Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks

K. Ganesh Reddy
Dept. of Computer Science & Engg.
NITK, Surathkal
guncity11@gmail.com

Dr. P. Santhi Thilagam
Dept. of Computer Science & Engg.
NITK, Surathkal
santhisocrates@gmail.com

Bommena Nageswara Rao
Dept. of Computer Science & Engg.
NITK, Surathkal
bnagesh.nitkian@gmail.com

ABSTRACT
Wireless Mesh Networks (WMNs) are a promising technology to provide the wireless internet connectivity. WMNs are becoming a popular choice for wireless internet service providers to offer internet connectivity as it allows a fast, easy and inexpensive network deployment. However, security in WMNs is still in its infancy. Security and privacy has been a major concern in WMNs. WMNs are susceptible to broad variety of attacks due to its open medium, dynamic topology and lack of physical security. WMNs are more vulnerable in Network layer. Several attacks are possible in the network layer. Some of the attacks have possible solutions but there is no solution for to detect Rushing attack which leads to the Denial of Service. In this paper, the authors proposed Cross-Layer Intrusion Detection System (CLIDS) for Rushing attack. We evaluated the performance of our technique using network simulator 2. Simulation results show that CLIDS has less false positive and false negative rates than single layer intrusion detection system.

Keywords
Wireless Mesh Networks, Rushing Attack, Cross Layer Approach and Intrusion Detection System.

1. INTRODUCTION
Wireless Mesh Networks (WMNs) [1-5] are dynamically self-organized and self-configured systems. WMNs are easy to setup, cost effective, offer network flexibility and self-healing reliability. It consists of Mesh Routers (MR) and Mesh Clients. Mesh Routers can relay data on behalf of other nodes, thus increasing communication range and bandwidth. In WMNs, each node is connected to many other nodes. If any node drops out of the network, due to some hardware problem or any other reason, its neighbors easily find another route. The principle is data will hop from one node to other until it reaches the destination. The characteristics of WMNs like the open medium, dynamic topology and lack of physical security make them extremely vulnerable to various kinds of attacks. As WMNs provide support for heterogeneous networks, there is no complete secure protocol. ecuring WMNs is the most challenging task. Many attacks are possible at different layers of the network.

CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India]

WMNs are more vulnerable especially in network layer followed by MAC layer and Physical layer. Network layer attacks are mainly of two types: control plane attacks and data plane attacks. Control plane attacks affect the route discovery and maintenance phases of reactive, proactive and hybrid routing protocols. Data plane attacks affect the actual data packets by dropping or modifying. Initially, rushing attack is one of the control plane attacks that are possible in WMNs. Once it is in active route then it starts doing all data plane attacks [16]. The study shows that Rushing attack is more dangerous and there is no specific method for the detection of attack. In this paper, we focus on the detection of Rushing attack in WMNs. Rushing attack exploits the route discovery phase. A hostile node launching this attack, broadcasts the rushed Route Request (RREQ) message before any other intermediate node by ignoring the delay. Thus, it increases the likelihood that the hostile node gets included in active path. This attack leads to data plane attacks also called Denial of Service (DoS) attacks. DoS attacks can reduce the resource availability and result in massive service disruption.

Intrusion Detection Systems (IDS) [6] are widely used in networks as a second line of defense to secure against attacks. Intrusion detection can be defined as the process of monitoring events happening in the network and assessing them for the signs of violation of security policies. These are of two types: single layer IDS and cross layer IDS. Single layer IDS functions based on information from a single layer whereas in cross layer IDS, behavioral information from two or more layers is used for detection. The experimental results and analysis show that Cross layer IDS is more effective than Single layer IDS. Cross-layer design in wireless networks is a widely research topic. We used multi-layered approach to detect malicious nodes on AODV protocol with parameters like Packet Drop Ratio (PDR), channel error rate, and hop_count and other routing flags. This method reduces the false positive and false negatives rates. False Negative is a failure of an IDS to detect an actual attack. False Positive is an event signaling an IDS to produce an alarm when no attack has taken place [3].

The rest of the paper is organized as follows. In this paper first, we discuss the related work in section 2. Section 3, illustrates the Rushing attack. Section 4, presents the proposed mechanism. We describe our proposed method to detect Rushing attack. Section 5, summarizes the results and analysis of performance and Section 6, draws conclusion.

