Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

A SURVEY ON INTRUSION DETECTION IN MANET

Karishma V R, Karthigha M

[1]PG Scholar, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore
[2]Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore

Abstract- *The Mobile ad-hoc Network(MANET) is a type of wireless technology which has mobility of nodes with self configuring ability. It is a future trend with emerging applications. It has been introduced to meet out the incorporated problems in wired networks. It has few limitations like network life time, multi-hop architecture, heterogeneity, limited communication bandwidth, etc. Though, it has been used widely for faster communication its dynamic topology is vulnerable to various attacks. To encounter those vulnerable attacks in MANET various intrusion detection system is used which will upgrade MANET with high security. Here we have examined various methodologies for detecting intrusion in MANET.*

1. INTRODUCTION

Mobile Ad Hoc Network(MANET) in recent years becomes an extensive area of research. The increase of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. The increase of mobile devices as well as development in wireless communication, ad-hoc networks is acquiring importance with the increasing number of widespread applications. Ad-hoc networking can be incultated anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or disquit to use.. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Ad hoc networking allows the devices to maintain connections to the network as well as easily connect and remove devices from the network . Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Nodes in mobile ad hoc network should be able to spot the presence of other nodes and perform necessary procedure to ease communication and sharing of service and data. Because of the nodal mobility, the network topology may change rapidly and unpredictably over time. In network there is no centralized control, where network organization and message delivery executed by the nodes themselves. As there are many irresistible future applications of mobile ad hoc networks (MANETs), there are still censorious issues to be confronted [1].The subsequent list of issues indicates the inadequacies and restrictions that have to be overwhelmed in a MANET environment. Restricted wireless transmission range, time-varying wireless link characteristics, broadcast nature of the wireless medium, packet losses due to transmission errors, mobility-induced route changes, mobility-induced packet losses, battery constraints, potentially frequent network partitions, ease of snooping on wireless transmissions (security issues), routing, quality of service [2].

Intrusion detection systems (IDS's) have become most important part in the Security. It is very important element of a complete information security system. Intrusion detection is the process of monitoring computer systems or networks for unauthorized access, activity, or file modification. IDS can also be used to monitor network traffic, so it can detect the system whether it is being targeted by a network attacks. An intrusion detection System can also be defined as a detection system which is of type automated and which is used to alert the available system and security management by generating an alarm at a location where the attack is taken place. If any attack or intrusions have taken place or something different from natural activity happened, IDS come into existence and actions have been taken[3].

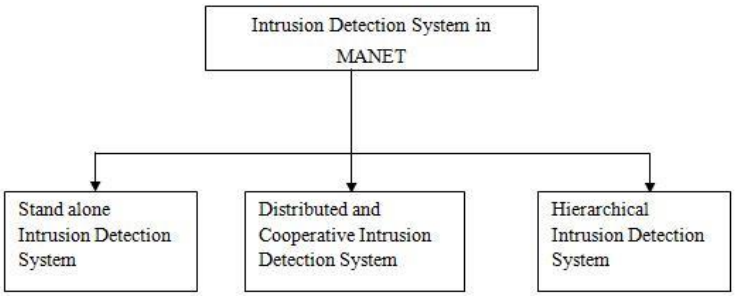

Figure 1.1 Intrusion Detection System in MANET

In Fig 1.1 the various intrusion detection system that have been used in MANET is categorized. Intrusion are the set of actions that attempt to modify the integrity, confidentiality or availability, and Intrusion Detection System (IDS) is a system or software application that monitors network traffic, and if any suspicious activity is found then it alerts the system or network administrator. The IDS can be easily implemented on these devices, because of Many intrusion detection systems have been proposed for wired network where all traffic goes through the switches, routers or gateway. While on the other hand MANET does not have all such nodes and any user can access it because of its open medium. Hence current IDS technique on wired network cannot be implemented directly on MANET. There are mainly three types of IDS techniques that can be applied on MANET.

A. Stand Alone Intrusion Detection System:

In this system, an intrusion detection system run's independently on individual node to determine intrusions. All decision taken about a particular activity is depend only on information gathered at its own node, because there is no collaboration among nodes in the network. Therefore, no information is transferred. Even, a node in the same network does not have any information about the other nodes in the network as no alert information is transferred. This model is not efficient because of its limitations, it may be effectively applicable in a network where all nodes already have an IDS installed. This system is also suitable for single layer network as compared to multi-layered network infrastructure. Because the available information on any single node is not sufficient to detect intrusions, this system has not been selected as IDS for MANETs .

