ISSN: 2456-2955
Volume 2, Number 2
UNIVERSAL JOURNAL OF COMPUTERS & TECHNOLOGY

Simulation And Auditing Of Network Security Based On Probabilistic Neural Network Approach

Dr. A. Jacob
Computers and Information Technlolgy department, Macquarie University, Australia
Prof. h. Lucas
Department of IT, Charles Sturt University, Australia

Abstract

Probabilistic Neural Network approach used for mobile adhoc network is more efficient way to estimate the network security. In this paper, we are using an Adhoc On Demand Distance Vector (AODV) protocol based mobile adhoc network. In our Proposed Method we are considering the multiple characteristics of nodes. In this we use all the parameter that is necessary in AODV. For simulation purpose we use the probabilistic neural network approach that gives more efficient and accurate results as comparison to the clustering algorithm in the previous systems was used. The performance of PNN (probabilistic neural network) approach is improved for identifying the particular attack like as wormholes, black holes and selfish.

Keywords*:* Mobile adhoc network, Adhoc On Demand Distance Vector Routing, probabilistic Neural Network Analysis , attacks.

1. Introduction

Network security is attracting more and more attention. Simulation is a better choice to research the problems of network security because of their high complexity. Based on the purpose and actuality of simulation of network security, this paper puts forward a simulation method of network security using system dynamics. After giving the steps of system dynamics simulation of network security, this paper has simulated the attack of worm using system dynamics[1]. The simulation results indicate system dynamics can describe the processes of worm attack well. The research of system dynamics of network security will extend the methods of simulation of network security. Mobile adhoc networks , wireless sensor networks (WSNs), and wireless mesh networks (WMNs), have received increasing attention in the past decade due to their easy deployment at low cost and broad applications, ranging from tactical communication in a battlefield, disaster rescue after an earth quake, to wildlife monitoring and tracking, last-mile network access, and etc. Routing in multi-hop wireless networks presents a great challenge mainly due to the following facts. First, wireless Links are unreliable because of channel fading [1]. Second, achievable channel rates may be different at different links since link quality depends on distance and path loss between two neighbors. Third, as the Wireless medium is broadcast in nature, the transmission on one link may interfere with the transmissions on the neighboring links. A new routing paradigm, known as Adhoc on Demand Distance Vector AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbors and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors" periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To- Infinity could happen.

AODV is an „on demand routing protocol" with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports uncast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by AODV is distributed, hop-by-hop, deterministic, single path and state dependent.

AODV uses IP in a special way. It treats an IP address just as an unique identifier. This can easily bend one with setting the subnet mask to 255.255.255.255 . But also aggregated networks are supported. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. In AODV the routing table is expanded by a sequence number to every destination and by time to live for every entry. It is also expanded by routing flags.

By using probabilistic neural network approach in mobile adhoc network identification of attacks on system dynamics is more accurate as comparison to clustering algorithm because the chances of overlapping was more. The performance of probabilistic neural network is also well.

2. Previous Work

THE STEPS OF SYSTEM DYNAMICS SIMULATION ABOUT NETWORK SECURITY PROBLEM[1]

According to the system dynamics modeling simulation theory and the purpose of network security simulation, system dynamics simulation of the network security problem includes the following four steps.

A. Analyzing the problem and establishing the causal loop B. Actuality of simulation of network security Diagram

C. Designing ingeniously and establishing system dynamic equations.

D. Setting the model parameter and carrying on the simulation and the model verification.

Since there is no data available about the network characteristics on attacked situation, hence it was needed to simulate the network for such condition and to collect the data, for this purpose a network simulator, and after simulating the network for different scenario the raw data is collected. Now this data is classified into different group based on the data type (delay, drop rate, conjunction, packet type, bandwidth utilization, process status, services running, and processor utilization), then each data set it normalized by detecting its maximum and minimum values by the following formula –

$$Vnorm=(V-Vmin)/(Vmax-Vmin)$$

$$TRNVEC=[Vnorm1,Vnorm2,\ldots\ldots Vnormr]$$

The normalized values set are arranged in an array to represent system condition by a vector this vector can be represented by Hence the system states can be projected into a hyper space of n dimensions.

According to the system states, vectors of that states are grouped and the centre for that group is calculated after that the maximum radius is also calculated (by measuring the distance from centre point to the point of maximum distance)[3].

State-transition analysis:- Here, an attack is described with a set of goals and transitions that must be achieved by an intruder to compromise a system. Transitions are represented on state-transition diagrams[5].

