International Journal of Engineering & Technology, 7 (2.20) (2018) 302-305

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Probability Model for Intrusion Detection System in Mobile Adhoc Network

Bharathisindhu.P[1*], Dr S.SelvaBrunda[2*]

[1] *Ph.D Scholar, Bharathiar University,Coimbatore*
[2]*Professor,Department of CSE, Cheran College of Engineering,Karur*
**Corresponding author E-mail:bharathisindhu.p@gmail.com*

Abstract

Wireless technologies increasingly exist everywhere in advanced networks; however, this new innovation accompanies its own set of challenges. The nodes in the wireless network are characteristically 'open' and viewable by all network scanners. Networks are protected using many firewalls and encryption software's. Firewalls restrict access between networks to prevent intrusion and do not indicate an attack within the network. An Intrusion Detection System (IDS) is required which monitors the network, detects misbehavior or anomalies and notifies other nodes in the network to avoid or punish the misbehaving nodes. In this paper, we propose a probability based IDS model that provides generalized solution to detect set of malicious nodes to improve the detection speed and accuracy.

Keywords: *Attacks; Intrusion Detection; MANET.*

1. Introduction

A mobile ad hoc network (MANET) is a group of mobile nodes which can transfer data packets between each other via wireless links either directly or depending on other nodes as routers. The operation of MANETs happens without a pre-existing infrastructure or base station. The nodes of the network move randomly without any restriction. Therefore, the network topology of a MANETs may change rapidly and unpredictably. The nodes themselves manage the change in topology and transferring data packets between the nodes. The size of the network may vary from a small, static network to a large-scale, highly dynamic mobile network.

Due to the features like dynamic network topology, poor central administration and restricted battery-based energy of mobile nodes, MANET is exposed to various types of attacks. The attacks can either be external attacks or internal attacks. The malicious and misbehavior nodes in the network are identified by acknowledgement based techniques. Malicious nodes are capable of inducing any one of the following attacks either to re-route the packets or to drop the packets [1].

- Black-hole Attack
- Gray-hole attack
- Worm-hole attack
- Denial of Service (DOS) Attack
- Distributed (DOS) Attack

It is very important to embed Intrusion Detection System (IDS) into MANETs to detect and prevent the attacks. IDS acts as a second layer of defense. Many researchers have contributed to the design of IDS for MANETs to detect and prevent these attacks. [2][3][4][5].

In this paper we propose a generalized solution to detect the set of malicious nodes such as black-hole, worm-hole, gray-hole and DOS attacks. The proposed probability based model improves the network performance by providing QOS and by eliminating the attacker nodes in the network and improves the detection speed and accuracy.

2. Related Work

The Watchdog mechanism is the most widely used method in all well-known IDSs. This mechanism detects the misbehaving nodes by eavesdropping on the wireless channel in passive mode. It decides whether or not the next-hop node to transmit the data packet. The receiving status of the next-hop's link is unknown. A failure counter is set, if the data packet forwarding by the next node is unsuccessful. When the value of this counter exceeds the predefined threshold value, the node is identified as malicious. The issues like receiver collisions, false misbehavior report, ambiguous collisions, limited transmitted power and partial dropping are not addressed by this scheme[6].

The TWOACK scheme overcomes the issues receiver collision and limited transmitted power that are not addressed in Watchdog. The acknowledgement for every data packet over three consecutive nodes is sent from the source to destination. If the acknowledgement (ACK) is not received in a predefined time, the other two nodes are identified as malicious. This TWOACK scheme has its limitations like increased overhead, limited battery power and the degradation in the life span of the entire network [7].

Adaptive ACKnowledgment (AACK) solves the limited transmission power and receiver collision problems. This is an enhanced version of TWOACK scheme. The detection overhead is reduced and the detection efficiency is improved [8].

The combined version of ACK and TWOACK has been proposed as AACK scheme. In this scheme, the source node sends data packet to every node until it reaches the destination. The receiver sends an ACK once the data packet is received. The concept of TWOACK scheme is adopted, it ACK is not received within the predefined time interval. This scheme reduces the overhead and fails to identify the malicious nodes with false misbehavior report [9].