B. Distributed and Cooperative Intrusion Detection System:

In this architecture, every node has an IDS agent which detects intrusions locally and collaborates with neighboring nodes for global detection whenever available evidence is indeterminate and a broader search is required. Whenever the intrusion is captured, an IDS agent can either issue a local response (*e.g.* alerting the local user) or a global response. Each node participates in intrusion detection method and response as having an IDS agent running on them. The responsibility of an IDS agent is to detect and collect local information and data to identify any attack if there is any attack in the network, and also take a response independently. However, neighboring IDS agents also cooperates in global intrusion detection when the evidence is inconclusive.

C. Hierarchical Intrusion Detection System:

Hierarchical IDS system enlarges the functions of distributed and cooperative IDS system and has been implemented for multi-layer network infrastructures where the network is divided into different small networks known as clusters. Each cluster head usually have more functionality as compared to other members in the cluster, like transmitting the data packets into other cluster. So, we can say that these cluster heads, in some way, perform their working as a central point's which are similar to wired network's controlling devices like routers, switches or gateway. The concept of multi-layering is applied to intrusion detection systems where hierarchical IDS are proposed. Each IDS agent run's on particular member node and is responsible for its node. They will monitor and decide on locally detected intrusions.

2. METHODOLOGIES USED FOR INTRUSION DETECTION IN MANET

A. GENETIC ALGORITHM

It is a method of soft computing which uses the laws of selection and evolution. These algorithms are implemented by converting a problem in a particular field into a model a chromosome like structure. In computer network security, it is mainly used to find an optimal solution to a problem . The Genetic Algorithm start by identifying a data set called population. Then these are individually encoded using bits, characters or integers and they form a chromosome.

The next operation on them is an 'Evaluation Function' used to determine the genuine chromosome.. During this process, two different operations namely, crossover and mutation are performed which is used to imitate the breeding and evolution. The selection of the chromosome is biased towards the fittest of the species. At last, the fit chromosome is selected once the optimization criterion is met [4].

The stepwise working procedure of Genetic programming,

(1) ***Get the network parameters of the nodes (15, 25,50) in the network.-*** This step includes getting the parameters like packet drop, request forwarding rate, reply receive rate , node id etc.

(2) ***Calculate the first threshold based on network parameters.-***The threshold is calculated as follows,

T1 = Average (NPi)

Where, T1 = First Threshold

NPi = Network Parameter such as PD, RFR, RRR

I = 1,2,3….N.

N= Total no of nodes in the network

(3) ***Encode the chromosomes based on threshold criterion.*** Determine the chromosomes greater than the threshold.

(4) ***Shortlist the chromosomes based on their fitness.-*** Calculate the optimum parameters value as follows, *If(NPi<=T1) then { NPi-op =1} else {NPi =0}* This results in denoting the corresponding network parameter as either '0' for fit nodes and '1' for unfit ones. Here 'op' represents the optimum value calculation.

(5) ***Determine the second threshold.(T2)***-This is done by calculating the weighted average of the individual network parameters of the fit chromosomes.

(6) ***Select the survivor based on selection and recombination criteria. –*** This requires an If loop to determine the node id with all the optimal parameters after the second threshold to be zero. The corresponding node becomes the survivor "Black Hole" node and hence the corresponding node id is displayed.

Genetic Programming has been proven to be a good paradigm in the scenario of Network Intrusion Detection Systems (NIDS) development[5]. The main reason is that the functions used by GP can be defined ad hoc for a particular scenario and then the algorithm selects and combines them in order to optimize the solution to the given problem. Accordingly, it is appropriate for the complex intrusion detection domain.

B. BEE COLONY OPTIMIZATION ALGORITHM

The Bees Algorithm is an optimization algorithm arised by the natural foraging behavior of honey bees to find the optimal solution [6]. The required number of parameters, like n- Number of scout, e- Number of best sites out of m selected sites, m- Number of sites selected out of n visited sites, (m-e)- Number of bees recruited for the other selected sites.

Algorithm follows

Step1. Population initialized with random solutions. **Step 2**Fitness of the population is evaluated.

Step 3. While (stop when criteria is not met) //Forming new population.

Step 4. Selecting sites for neighborhood search.

Step 5. enrol bees for selected sites (more bees for best e sites) and evaluate fit nesses.

Step 6. Fittest bee is selected from each patch **Step 7.** Fitness of the bees are randomly checked. **Step 8**. End While.

The Bee Colony Optimization Algorithm works well in dynamic topology and self configuring nature. The most important way of communication is their dancing, the bee communicate with their neighborhood. Onlooker bees select the most profitable source on the basis of the all information revealed by the waggle dances [15].

