ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Parametric Threshold Effectuation for Single Step Wormhole Tracking Down

K. Aathi Dharshini[#1], C. Susil Kumar[*2], E.Babu Thirumangai Alwar [#3]

[#1] ECE Department, Velammal College Of Engineering and Technology, Madurai, Tamil Nadu, India

[*2]CSE Department, Hindusthan Institute Of Technology, Coimbatore, Tamil Nadu, India

[#3] ECE Department, Velammal College Of Engineering and Technology, Madurai, Tamil Nadu, India

ABSTRACT— Communication in mobile Adhoc networks is completed via multi-hop ways. Owing to the distributed specification and restricted resource of nodes, Manet is a lot prone to wormhole attacks i.e. wormhole attacks place severe threats to each adhoc routing protocol and a few security enhancements. Thus, so as to discover wormholes, totally different techniques are in use. In all those techniques fixation of threshold is merely by trial & error methodology or by random manner. Conjointly wormhole detection is in twin part by putting the nodes that is higher than the edge in a suspicious set, however predicting the node as a wormhole by using some other algorithms. Our aim in this paper is to deduce the traffic threshold level by derivational approach for identifying wormholes in a very single phase in relay network having dissimilar characteristics.

KEYWORDS— Manet, wormhole, Traffic prediction, parametric threshold implication, derivational approach.

I. INTRODUCTION

A mobile unintended network (MANET) could be a self configuration infrastructure less network with non centralized administration. A mobile Adhoc or unintended network is an autonomous assortment of mobile devices (laptops, smart phones, sensors, etc.,) that communicate with one another over wireless links and collaborate in a distributed manner so as to produce the required network Practically within the absence of a fixed infrastructure. Every device in a MANET is unengaged to move independently in any direction, and can amend its links to different devices often. This type of network, operating as a complete network or with one or multiple points of attachments to cellular networks or the web, paves the approach for variable new and exciting applications. Application scenarios embrace, however are not restricted to: emergency and rescue operations, conferences are field settings, automobile networks, personal networking, etc. In wormhole attack, malicious node receives knowledge packet at one point within the network and tunnels them to a different malicious node. The tunnel existing between two malicious node is named as a wormhole. The tunnel gets the information from one network and replicates to different network. A wormhole therefore permits an attacker to form two attacker controlled choke points which may be utilized by the attacker to degrade or analyze traffic at a desired point. TPIDS is a lightweight traffic prediction intrusion detection theme that tumbling the value of communication and energy by hastily detecting the behavior of the intrusions. Some work has been done to wormhole attack in mobile unintended networks however it cause excessive false alarm rate. In this paper we are focusing on reducing warning rate by choosing optimum threshold value to save lots of wastage of energy and information measure of mobile nodes in sleuthing wormholes. The remaining components of this paper is organized as follows: section III provides traffic prediction supported ARMA, section IV provides experimental analysis and results, section V presents relation between attributes of the network and threshold values, section VI presents threshold selection, finally conclusion is conferred in section VII.

II. RELATED WORK

The discussion starts by Yu Bo's paper that relies on the discovery of multi-hop recognition theme to detect attacks caused by the selection of transmitting the irregular packet loss. In this theme, a region of the transmission path, nodes are going to be randomly selected for testing. Detection point is going to be generated for every incident packet to the upstream transmission methods, any node within the middle, if not adequately recognized package, can generate warning data of abnormal packet loss and to submit a multi-hop to the supply node. Here, we have considered ton choosing transmission attack is taken into account, that introduces larger communications and computing prices. Then khin sandar win [6] proposes solely an analysis of detecting wormhole attack in wireless network, simply by quoting the benefits and drawbacks not suggesting for the foremost economical one. Han zhijie[1] instructed traffic prediction methodology, however he didn't decrease the false alarm rate whereas detecting wormholes. Faizal M.A.[2] offers regarding solely a way to verify threshold values by using SPC approach that are more necessary for detection of wormholes and conjointly to scale back false alarm rate within the MANET. This observation is finished on real time network traffic having the aim of distinguishing the typical connection created by the host or hosts to single victim among one second interval.