Two-fold approach IDS is presented to detect and isolate the nodes that drop data packets. The ACK packets are sent by each intermediate node to the source node to confirm the reception of data packet. The misbehavior of nodes is detected and malicious activity is identified. As the acknowledgement packets are sent by every intermediate node to the source the overhead is high in this approach [10].

Enhanced Adaptive Acknowledgment (EAACK) scheme is an improved version of the earlier IDS schemes that resolves the issues false misbehavior, limited transmission node and false misbehavior of the nodes. This scheme is the combined version of ACK, S-ACK and Misbehavior Report Authentication (MRA). This is an acknowledgement based IDS. All the acknowledgement packets are digitally signed before they are transmitted and received [11].

3. Proposed Model

The existing IDS schemes were implemented by Route Establishment Phase and Acknowledgement phase. Route establishment is done during the initiation of data transmission or during the route failure including the link and node. Acknowledgement phase takes care of sending the ACK to the source on receiving the data packets.

The proposed model provides the improved capacity for detecting the malicious nodes in the network. Each node maintains monitoring timer with the packet receiver count and packet send count. If the monitoring timer expires, Nodes will calculate difference between these two and detects the malicious nodes. This model provides a generalized solution to detect the set of misbehavior nodes in the network, supervised learning based classifier is used.
This probabilistic model identifies the relationship between the data values. And then calculates the correlation then identifies the differences between data values. By applying thresholding, malicious node is detected by comparing the relationship between the data values.The relationship is estimated by spatio-temporal method. The relationship is estimated in terms of mean, standard deviation, expectation and differentiation value.

$$\text{Mean}=\frac{s1+s2+s3+s4+s5}{5} \quad \text{----------} \quad \text{--(1)}$$

Standard deviation =

$$\frac{1}{n}\sqrt{\sum_{i=1}^{n}(X_i-mean)^2} \quad \text{----------} \quad \text{----------(2)}$$

$$\text{Variance} = (\text{S.D})^2 \quad \text{----} \quad \text{----------(3)}$$

$$\text{Expected value= (mean+ variance)} \quad \text{----------(4)}$$

Overhearing model is used to provide a unique solution. The detection is based on packet generation rate, packet loss rate and packet delay.

Packet generation rate is estimated as (no of packet generated / time)

Packet loss rate = (number of packet generated – number of packet received) / time

Packet delay = (packet receive time – packet send time)

Overall packet delay = sum of (packet receive time – packet send time) / number of packets

The parameters are estimated as
P1=avg generation rate/max generation rate

P2= avg loss rate/max loss rate

P3=avg delay/max delay

Weight factor=(α1,α2,α3)

Final value=p1.α1+p2.α2+p3.α3

During the decision making phase nodes are differentiated,

If(Node parameter value>final value)
Node as malicious node
else
Node is normal node[for DOS/DDOS attacks]
For the classification process,Probability based hypothesis model is used. Trust value for expectation is listed as follows,
Tv=<{normal behavior(LB)
Tv=>(UB)

Hypothesis-p0,p1
LB<TV<UB
(NV/LB)<TV
(NV/UB)>TV
P0-normal behavior
P1-malicious behavior
P1-normal behavior
P0-malicious behavior

Null hypo=∑trust value/min trust
Alternate=∑trust value/max trust
Normal\misbehavior
Lognormal prob=log(pr(BER/H1)/pr(BER/H0))
=>ώn=||BER|| where(i==1)
ώn=no of positive
n = total count
log normal prop=>ώn α log(p1/p0)+(n-ώn) α log((1- p1)/(1-p0))

The malicious nodes are identified for packet data changer attacks.Once the malicious node is identified by probability model,malicious announcement message is sent as network wide broadcast message and then the node is eliminated from the network.