C. ANT COLONY ALGORITHM

An Ants wander randomly, and after getting food return to their colony while laying down trails. After other ants found such a path, then the trail is followed by this path, but not randomly. If those ants find food then the trail starts evaporate and this will effect on the strength of that trail. Pheromone evaporation also has the nature of avoiding the convergence to a locally

optimal solution. The paths chosen by the first ants would tend to be excessively interested to the ants that follows them, if there is no evaporation. In that case, the probe of the solution space would be limited. Thus, when one ant finds a good path from the colony to a food source, other ants are more likely to follow the same path [6].

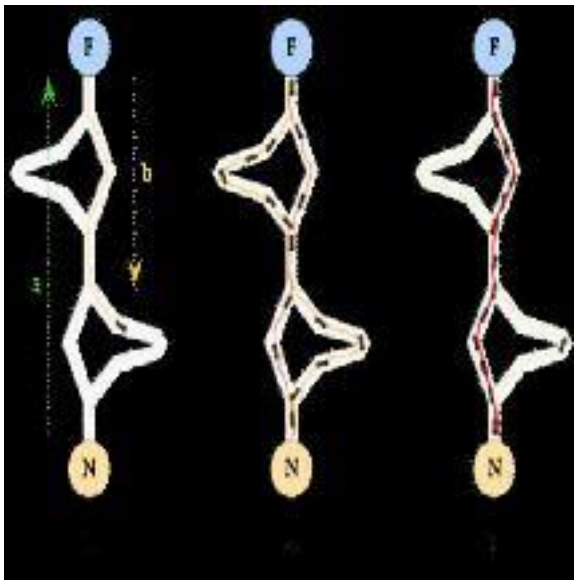

Figure 2.1 Ants follow a path between Nest and Food[13].

In general, an ACO algorithm can be applied to any optimization problem as far as it can be defined:

(1) ***An appropriate graph representation for problem*.** The problem must be described as a graph with a set of nodes and edges between nodes. The graph should accurately represent all states and transitions between states.

(2) ***Heuristic desirability*.** A suitable heuristic measure can be defined to describe the goodness of edges from one node to every other linked node in the graph.

(3) ***Solution construction mechanism*.** A method must be defined for building possible solutions.

(4) ***An autocatalytic feedback process*.** A suitable method of updating the pheromone levels on edges is required.

(5) ***A constraint-satisfaction method***. A mechanism is needed to ensure that only feasible solutions are constructed.

D.LOCALIZABILITY AIDED LOCALIZATION ALGORITHM

LAL can adequately manage the alteration of the traditional system, while conventional methodology could just make indistinctive increases [7].

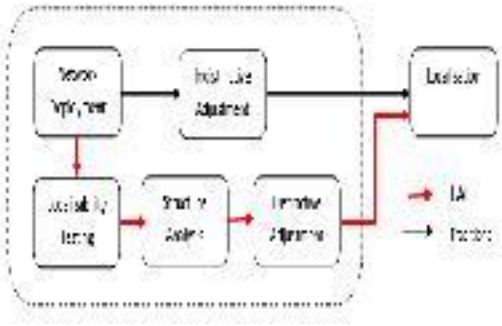

Figure2.2. Traditional and LAL work flow [7].

Fundamentally, LAL comprises of three noteworthy strides,

Step 1: Localizability testing

when a system is sent in an application field, because of some specific or environment variables fickle is meant to be faced in the outline stage, it might be not prepared for restriction, The localizable and non localizable centre in a system for further modification is happened due to the centre localizability testing is directed as formidable in LAL.

Step 2: Structure analysis

To assistance the fine-grained control, separation diagram is break down into two joined segments. These parts are composed in a tree structure and the one containing reference points is the root. Changes are led along tree edges from the root to clears out.

Step 3: Distinctive adjustment

LAL treats centre contrastingly as per their localizability and places in the segment tree. Through vertex growth, LAL without localizable they will change.

The source centre point stochastically picks an adjacent centre point with which to work together, as in the area of this centre is used as trap destination area to catch vindictive centre points to send an answer RREP (Route Reply) message. Noxious centers are along these lines perceived and kept from taking an enthusiasm for the guiding operation, using an opposite after framework. In this setting, it is acknowledged that when a significant drop happens in the pack movement extent, an alert is sent by the destination centre back to the source centre to trigger the acknowledgment framework yet again. LAL arrangement solidifies the advantage of proactive area first step and the predominance of open response at the following steps to reduce the benefit wastage.