2. RUSHING ATTACK
Rushing attack exploits the route discovery process to increase the likelihood that a malicious node is included in a given route. Rushing attack is a zero delay attack. On-demand routing

protocols like AODV/DSR are more vulnerable to this attack. In route discovery phase, source node floods the route request (RREQ) packet in the network. The intruder receives the route request packet and broadcasts it without any delay in the network. Whenever the legitimate nodes receive the original packet, the nodes drop this packet because these nodes already received packet from the intruder and consider it as duplicate packet. The purpose of this attack is to increase the probability that a hostile node is included in a given route. It is more effective when an adversary node is nearer to either source or destination.

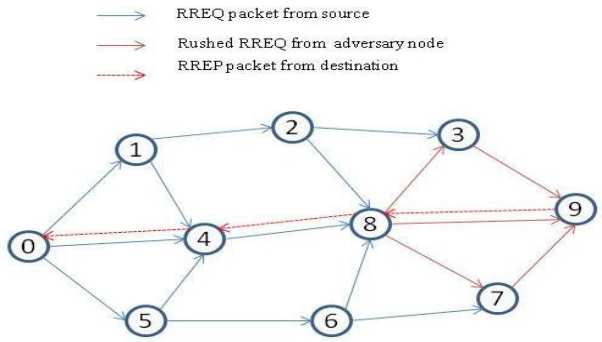

Figure 1. Rushing attack

Figure 1 shows an example of rushing attack. The source node 0 broadcasts RREQ packet in network. The hostile node 8 receives RREQ packet and broadcasts it without any delay in the network. The intermediate nodes 3, 7 and destination node 9 receive this packet. The nodes 3 and 7 suppress the actual RREQ received from nodes 2 and 6 respectively due to their RREQ duplicity. Eventually destination node 9 includes an adversary node 9 as an intermediate node in the route.

3. RELATED WORK

We found some of existing detection systems available for WMNs. Here, we present some of the works carried out recently. Zonghua Zhang *et al.* [7] developed a protocol called RADAR – a reputation-based scheme for detecting anomalous nodes in WMNs. RADAR uses the concept of reputation and describes a reputation-based anomaly scheme for detecting malicious nodes in these networks. Bose *et al.* [9] proposed a cross layer based intrusion detection system for the detection of denial of service attacks. They focused on the detection of collision, packet drop and misdirection attacks.

Xia Wang *et al.* [10] proposed cross-layer based anomaly detection in Wireless Mesh Networks. They presented a cross-layer based anomaly detection model which utilizing machine learning algorithms for profile training and intrusion detection. Latha *et al.* [11] proposed a solution to prevent rushing attack in wireless mobile ad hoc networks. In the existing protocols, since every node forwards only the first RREQ it receives, the rushing attacker tries to forward the received request first to its neighbors. But they changed this property to overcome this attack. However, it does not guarantee the complete prevention of Rushing attack.

Ferreira *et al.* [12] proposed an intrusion detection mechanism for WMNs using a hybrid approach. In this approach, the concepts of wavelets and neural networks are used for detection and classification of attacks. Jim Parker *et al.* [13] proposed cross-layer analysis for detecting wireless misbehavior. Their scheme employs cross-layer interactions based on observations at various networking layers to decrease the number of false positives. Thamilarasu *et al*. proposed a cross layer based IDS to detect malicious nodes. They mentioned lower false positives using watchdog monitoring mechanism. John *et al.* [6] had done analysis on single layer and cross layer approaches for intrusion detection in MANETs. They examined strengths and weaknesses of single layer and cross layer approaches. The experimental results and analysis clearly show that cross layer approaches are more effective than single layer approaches.

Some of the above papers focused on attacks such as packet dropping, collision and misdirection attacks. Some concentrated on misbehavior in WMNs. There is no solution for the detection of Rushing attack. Our work provides a solution against the dangerous Rushing attack in WMNs. Our method uses cross layer interactions for the detection of attack. The false positives and false negatives are very low. It offers high detection rate and increased throughput.

4. Cross-Layer Intrusion Detection System (CLIDS)

In this section, we discuss our proposed mechanism for the detection of Rushing attack in WMNs. Our solution is a cross-layer design because it uses behavioral information from two layers for the detection. It makes use of parameters like packet drop ratio, channel error rate from MAC layer, delay, and hop count from network layer. Packet drop ratio is the ratio of number of packets dropped to number of packets sent. Table 1 show the parameters used in our detection mechanism.