III. TRAFFIC PREDICTION BASED ON ARMA

The existing traffic prediction model includes Poisson model, Markov model, auto-regressive model where Poisson is not suitable for the flow characteristics of MANET. This paper gathers information from Markov model and enhances it in auto-regressive moving average model to predict MANET traffic and the specific prediction model which is shown below:

Each and every node in MANET has its own random variable sequence $X_0, X_1, X_{2,}...$ is used to denote the state of the node at the same time; different nodes can be in different modes. Assume $X_n = i$ that is nodes are in the operational mode i when it is in time domain n and also assume that the entire state transition take place at the beginning of any time domain, each node has some fixed probability in the state i .if the next state is j , then this is denoted by P_{ij}

$$P_{ij} = P\left\{X_{m+1} = j \mid X_m = i\right\} \tag{1}$$

Where

P_{ij} $\rightarrow$ The probability of entering the state j when a node is in the operational state i .

The migration probability of second-order is defined as P_{ij}^2 that is, a node in the current state of i will enter the state j after having two state transitions. (i.e.)

$$P_{ij}^{(2)} = P\left\{X_{m+2} = j \mid X_m = i\right\} \tag{2}$$

This can be calculated by the following formula:

$$P_{ij}^{(2)} = \sum_{k=1}^{M} P_{ik} P_{kj} \tag{3}$$

The migration probability of n order is denoted as

P_{ij}^2 which is taken from the chapman- kolomogorov equation:

$$P_{ij}^{n} = \sum_{k=1}^{M} P_{ik}^{(r)} P_{kj}^{(n-r)} \tag{4}$$

Where

γ can take any arbitrary values between 0 and n.

A further notation of Markov chain for probability is to use M*M matrix of P which is called as migration probability matrix. In this matrix, the element P_{ij} represents the probability in the i th row and j th column.

$$\begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1M} \\ P_{21} & P_{22} & \cdots & P_{2M} \\ . & . & \cdots & \cdots \\ P_{M1} & . & . & P_{MM} \end{bmatrix} \tag{5}$$

Here, P^2 can be calculated by P*P and in general, $P^{(m+n)=}P^{(m)}*P^{(n)}$ which is similar to

By migration probability matrix and the initial X_0 of each node, we can build the sequence while comparing energy consumption and mobility for the entire MANET. If a node travels from i^{th} state to s^{th} state, then the number of time domains the node remains in the s^{th} state is given by:

$$\sum_{t=1}^{T} P_{is}^{(t)} \tag{6}$$

Assuming that B_S is the data transmissible data quantity of a node stays at state s. then after calculating the number of domains, the total data transmissible quantity is given by the formula:

$$B^T = \sum_{s=1}^{M} \left(\sum_{t=1}^{T} P_{is}^{(t)} \right) * B_S \tag{7}$$

And also the data of each node in the time can be calculated by equation (7).the transmissible data quantity for the total number of nodes in a cluster is given by

$$B_{total} = \sum_{C_{k-1}}^{C_{k-n}} \sum_{s=1}^{M} \left(\sum_{t=1}^{T} P_{is}^{(t)} \right) * B_s \tag{8}$$

Where

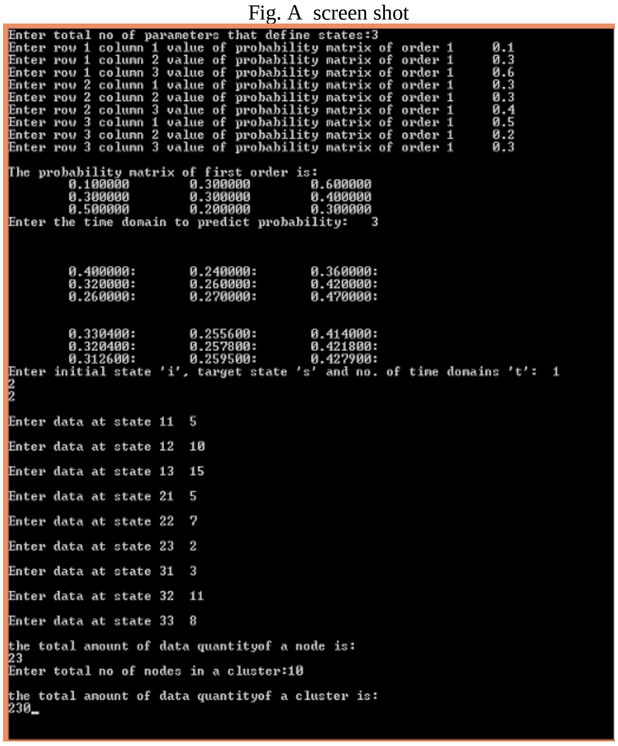
$C_k \rightarrow$ it is to represent i^{th} node, in cluster $C_{k.}$