E. BAYESIAN NETWORK USING K2 ALGORITHM

Bayesian network is a graphical tool used to fashion decision difficulty containing uncertainty. It is a directed loop less graph where each node represents a discrete speed vary of curiosity. Each node contain the states of wandering parliamentary variables that it represents and a conditional likelihood table which give conditional likelihood of these variable such as conaissance of other connected variables based upon baye's rule.

$$P(B/A)=p(A/B)P(B)/P(A) \quad \text{eq----------} \quad (1)$$

Conditional Probability table of a node contains probabilities of the node beings in a explicit state given the polity of the parents [9].

K2 is a division of the regularly used algorithms are under the control of Bayesian Networks. It is an algorithm for developing Bayes Network from a recorded databases. The algorithm requires a rest of nodes, a before recognized order on the nodes, a top certain on the wide diversity of root node may also have, and a database hold viable cases. It starts with the aid of consider that a node has no roots, after which; in each step it provides increase the root whose accumulation in the main increases the likelihood of the ensuing structure. The algorithm terminates adding mother and father to the nodes, when the accumulating of single root can't increment the probability of the network given the data. Though the K2 algorithm works properly for intrusion detection along with exceptional error rate, it then again requires an ordered set described as heuristic and it additionally lacks in computational simplicity. The fundamental middle of thought of our algorithm is to attain a node ordering from data. This ordering can then be second-hand as an input parameter to the K2 algorithm, which will then learn the shape of the BN with higher accuracy [10].
Working procedure of K2 algorithm,

{ Input: A accept of n nodes, an ordering regarding the nodes, an upper bound u on the longevity variety regarding mother and father a node might also have, then a database D containing m cases.}

{Output: For each node, a printout of the root node} **Step1**. Begin

Step2. i:=1;

Step 3. πi:= θ

Step 4. Pold:= g(xi, πi) **Step 5**. J:= i+1;

Step 6. Add (xj, πj) **Step 7**. Pnew =g(xj, πj)

Step 8. If Pnew>Pold Then Pold: = Pnew

Step 9. else Delete xj, from πj

Step 10. j:= j+1;

Step 11. If j>n Then i:= i+1; **Step 12**. Else go to step 3 **Step 13**. If j>n; Then i = i+1; **Step 14**. Else go to step 5 **Step 15**. If i== n Then End **Step 16**. Else go to Step 3

F. GAME THEORY

Game theory usually considers a multi-player decision problem where multiple players with different objectives can compete and interact with each other. Game theory classifies games into two categories: Non-cooperative and cooperative. Non-cooperative games are games with two or more players that are competing with each other. On the other hand, cooperative games are multi-players cooperating with each other in order to achieve the greatest possible total benefits.

A game consists of a set of players a set of moves available to those players, and a identification of payoffs for each combination of strategies. A player's plan for a strategy for actions in each possible scenario in the game. A player's payoff is depand on the condition where the player wins or loses in a particular situation in a game. A player has a dominant strategy if that player's best strategy does not depend on what other players do [19].

There are many Game theory algorithm existing based on cooperative and non-cooperative gaming methodologies.

Cooperative Game (Shapley value Approach) the cooperative intrusion detection technique in MANET using cooperative game theory concept (shapely value) for reducing the number of false positives generated in an IDS [21]. Every node in the network participates in detecting and responding to intrusions. Furthermore, every mobile node runs IDS locally to perform local data collection and anomaly detection also only two common intrusions: Cache poisoning and malicious flooding is considered. In the former, an adversary can compromise the information in the routing table through modifying its content, deleting information from it, or by injecting fake information.

Consider the model of a network in which sets of cache poisoning and malicious flooding are defined as follows: C = {0, 1} and M = {0, 1}. Each node is able to detect both intrusions. A one-to-one mapping O from the set of nodes N to C ×M, is defined as O: N → C × M, where O (Ni) = (ci, mi) means node Ni has detected cache poisoning (malicious flooding) attack, if ci(mi) is equal to one and has not detected otherwise. These sets will be used later on to indicate whether a node has sensed an intrusion or not. Here the MANET is modeled as an undirected graph G = (N,E), where N = {N1,....,Nl} is the set of mobile nodes.

The leader-IDS for increasing the effectiveness of IDS for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. Even most current solutions elect a leader randomly without considering the resource level of nodes. Such a solution will cause nodes with less remaining resources to die faster, the cluster lifetime is reduced faster. It is also vulnerable to selfish nodes that do not provide services to others while at the same time benefiting from such services. To increase the performance of IDS in MANET, a unique framework is proposed that is able to (i) Balance the resource consumption among all the nodes and thus increase the by electing truthfully and efficiently the overall lifetime of a cluster is maintained, most cost-efficient node known as leader-IDS. (ii) Catch and punish a misbehaving leader through random checkers that monitor the behavior of the leader [21].