4. Experimental Results

The proposed Probability based IDS is evaluated with the ns-2 network simulator. The numbers of nodes considered for simulation is 100 mobile nodes. Table 1 depicts the simulation parameters.

Table 1: Simulation Parameters

Topology area	*1000x1000m*
Transmission range(coverage)	*250m*
Number of nodes	*100*
Connection type	*UDP*
Traffic Application	*CBR*
Packet generation interval	*0.1s*
Packet Size	*1000b*
Mac layer type	*802.11*
Interface queue	*Priority queue*
Antenna model	*Omni-directional antenna*
Simulation time	*250s*

the following performance metrics are used for evaluating the simulation.

- Throughput
- Packet Delivery Ratio
- Transmission Rate
- Dropping Ratio
- Normalized Dropping Overhead
- Delay

The transmission of packets is depicted in the Figure 4.1. The transmission rate is on the rise with respect to the proposed model. As the attacks are detected earlier, the packet drop is reduced.

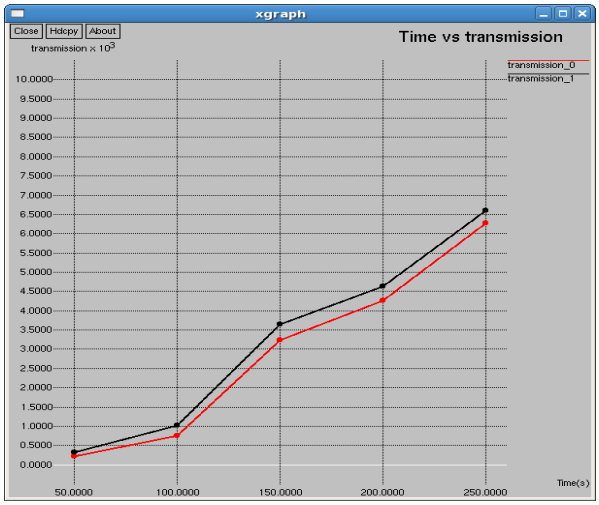

Figure 4.1 Time vs Transmission

The Packet Delivery Ratio is presented in Figure 4.2. The PDR is on the rise even though the number of nodes increases.

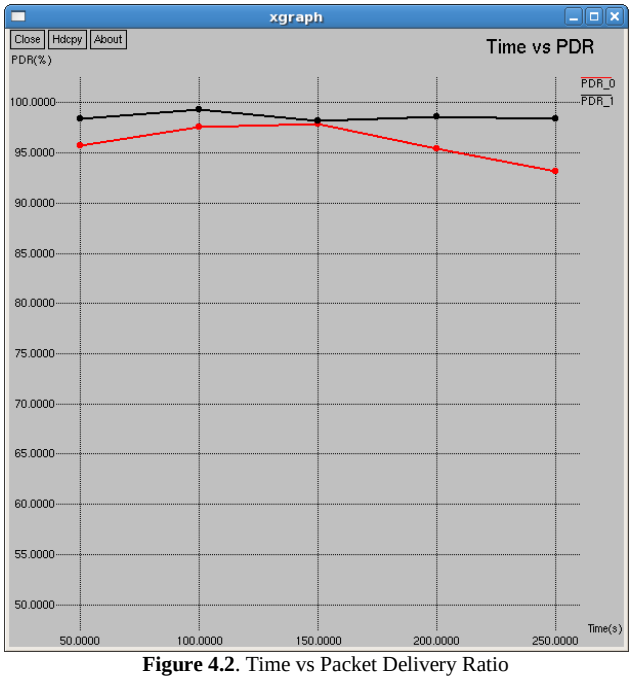

Figure 4.2. Time vs Packet Delivery Ratio

It is very clear that the proposed model provides a high throughput when compared to ACK based IDS. The throughput is presented in Figure 4.3.Malicious nodes may hinder the data transfer between nodes. The malicious nodes in the network are identified by the probability hypothesis. This improves the throughput of the network in the proposed model. Throughput is evaluated at different time intervals. At all the times, the throughput is always high in the proposed model whereas it is less in the ACK based IDS.