$P_{is}^{(t)} \rightarrow$ is the probability from i th state migrating to the s^{th} state.

IV. EXPERIMENTAL ANALYSIS AND RESULTS

Generally, networks of nodes are created which generates its traffic randomly with specific direction and velocity. Using ARMA algorithm, traffic prediction for single node is found by equation (7) and also traffic prediction for cluster of different nodes is calculated by equation (8). Using intrusion detection system, detected traffic for each node is analyzed which results node with high traffic is finally concluded as wormhole. Further this paper focused on detecting anomalies caused by the invasion and leaving decision making and counter measures.

Fig. A screen shot



The Fig A shows the combined execution of both prediction data algorithm and the wormhole detection algorithm. Since the predicted data is got from the ARMA algorithm, it uses probability matrix i.e the probability of a nodes to go from state 'i' to state 'j' after time 't' is shown in the above result.

In order to deduce the relation between the threshold and network attributes first we have to stumble on the relationship between the varying network characteristics and the normalized data. For this we reflect on the data present in each node, number of nodes, time instants etc.

Varying the network attributes like amount of data in nodes, number of nodes, number of time instants the results have been simulated.

A. Analysis Using Data

By varying the amount of data in each node in both prediction algorithm and wormhole detection algorithm, the total predicted data the actual data in the wormhole and the data in other nodes after certain number of transmissions is analyzed.

TABLE I
ANALYSIS USING DATA

S.NO	Data in each node	Predicted data	Actual data in wormhole	Data in other nodes
1	2,2,2	11.88001	12	5,3
2	2,4,6	28.20005	28	3,7
3	5,10,15	43.2000	55	6,16
4	20,30,40	129.60086	170	21,51
5	60,70,80	189.000031	410	61, 131
6	50,100, 150	180	550	51, 151

This table (I) describes the relation between the predicted data and actual data in wormhole by varying the amount of data in each node. The inference is that data in wormhole is more than data in other nodes. More the increase in data in each node more will be the variation in predicted and the actual one. With this variation into concern the below graph is plotted.

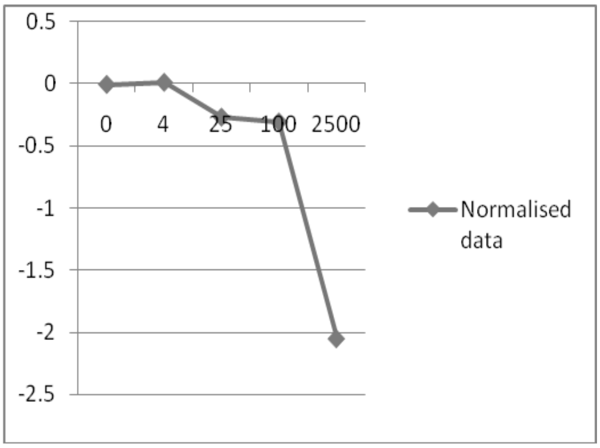


Fig. 1 Variance Vs Normalized data

The Fig 1 is plotted against variance calculated from the amount of data in each node, and the normalized data calculated from the formula

$$\text{Normalized data} = \frac{\text{Predicted Data} - \text{Actual Data}}{\text{Predicted Data}} \quad (9)$$

This graph infers that there is a diminishing relation between the amount of data in each node, and the normalized data which is above calculated.