Table 1. Parameters used in algorithm

T_p	Time taken for a request to travel from source to destination (Practical)
T_t	Time taken for a request to travel from source to destination (Theoretical)
H_c	Number of hops in route (Hop Count)
d	Delay at each node to transmit the request
pdr	Packet Drop Ratio
cpdr	pdr with channel errors
p_t	Periodic interval

Algorithm: CLIDS for Rushing Attack

1. Find the time (t_1) at which the source node S initiates route discovery process.
2. The node S initiates route discovery process by broadcasting RREQ packet in network. The intermediate nodes also broadcast the packet until it reaches destination node D.
3. Find the time (t_2) at which the node D receives RREQ packet.
4. Calculate the time T_p by using the equation: $T_p = t_2 - t_1$.
5. Get the number of hops in route (H_c).
6. Calculate the time T_t by using the equation: $T_t = H_c * d$.
7. **If** T_p is less than T_t **then**
8. Alert "Rushing attack is suspected in the given route".
9. **For** each node in the route **do**
10. **If** pdr > cpdr **then**

11. Alert “The node is an adversary node”.
12. **End if**
13. **End for**
14. **If** no node is detected **then**
15. goto step 9 and repeats for every p_t
16. **End if**
17. Down the current path and take another path.
18. **Else**
19. Alert “Rushing attack is not suspected in the given route”.
20. **End if**

In our solution, we calculate theoretical time required for a RREQ message to travel from source to destination. We also calculate practical time required for RREQ message to travel from source to destination. Then we compare these two values. If practical time is less than theoretical time, it will alert the rushing attack is suspected. Whenever the rushing attack is suspected, for each node in the route, check for packet drop ratio of it. This method calculates packet drop ratio for each node by monitoring the network in promiscuous mode using watchdog. Initially, packet drop ratio for each node is set to zero. Later, these values will be updated in regular intervals. For a node, its neighbors calculate the packet drop ratio. A packet may be dropped due to several other reasons such as link error, network congestion, queue overflow and channel errors. To reduce the false positive and false negative rates, this method also consider channel error rate into account for the detection of malicious node. If the difference of packet drop ratio of a node and channel error rate is positive then the node is an adversary node. In case, current route is suspected as Rushing attacker but no such attack is identified in this path. However, this process will repeat for every periodic interval p_t to identify the adversary nodes in the suspected path.

5. SIMULATION AND RESULTS

We have simulated our mechanism in network simulator (ns-2.34), an object oriented, discrete event driven network simulator developed at Berkeley written in C++ and OTcl.

Table 2. Simulation Parameters

Property	Value
Nodes	50
Simulation Time	100 seconds
Routing Protocol	AODV
Application Traffic	CBR
Coverage Area	800m X 800m
Number of attackers	10 % and 20 %

The table 2 shows parameters used for simulation. Two simulation tests, each having different number of hostile nodes, were run to plot a graph throughput versus time. Throughput is the number of bits transmitted in unit of time.

We have compared the two different scenarios to find the false positive and negative rates

1. With Single Layer IDS(SLIDS-network layer only)
2. With Cross-Layer IDS(CLIDS)

Network layer IDS only consider network layer metrics such as delay and number of hops. Cross-Layer IDS consider the network layer metrics as well as MAC layer metrics to reduce the false positive and false negative rates.