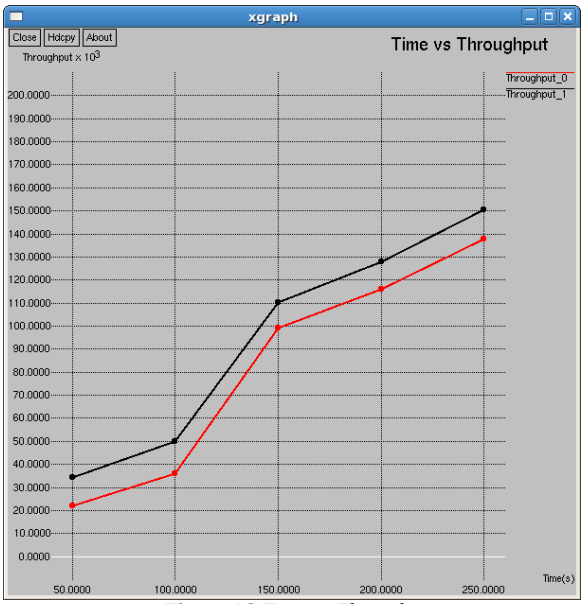

Figure 4.3 Time vs Throughput

The delay of the network is depicted in Figure 4.4. The delay of ACK based IDS is high when compared to the proposed model. This gives the better performance of the network. In a 250 node network, the delay is 0.4ms with ACK based IDS whereas it is 0.3 ms in the proposed model. As the malicious nodes are detected at the earliest, the delay of transmission is reduced. The delay is measured at different time intervals. The probability based approach provides less delay.

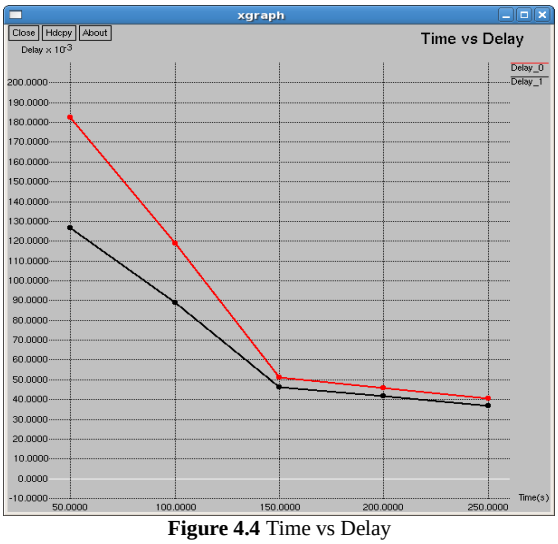

Figure 4.4 Time vs Delay

The Dropping Ratio is presented in Figure 4.5. The Dropping Ratio is reduced in the proposed model. The proposed model outperforms ACK based IDS. As the attackers are detected at the earliest, the packet drop is minimized and the network performance is improved.

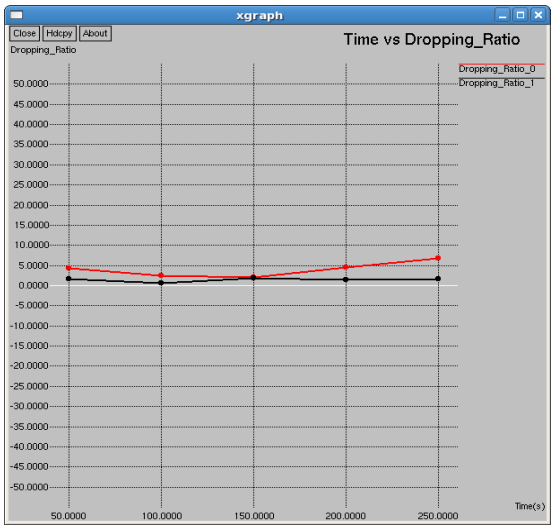

Figure 4.5 Time vs Dropping Ratio

The Normalized Routing Overhead (NRO) is presented in Figure 4.6. The NRO is reduced in the proposed model. In the 200 nodes network, the NRO of acknowledge based IDS 2 where as the proposed IDS is 3.