3.CONCLUSION

We had a deep survey on various intrusion detection system that have been used in MANETs. There are various methodologies that are uniquely supporting the nature of the mobility of the nodes in the MANET. The algorithm has its own merits and limitation over various parameters, but enhancement in the parameters may help the algorithm to improvise to meet the limitation of the MANETs characteristics. IDS may help the MANET network to overcome the security issues. The algorithms encounters the various parameters like detection rate, efficiency of the system to increase the performance of the system.

REFERENCES

[1] Ankur O.Bang, Prabhakar L. Ramteke," MANET: History, Challenges and Applications",International Journal of Application in Engineering & Management, Volume 2, Issue 9, September 2013.

[2] Naeem Raza, Muhammad Umar Aftab, " Mobile Ad-Hoc Networks Apllications and its Challenges", Communication and Network, Volume 8, pp. 131-136, 2016.

[3]Mohit Soni, Manish Ahirwar, " A Survey on Intrusion Detection Technique in MANET", International Conference on Computational Intelligence and Communication Networks,2015.

[4] Sujatha K S, Vydeki Dharmar, " Design of Genetic Algorithm Based IDS for MANET",IEEE 2012.

[5] Sergio Pastrana, Aikateria Mitrokotsa,"Evaluation of Classification Algorithm for Intrusion Detection in MANETS", Article in Knowledge based system, December 2012.

[6] Harsimran Kaur, " Algorithm used in Intrusion Detection System: a review", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, May 2014.

[7] Josephin Asha Grace, Kavipriya G, " Intrusion Detection System in Stand alone and Cooperative Networks", ARPN journal of Engineering and Applied Sciences, Vol. 11, Issue 13, July 2016.

[8] Md Tarik, Amandeep Singh, " Intrusion Detection System using K2 Self Learning Algorithm and Open Attacking Platform", International Journl of Scientific & Engineering Research, Volume 6, Issue 3, March 2015.

[9] Sable Ankita, Poonam Kamble, Dhanvate Bhagyshri, "Intrusion Detection System Using K2 Algorithm", Imperial Journal of Interdiscipilanry Research, Volume 3, Issue 5, 2017.

[10]Anthony Paul Raj A, Kani Mozhi J K, " Bayesian Networks for Intrusion Detection Systems using K2 algorithm", International Journal of Advance Research in Science and Engineering, Volume 7, Issue 1, January 2018.

[11]Mradul Dhakar, Nisha Chaurasia, Akhilesh Tiwari, " Analysis of K2 based Intrusion Detection System, Current Research in Engineering Science and Technology, February 2014.

[12] Mehdi Hosseinzadeh Aghdam, Peyman Kabiri, " Feature Selection for Intrusion Detection System Using Ant Colony Optimization", International Journal of Network Security, Volume 18, Issue 3, PP. 420-432, May 2016.

[13] Zainab Mohammmad Abdullah, Ayad Imad Atallah, " Intrusion Detection and Classification Using Ant Colony Optimization Algorithm", Iragi Journal of Statistical Sciences, 2013.

[14]Kanaka Vardhini K, Dr. Sitamahalakshmi T, " Enhanced Intrusion Detection System Using Data Reduction : An AntColony Optimization Approach", International Journal of Applied Engineering Research, Volume 12, Issue 9, PP. 1844-1847.

[15]Monther Aldwairi, Yaser Khamyseh, " Application of Artificial Bee Colony for Intrusion Detection Systems", Security and Communication Networks, 2012.

[16]Monika Gupta, "Intrusion Detection System based on SVM and Bee Colony", International journal of Computer Application, Volume 111-No 10, February 2015.

[17]Amudha P, Abdul Rauf H, " A Study on Swarm Intelligence Techniques in Intrusion Detection", Computaional Intelligence & Information Security, 2012.

[18]Seyed Mojtaba Hosseini Bamakan, Behnam Amiri, " A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", Information Technology and Auantitative Management, 2015.

[19]Marjan Kuchaki Rafsanjani, Laya Aliahmadipour, " A Hybrid Intrusion Detection by Game Theory Approaches in MANET", Indian Journal od Science and Technology, Volume 5, February 2012.

[20]Saranya J, Lekha J, " A Review On Intrusion Detection Systems in Wireless Sensor Networks using Game theory Approach", International Journal of Contemporary research in Computer Science and Technology, Volume 1, Issue 6, September 2015.

[21]Paramasivan B, Mohaideen Pitchai, " Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks", twork Security and Cryptography, 2011.