Statistical analysis approach:- This is a frequently used method (for example SECURENET). The user or system behavior (set of attributes) is measured by a number of variables over time. Examples of such variables are: user login, logout, number of files accessed in a period of time, usage of disk space, memory, CPU etc. The frequency of updating can vary from a few minutes to, for example, one month. The system stores mean values for each variable used for detecting exceeds that of a predefined threshold. Yet, this simple approach was unable to match a typical user behavior model. Approaches that relied on matching individual user profiles with aggregated group variables also failed to be efficient. Therefore, a more sophisticated model of user behavior has been developed using short- and long-term user profiles. These profiles are regularly updated to keep up with the changes in user behaviors. Statistical methods are often used in implementations of normal user behavior profile-based Intrusion Detection Systems[6].

3. MOBILE AD HOC NETWORKS USING AODV ROUTING PROTOCOL

A mobile ad hoc network is a collection of autonomous mobile nodes that communicate with each other over wireless links. Such networks are expected to play increasingly important role in future civilian and military settings, being useful for providing communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. However, since there is no stationary infrastructure such as base stations, mobile hosts need to operate as routers in order to maintain the information about the network connectivity. Therefore, a number of routing protocols have been proposed for ad hoc wireless networks.

MANETs routing protocols are characteristically subdivided into three main categories. These are proactive routingprotocols, reactive on-demand routing protocols and hybrid routing protocols.

A new routing paradigm, known as Adhoc on Demand Distance Vector AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbors and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To- Infinity could happen. AODV is an „on demand routing protocol" with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs. In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent.

AODV uses IP in a special way. It treats an IP address just as an unique identifier. This can easily bend one with setting the subnet mask to 255.255.255.255 . But also aggregated networks are supported. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. In AODV the routing table is expanded by a sequence number to every destination and by time to live for every entry. It is also expanded by routing flags..

4. Proposed Algorithm

In this first we simulate the mobile adhoc network by OPNET modeler for five scenarios. After properly simulation of all attacks all the data collected by this will be use in training algorithm of neural network. After training completion for particular type of system dynamics values we estimate the condition of network and specific attack can be identified.

Probabilistic Neural Network Approach-

Neural networks use their learning algorithms to learn about the relationship between input and output vectors and to generalize them to extract new input/output relationships. With the neural network approach to intrusion detection[15], the

main purpose is to learn the behavior of actors in the system (e.g., users, daemons). It is known that statistical methods partially equate neural networks. The advantage of using neural networks over statistics resides in having a simple way to express nonlinear relationships between variables, and in learning about relationships automatically. Experiments were carried out with neural network prediction of user behaviors. From the results it has been found that the behavior of UNIX super-users (roots) is predictable (because of very regular functioning of automatic system processes). With few exceptions, behavior of most other users is also predictable. Neural networks are still a computationally intensive technique, and are not widely used in the intrusion detection community[4]. This aw of nearest-neighbor-like algorithms has been recognized before, and there have been a few proposed solutions. They all use what Dasarathy (1991) calls modified metrics", which are non-Euclidean distance measures in feature space. All the approaches to modified metrics criteria which the chosen metric should optimize. Some criteria allow explicit derivation of the new metrics. However, the validity of these derivations relies on there being a very large number of exemplars in the training set. A more recent set of approaches

(i) Use criteria which measure the performance on the training set using leaving-one outcross-validation (ii) restrict the number of parameters of the metric to increase statistical significance.

(iii) Optimize the parameters of the metric using non-linear search techniques. For this technique of locally weighted regression, uses an evaluation criterion which is the sum of the squares of the error using leaving-one-out. His metric has the form d2 = w1(x1+y1)2+:::+wk(xk+yk)2, and hence has k free parameters w1; :::;wk. it uses Levenberg-Marquardt to optimize these parameters with respect to the evaluation criterion. For their Weighted K-Nearest Neighbors (WKNN) algorithm, Kelly and Davis (1991) use an evaluation criterion which is the total number of incorrect classifications under leaving-one-out[16]. Their metric is the same as Atkeson's, and their optimization is done with a genetic algorithm. We use an approach similar to make PNN more robust with respect to transformations.

Syntax-

net = newpnn(P,T,spread)

Description

Probabilistic neural networks (PNN) are a kind of radial basis network suitable for classification problems.

net = newpnn(P,T,spread) takes two or three arguments,

P

R x Q matrix of Q input vectors

T

S x Q matrix of Q target class vectors

Spread

Spread of radial basis functions (default = 0.1) and returns a new probabilistic neural network. If spread is near zero, the network acts as a nearest neighbor classifier. As spread becomes larger, the designed network takes into account several nearby design vectors.