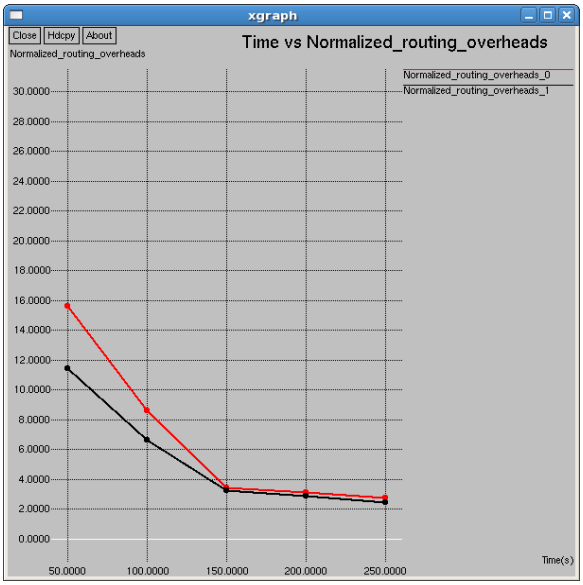

Figure 4.6 Time vs Normalized Routing Overheads

5. Conclusion

MANETs are exposed to different types of attacks. The node misbehavior due to packet dropping or route failure may weaken the performance of the network. In this paper a Probability based Intrusion Detection System is proposed for identifying the malicious nodes at the earliest. The proposed approach improves the detection speed and accuracy with less overhead. The simulation of the proposed approach is implemented in Network Simulator 2 and the results show that the proposed probability based IDS model outperforms the existing ACK based IDS schemes.

References

[1]Y.C.Hu, A.Perrig and D.B.Johnson, "Ariadne:A Secure on-demand routing protocol for adhoc networks," Proc. of MobiCom '02, pp.2-23, 2002.

[2]Buchegger, S. and Le Boudec, J.Y, Performance analysis of the CONFIDANT protocol: Cooperation of nodes, fairness in dynamic ad-hoc networks. In Proceedings of MobiHoc'02.

[3]Buttyan, L. and Hubaux, J.P, Enforcing service availability in mobile ad-hoc WANs. In Proceedings of the 1st ACM international Symposium on Mobile Ad Hoc Networking & Computing (Boston, Massachusetts).International Symposium on Mobile Ad Hoc Networking & Computing.IEEE Press, Piscataway, NJ, 87-96.

[4]Hubaux, J-P., Gross, T., Boudec, Le and Vetterli, M, Toward self-organized mobile ad hoc networks: The terminodes project. In IEEE Communications Magazine.

[5]Jakobsson, M., Hubaux, J-P. andButtyan, L., A micropayment scheme encouraging collaboration in multihop cellular networks. In Proceedings of Financial Cryptography, Jan 2003.

[6]Marti, S., Giuli, T. J., Lai, K., and Baker.M, Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (Boston, Massachusetts, United States, August 06 - 11, 2000).MobiCom '00. ACM, New York, NY, 255-265..

[7]K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehaviour in MANETs, IEEE Trans. Mobile Computing,vol. 6, no. 5, pp. 536–550, May 2007.

[8]A Al-Roubaiey et al., AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement, 24th IEEE International Conference on Advanced Information Networking and Applications, 2010,

[9]T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, Video transmission enhancement in presence of misbehaving nodes in MANETs,‖ Int. J. Multimedia Systems, Vol.15, No.5, pp. 273–282, Oct. 2009

[10]Muhammad Zeshan, Shoab A. Khan, Ahmad RazaCheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," in International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[11]Nan Kang. Elhadi M. Shakshuki, Tarek R. Sheltami, "Detecting Misbehaving Nodes in MANETs", iWAS2010, 8-10 November, 2010, Paris, France.