]	Node watches the next hop in the present path and compares with the Threshold value
3.	Signature based algorithm[12]	In it, source route nodes are checked and then malicious nodes are located.
4.	Distributed intrusion[15]	Cluster techniques are used where a node monitors the cluster for a time period.

A. Intrusion Detection System for WMN

An intrusion can be any of the unwanted activity in the form of active or passive attacks, which attacker uses to create unwanted situation and bad results for user's confidentiality, integrity of network or availability of network resources [7]. Intrusion is simply an action that compromises data integrity, confidentiality of user, integrity of network or network resources availability. A system that is used to detect such malicious actions in network or node is called Intrusion Detection System or IDS. By implementing the IDS, security of wireless networks can be increased to certain limit. Two types of intrusion detection systems exist *i.e*. Pattern based systems which identifies all the unknown attacks and anomaly based mechanism have astuteness to identify and respond to new intrusions which are not known [19]. IDS are further classified into Stand-alone IDS, Cooperative and Distributive IDS and Hierarchical IDS. Stand-alone IDS operates independently on each node to monitor the internal events that are verified in system logs. In Distributive and Cooperative IDS, each node contribute in detection and response of intrusion and in hierarchical IDS, child nodes are monitored by cluster-heads and responds on intrusion detection.

4. INTRUSION DETECTION SYSTEM USING CROSS-LAYER

Proposed mechanism for the recognition of Grayhole attack in WMNs is as below. The proposed technique is a cross-layer design as it practices behavioural information from two different layers for the detection. The parameters to be used are PDR (packet drop ratio) from MAC layer, delay and hop count from routing layer. PDR is the ratio of number of dropped packets to number of packets sent is given in table 2 below.

Table 2. Algorithm Parameters

Tp	Practical time taken to deliver a packet from starting to final node
Tt	Theoretical time taken to travel a packet from starting to final node
Hc	Hops taken in route
D	Time taken at each node to transfer the request
pdr	Packet drop ratio
Pt	Time interval for a period

Algorithm : Intrusion detection system for Grayhole attack using cross-layer

```
1.  Find the time (t1) at which packet starts from source node S.
2.  The node S starts the process and sends packet to intermediate nodes through AODV protocol route
    until reaches it reaches destination node D.
3.  Find time (t2) at which node D receives packet.
4.  Calculate Tp using e.q. Tp = T2–T1.
5.  Get number of hops in route Hc.
6.  Calculate time Tt using :Tt = Hc*d.
7.  if Tp > Tt then
8.  Alert "Grayhole attack is suspected in given route "
9.  For each node in the route do
10. if pdr > 0.60
11. Alert "The node is adversary"
12. end if
13. end for
14. if no node is detected then
15. goto Step 9 and repeat for every pt.
```

```
end if
Down the current path and take another path
else
Alert "Grayhole attack is not suspected in the given route"
end if
```

5. SIMULATON AND RESULTS

The simulation is done using network simulator 2.

Table 3. Parameters used in simulation

Property	***Value***
No. of Nodes	24
Time of simulation	14 seconds
Protocol used for routing	AODV
Area of coverage	800 m *800 m

The table 2 shows the measuring metrics used in simulation. Simulation tests were run having hostile node dropping packets to design a graph of throughput versus time. Throughput in this is defined as bits transmitted in per unit of time. Comparison of the scenarios using single layer and cross-layer is plotted with throughput along X axis and the time taken along Y axis as depicted in figure 2. The figure shows that with the increase in time throughput increases more in case of cross layers as compared to single layer.

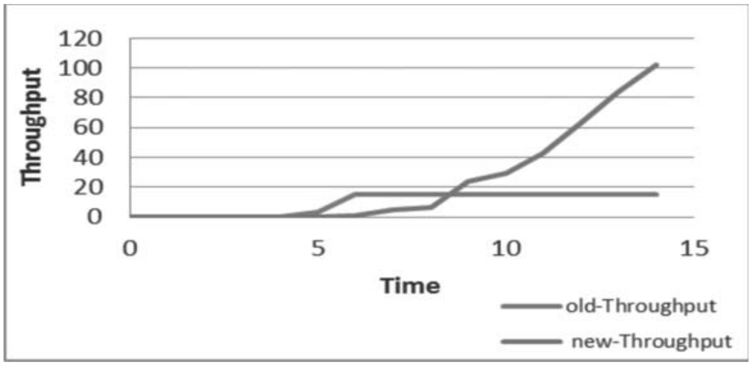

Fig. 2. Throughput *vs* Time

Similarly, figure 3 shows the packets dropped along Y axis and the time taken along X axis. The figure shows that the packet drop ratio increases along with the increase in time; packets dropped increases slowly in case of cross layers as compared to single layer where packets dropped are high with constant value.

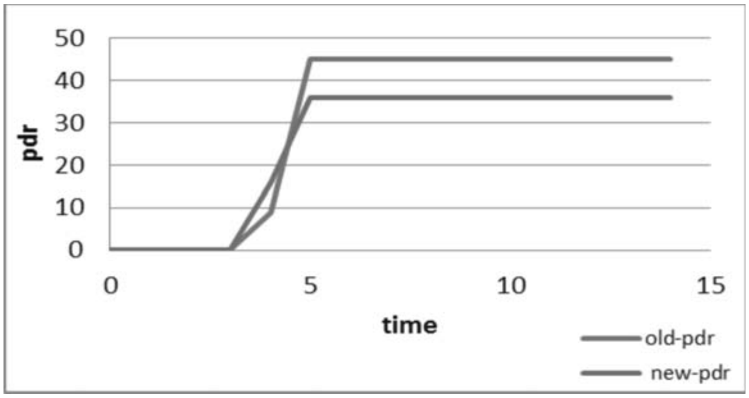

Fig. 3. Packet drop ratio vs Time

A delay is defined as the time taken by a bit to travel across a network from one node to another. Figure 4 is plotted with delay along Y axis and the time taken along X axis. The figure shows that with the increase in time, delay is more for single layer as compared to cross layer in the network.