B.Analysis Using Number of Nodes

By varying the number of nodes in both prediction algorithm and wormhole detection algorithm, the total predicted data, the actual data in the wormhole and the data in other nodes after certain number of transmissions is analyzed.

TABLE II
ANALYSIS USING NUMBER OF NODES

S. NO	No. of nodes	Data in each node	Prediction data	Actual data in worm hole	Data in other nodes	No. of txm
1	4	20,30,40,50	1783.5	291	22, 51, 110	4
2	5	20,30,40,50,60		391	22, 51, 91	5
3	6	20,30,40,50,60,70	9007.2	551	22,52, 91,110,101	6
4	7	20,30,40,50,60,70,80	25278	651	22,51, 91, 111	7
5	8	20,30,40,50,60, 70,80,90	33282	811	22,51, 91,111,131	8
6	9	20,30,40,50,60	5116.4	991	22,51, 91,111	9

This table (II) infers that while varying the number of nodes a suitable relation is formed between the predicted data and actual value of data from which a graph is plotted.

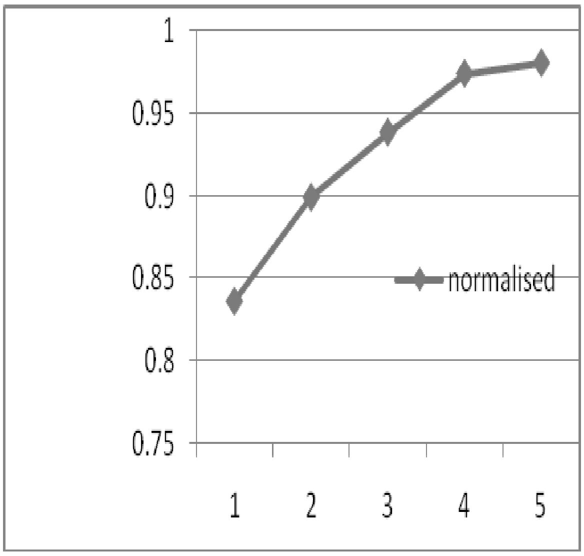


Fig. 2 No. of Nodes Vs Normalized data

This Fig. 2 infers that there is some linear relation between the varying nodes and the normalized value calculated from the above equation (9) by tagging the varying number of nodes in the X-axis.

TABLE III
ANALYSIS USING NO. OF TIME INSTANTS

No. of node	Data in each node	No. of Time instants	Predicted data	Actual data	Data in other nodes
3	20,30, 40	3	1693.44	230	22,51
3	20,30, 40	4	2572.884	230	22,51
3	20,30, 40	5	8593.874	230	22,51
3	20,30, 40	6	5567.020	230	22,51
3	20,30, 40	7	20564.02	230	22,51
3	20,30, 40	8	299.2551	230	22,51

By varying the time instants in this table (III) a graph with some relation between the normalized data and the variable instants is plotted.

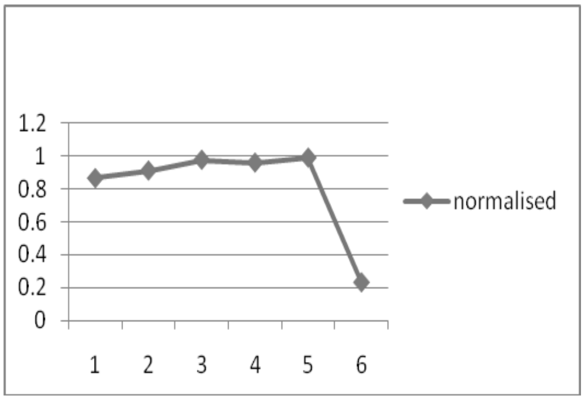


Fig. 3 No. of Time Instants Vs Normalized Data

This Fig. 3 shows a decreasing relation on comparing the normalized data and the number of time instants by labeling them in the Y-axis and X- axis respectively.