Examples

Here a classification problem is defined with a set of inputs P and class indices Tc.

P = [1 2 3 4 5 6 7];

Tc = [1 2 3 2 2 3 1];

The class indices are converted to target vectors, and a PNN is designed and tested.

T = ind2vec(Tc)

net = newpnn(P,T);

Y = sim(net,P)

Yc = vec2ind(Y)

Algorithm

newpnn creates a two-layer network. The first layer has radbas neurons, and calculates its weighted inputs with dist and its net input with netprod. The second layer has compet neurons, and calculates its weighted input with dotprod and its net inputs with netsum. Only the first layer has biases.

newpnn sets the first-layer weights to P', and the first-layer biases are all set to 0.8326/spread, resulting in radial basis functions that cross 0.5 at weighted inputs of +/- spread. The second-layer weights W2 are set to T.

In this probabilistic neural network approach we used an K-Means algorithm for training and estimation of network attack. So this will give the curved output. The chances of overlapping definitely reduced and identifying the particular attack becomes simple. This method gives up to 79 to 81% accuracy.

5. Results

We are expecting that the performance of this algorithm will be more efficient then comparison to previous casual loop diagrams and rough clustering algorithms . we are expecting that the accuracy of this algorithm will be 80% and the identification of particular attack like worm holes, black holes ,selfish and sleep will be efficiently and accurately.

6. Conclusion

This probabilistic neural network approach will be more efficient and accurate as comparison to previous casual loop clustering algorithm. The measurement of accuracy will be about approximate 80%. So it reduces the chances of overlapping of attack area. So the identification of attacks based on system dynamics will be more accurate.

7. Acknowledgement

I express my deep sense of gratitude to Dr. Manish Shrivastava (head of department IT) ,LNCT BHOPAL(MP), whose kindness valuable guidance and timely help encouraged me to complete this paper. And a special thanks to Asst. Prof. Kavita Deshmukh, who helped me in completing this research and she exchanged her interesting ideas, thoughts, and made this research easy and accurate.

8. REFERENCES

[1] Kong Hong-shan, Zhang Ming-qing, Tang Jun, Luo Chang-yuan “The research of simulation for network security based on system synamics”,ICIAS,2009.

[2] Handan, Hebei Province,”Investigation of PCFA in assessing main function indexes of intrusion detection system in network security”,ISIEEC,2009.

[3] Li Cong-cong1,Guo Ai-ling2,Li Dan3 “Application Research of Support Vector Machine in network Security risk evaluation”,2007.

[4] D. Couto, D. Aguayo, J. Bicket, and R. Morris, “A high-throughput path metic for multi-hop wireless routing,” in Proc. ACM MobiCom‟03, San Diego, CA, Sept. 2003.

[5] M. Zorzi and R. R. Rao, “Geographic random forwarding (geraf) for ad hoc and sensor networks energy and latency performance,” IEEE Trans. Mobile Computing, vol. 2, no. 4, 2005.

[6] S. Biswas and R. Morris, “Exor: opportunistic multi hop routing for wireless networks,” in Proc. SIGCOMM‟05, Philadelphia, PA, Aug. 2005.

[7] P. Garcı´a-Teodoroa, J.Dı´az-Verdejo, G. Macia´- Ferna´ndeza, E. Va´zquezb “Anomaly-based network intrusion detection Techniques, systems and challenges ” published on computers & security 28 (2009) 18 – 28

[8] H. Dubois-Ferriere, M. Grossglauser, and M. Vetterli, “Least-cost opportunistic routing,” School of Computer and Communication Sciences, EPFL, Technical Report LCAV-REPORT-2007-001, 2007.

[9] K. Zeng, W. Lou, J. Yang, and D. R. Brown, “On throughput efficiency of geographic opportunistic routing in multihop wireless networks,” in Proc. QShine‟07, Vancouver, British Columbia, Canada, Aug. 2007.

[10] K. Zeng, W. Lou, and Y. Zhang, “Multi-rate geographic opportunistic routing in wireless ad hoc networks,” in Proc. IEEE Milcom, Orlando, FL, Oct. 2007.

[11] K. Zeng, W. Lou, J. Yang, and D. R. Brown, “On geographic collaborative forwarding in wireless ad hoc and sensor networks, ” in Proc. WASA‟07, Chicago, IL, Aug. 2007.

[12] B. Awerbuch, D. Holmer, and H. Rubens, “The medium time metric: High throughput route selection in multi-rate ad hoc wireless networks,” MONET, vol. 11, no. 2, pp. 253–266, 2006.