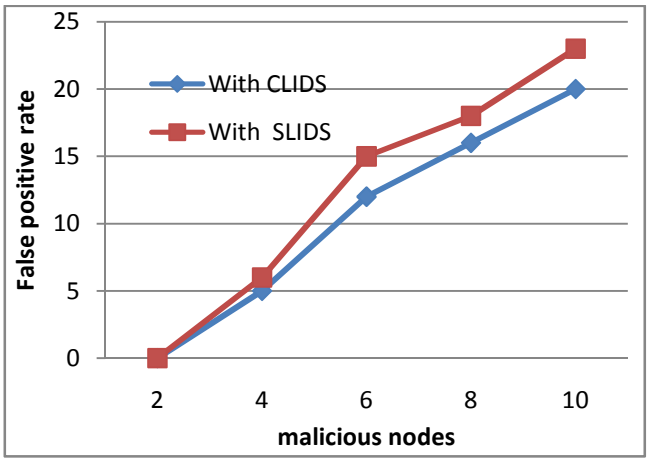

Figure 2.False positive rate vs. No. of malicious nodes

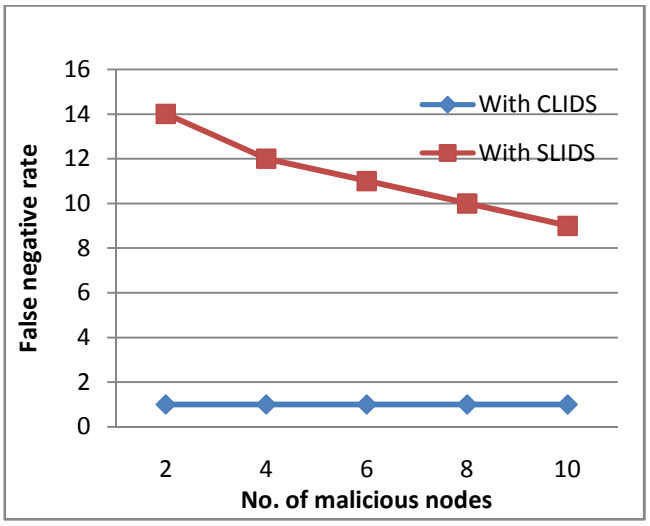

Figure 3. False negative rate vs. No. of malicious nodes

The figure 2 is plotted false positive rate versus number of malicious nodes where false positive rate is taken along X-axis and number of malicious nodes is taken along Y-axis. Figure 2show that CLIDS false positive rate is increasing with respect to number of malicious nodes. Because when there are more malicious nodes, every node may not get included in active route. So detection rate is less when there are more malicious nodes. In SLIDS the false positive rate is more when compare with CLIDS false positive rate. The figure 4 is plotted false negative rate versus number of malicious nodes. In which CLIDS false negative rate is only 1%. This rate is constant even when the number of attacker’s are increased in the network. In SLIDS average false negative rate is 11% which is ten times higher than CLIDS false

negative rate. As a result, CLIDS can effectively identify and isolate the Rushing attacks.

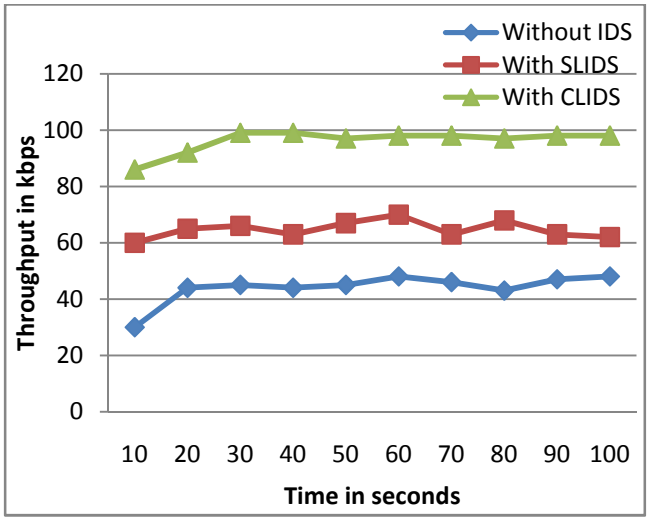

Figure 4.Throughput vs. Time

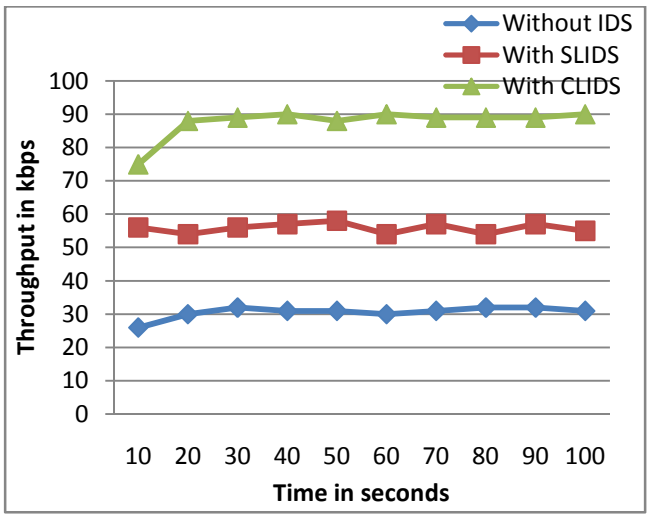

Figure 5.Throughput vs. Time

We also observe the throughput results in three different scenarios:

3. Without IDS
4. With Single-Layer IDS(SLIDS)
5. With Cross-Layer IDS(CLIDS)

The figure 4 and the figure 5 are plotted throughput versus time where time taken on X-axis and throughput taken on Y-axis. In figure 2, 10% nodes are adversary nodes whereas in figure 3, 20% nodes are adversary nodes. In both cases we have observed the throughput in all three scenarios. Without IDS mechanism throughput is severely degrade and average throughput falls between40-20 kbps. SLIDS only considers network layer parameters due to this it has high false negative rate. As a result, the average throughput falls between and 55-65kbps. CLIDS overcomes this problem by considering network and MAC layer permeates at same time. Hence, the CLIDS average throughput is increased and falls between 85-97 kbps.

6. CONCLUSION

In this paper, we have presented cross-layer intrusion detection system (CLIDS) for the detection of Rushing attack in Wireless Mesh Networks. CLIDS mainly consider the both network layer and MAC layer parameters to reduce false positive and false negative rates. This solution is simulated using Network Simulator. Our CLIDS gives better throughput and less false positive and rate. We also prove that CLIDS is better than SLIDS.

[1] Ian, A., Wang, X., and Kiyon. 2005. A Survey on Wireless Mesh Networks. In Proceedings of the IEEE Radio Communication.s23–s30.

[2] nitin.;Mattord, verma (2008). Principles of Information Security. Course Technology. pp. 290–301.ISBN 978-1-4239-0177-8.

[3] Salem, N. and Hubaux, J. 2006. Securing Wireless Mesh Networks. In *Proceedings of the IEEE Wireless Communications*. 50–55.

[4] Ping, Y., Tianhao, T., Ning, L., Yue, W., and Jianqing M. 2009. Security in Wireless Mesh Networks: Challenges and Solutions. In *Proceedings of theIEEE – International. Conference on Information Technology*. 423–428.

[5] Muhammad, S. and Hong, C. 2007. Security Issues in Wireless Mesh Networks. In *Proceedings of the IEEE – International Conference on Multimedia and Ubiquitous Engineering*. 717–722.

[6] Joseph, J. F. C., Das, A., Seet, B. C., and Lee, B. S. 2007. Cross Layer versus Single Layer Approaches for Intrusion Detection in MANETs. In *Proceedings of ICON*. IEEE, 194–199.

[7] Zhang, Z., Nait-Abdesselam, F., Ho, P.H., andLin, X. 2008. RADAR: a reputation-based scheme for detecting anomalous nodes in wireless mesh networks. In*Proceedings of WCNC*. IEEE, 2621–2626.

[8] Thamilarasu, G., Balasubramanian, A., Mishra, S., and Sridhar R. 2005. ACross-Layer based IntrusionDetection Approach for Wireless Ad-hoc Networks. In *Proceeding of the IEEE International Conference in Mobile Adhoc and Sensor Systems Conference*, 2005. 1- 8

[9] Bose, S. and Kannan, A. 2008. Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks. In *Proceedings of the IEEE – International Conference on Signal processing, Communications and Networking*. 182–188.

[10] Wang, X., Johnny, S. W., Stanley, F., and Samik, B. 2009. Cross-layer Based Anomaly Detection in Wireless Mesh Networks. In *Proceedings of the IEEE – Annual International Symposium on Applications and the Internet*. 9–15.

[11] Latha, T., and Sankaranarayanan, V. 2006. Solution to Prevent Rushing Attack in Wireless Ad hoc Networks. IEEE, 42–47.

[12] Ferreira, E. W.T., Oliveira, R.,Carrijo, G.A., andBhargava, B. 2009. Intrusion detection in wireless mesh networks using a hybrid approach. In *Proceedings of the 29th IEEE*

[13] *International Conference on Distributed Computing Systems Workshops*. pp 451–454.

[14] Parker, J., Anand, P., and Joshi, A. 2006. Cross-layer Analysis for Detecting Wireless Misbehavior. In *Proceedings of the IEEE CCNC*. pp 6–9.

[15] Steve, G., Portmann, M., and Muthukkuumarasamy, V. 2008. Securing Wireless Mesh Networks. In Proceedings of the IEEE Internet Computing.pp 30–36.

[16] Ganesh and P. Santhi (2012) Taxonomy of Network Layer Attacks in Wireless Mesh Proceedings of the Second International Conference on Computer Science, Engineering & Applications (ICCSEA 2012), 167, pp 927-935