V. RELATION BETWEEN NETWORK ATTRIBUTES AND THRESHOLD VALUES

Assume completely different threshold values then experiment it with a network having characteristics like range of nodes, traffic intensity, node density and additionally wormhole density. And then, realize false alarm rates for every assumed threshold values. The detection rate performance is highest for one threshold worth for this network of certain parameters. The experiment is then repeated by varying the characteristics of the network and similar threshold values with best performance are obtained. Such threshold values of highest detection rate performance are found for every network with varied parameters. A mathematical relation is then deduced between the parameters of the network and thus obtained threshold values. Based on this relation, an optimum threshold value with least false alarm rate may be selected for a network with any parameter set. This experiment result would be within the kind of a mathematical expression obtained by theoretical analysis.

VI. THRESHOLD SELECTION

The normal and the abnormal traffic are differentiated employing a threshold value. Thus appropriate selection and therefore the correct threshold value add an additional advantage for IDS to notice anomalies within the network. Choosing inaccurate threshold value can cause an excessive false alarm particularly if the vales is simply too low or if it’s too high, it can cause the intrusion activity being considered as traditional traffic. Most of the analysis doesn’t propose a correct technique to spot the threshold technique. Dynamic threshold is set by dynamic threshold technique needs previous data of the network traffic before the threshold worth are often designated.

VII. CONCLUSION

In this paper, anomaly detection and security scheme based on Markov model is used by each node in MANET to predict traffic (TPIDS). All the above analysis shows that there exists a perceptible relation obtained by altering the network attributes, with this noticeable relation it is evident that there prevails an optimal threshold based on this relation. On deriving this relation wormhole detection can be ended in single phase. This relation is malleable to the protocol DSDV which finds the wormhole by using shortest distance, hence in future work the optimal threshold for other routing protocols such as AODV etc can be deduced.

REFERENCES

[1] C Han Zhijie, Wang Ruchuang: “Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model”, *2012* International Conference on Solid State Devices and Materials Science.

[2] Faizal M. A., Mohd Zaki M., Shahrin S., Robiah Y, Siti Rahayu S., Nazrulazhar B.: “Threshold Verification Technique for Network Intrusion Detection System”, (*IJCSIS) International Journal of Computer Science and Information Security*,Vol. 2, No. 1, 2009.

[3] Ankita Gupta,Sanjay Prakash Ranga: “Wormhole Detection Methods In Manet*”,International Journal Of Enterprise Computing And Business Systems(IJECBS),* Vol. 2 Issue 2 July 2012.

[4] Moutushi Singh, Rupayan Das: “A Survey Of Different Techniques For Detection of Wormhole Attack In Wireless Sensor Network”, *International Journal of Scientific & Engineering Research* Volume 3, Issue 10, October-2012.

[5] Murad A. Rassam, M.A. Maarof and Anazida Zainal: “A Survey of Intrusion Detection Schemes in Wireless Sensor Networks” *American Journal of Applied Sciences*, 2012.

[6] Khin Sandar Win, Pathein Gyi: “Analysis of Detecting Wormhole Attack in Wireless Networks”, *World Academy of Science, Engineering and Technology* , 2008.

[7] Lukman Sharif and Munir Ahmed, “The Wormhole Routing Attack in Wireless Sensor Networks (WSN)”, *Journal of Information Processing Systems*, Vol.6, No.2, June 2010.

[8] Jing Deng, Richard Han, and Shivakant Mishra, “Defending against Path based DoS Attacks in Wireless Sensor Networks’ SASN’05, November 7, 2005.

[9] Llker Demirkol, Fatih Alag¨oz,Hakan Delic, Cem Ersoy. Wireless Sensor Networks for Intrusion Detection: Packet TrafficModeling[EB/OL].www.cmpe.boun.edu.tr/~ilker/IlkerDEMIRKOL_COMML_ext_abstract . pdf.

[10] Onat I , Miri A. ‘An intrusion detection system for wireless sensor networks/Proceedings of the IEEE International Conference on Wireless and Mobile Computing’ , Networking and Communications (WiMOB’05) Mont real , Canada , 2005.