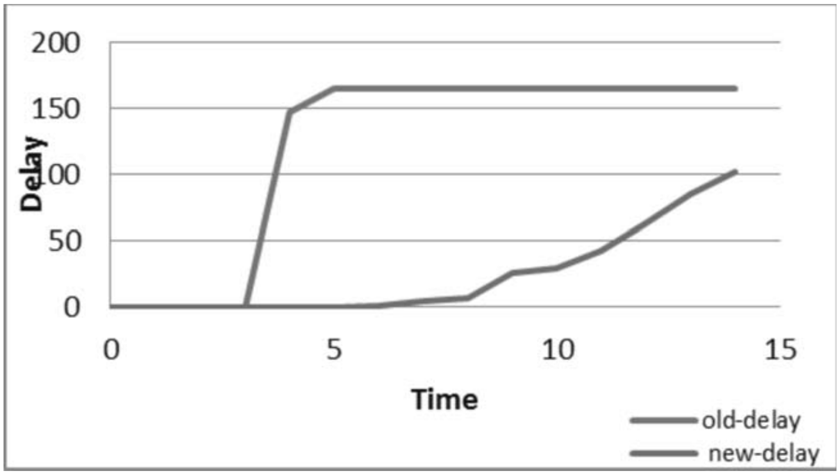

Fig. 4. Delay Vs Time

6. CONCLUSION

In this paper, we gave a cross-layer intrusion detection system (CLIDS) for Grayhole attack in WMN. Cross layer taking parameters from both the MAC layer and the Routing layer. The solution is simulated using Network Simulator 2. The results shows there is an increase in throughput and the improvement in packet drop ratio. With the use of cross layer designs, researchers are implementing smart communication systems by stressing on the optimization of network performance with the help of different layers. At various layers information is being shared and actions are coordinated to jointly optimize the performance of the network. But still more research need to be carried by utilization of more layers for better intrusion detection and network performance.

7. REFERENCES

1. I.F.Akyildz, X. Wang,W.Wang ,”Wireless mesh networks:a survey” ,ELSEVIER 2005,pp. 444-448.
2. F.S.Al-Anzi and S.Khan,”Wireless Mesh Network Cross-layer Intrusion Detection”,in Journal of Computer Science 2014,pp.2366-2368.
3. M.D.Nikose,”A review of Cross layer design”,IJETET 2013, Vol.2,No.1,page-8.
4. S.Seth, A. Gankotiya,”Denial of Service attacks and Detection Methods in Wireless Mesh Networks “, IEEE 2010,pp.238-239
5. X.Wang, J. S. Wong, F. Stanley and S.Basu,”Cross-layer Based Anomaly Detection in Wireless Mesh Networks” , in Ninth Annual International Symposium on Applications and the Internet, IEEE 2009,page-10
6. M.Verma,N. C. Barwar,”A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole attacks in MANET” ,in International Journal of Computer Science and IT 2014, Vol.5,No.6,pp.7228-7230
7. S.Khan, K.K.Loo and Z.U.Din ,”Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh”,published in International Arab Journal of IT,Vol.7,No.4,2010,pp-436-437.
8. B. Sun, Y.Guan,J.Chen, Pooch U. W.,” Detecting Black-hole Attack in Mobile Ad Hoc Networks”,in Fifth European Personal Mobile Communications Conference, 2003.
9. P. YI, T.ZHU, N.LIU , Y. WU,”Cross-Layer detection for Blackhole Attack in Wireless Network”, Jianhua LI Journal of Computational Information System 2012,Vol.8,No.10,page-4103
10. K. G.Reddy, P. S. Thilagam,B.N. Rao,”Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks”,ACM 2012,page-396.
11. I. Askoxylakis, B. Bencsath, L.Buttyan, L. Dora, V.Siris and A.Traganitis Cross-layer security and resilience in wireless mesh networks, ,2013,pp. 3-6

12. G.Xiaopeng, C.Wei, “A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks”in , IFIP International Conference on Network and Parallel Computing Workshops, 2007

13. D. Boneh, C. Gentry, B. Lynn, H. Shacham,” Aggregate and Verably Encrypted Signatures from Bilinear Maps”, Advances in Cryptology-EUROCRYPT’03: LNCS 2656. Berlin: Springer Veralg,2003,page-2.

14. Shila, D. M., Anjali, T., “Defending selective forwarding attacks in WMNs”, IEEE International Conference on Electro/ Information Technology,2008,pp.96-101.

15. P.Yi, X.Jiang, Y. Wu,” Distributed Intrusion Detection for mobile ad hoc networks”,Journal of Systems Engineering and Electronics, Vol. 19, issue 4,2008.

16. P.Yi, Y. Wu, N.Liu, Z. Wang, “Intrusion Detection for Wireless Mesh Networks using Finite State Machine”,in China Communications 2010

17. S.Ravichandran, “Secured identity based approach with privacy preservation for wireless mesh networks”,in International Journal of Communication and Networking System.,Vol. 1, issue 2, 2012.

18. S.Navitha,T.Velmurugan, “A survey on the Simulation Models and Results of Routing Protocols in Mobile Ad-hoc Networks”,in International Journal of Communication and Networking System ,Vol. 4, issue 2, 2015.

19. S.Murugan,M.Sundara Rajan,”Role of Anomaly IDS in Network,International Journal of Communication and Networking System”, Vol. 2, issue 2, 2013.