International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 5363-5375

http://www.ripublication.com

A Review on Anomaly Detection in MANET using Antnet Algorithm

[#1]Soma Pal, [2]Karthi Ramachandran,[3] Surender Dhanasekaran, [4]Immanuel Dinesh Paul &[5]Amritha

[#1, 2, 3, 4&5]Assistant Professor, SOE,
Vel Tech University
Avadi-VelTech Road, Chennai, India
[#1]somapal@veltechuniv.edu.in, [2]grkarthi@veltechuniv.edu.in,
[3]dsurender@veltechuniv.edu.in, [4]immanueldp@veltechuniv.edu.in
&[5]amirthac56@gmail.com

Abstract

Mobile Ad-hoc NETwork are decentralized wireless network. Therefore, identifying and tracing a malicious host is a difficult task, as the topology of the network is not fixed. Hence forth, malicious host can easily interrupt a specific route for which it is one of the forming nodes in the communication path. Several methods have been proposed to detect such malicious node using static baseline profile. Since the topology of a specific MANET dynamically changes, mere use of static baseline profile will not be efficient. Therefore, in this paper, we propose an algorithm which uses Antnet algorithm and Ad-hoc on demand distance vector (AODV) routing protocol for anomaly detection. Antnet approach belongs to the class of routing algorithm inspired by the basic behavior of ant colonies in locating and storing food.

Keywords: MANET, Anomaly Detection, AODV, Topology.

1. Introduction

Wireless networking has grown rapidly though wireless network provides many advantages, successful connectivity is still a challenging problem and many protocols have been proposed in order to overcome this problem [1] [2]. MANET is receiving more attention as part of the next – generation network technologies [3]. These networks are constructed by using mobile and wireless hosts with minimum or no central control point of attachment, such as a base station. These networks can be useful for various applications such as disaster and military applications, and

entertainment industry etc. As in MANET, topology keeps changing there is no centralmanagement entity, hence routing among various nodes for a particular application must be done in a collaborative manner. Thus, it is unrealistic to introduce an authentication server that employs conventional cryptographic schemes to secure the network against attacks from malicious hosts. Typical types of attacks in MANET includes eavesdropping, address spoofing, forged packets and denial of service (DOS).

In most of the secure routing protocols [4] [5] [6] key based cryptographic technologies are being applied to meet the increasing demands for MANET security. However, besides topology issue, these methods cannot protect the network from attacks by malicious node that manages to acquire the network key. Therefore, other security methods are required to be developed. If a well-known attack in the TCP/IP protocol stack is launched in a MANET, then it is possible to protect the network by using conventional techniques [7]. However, if the attacker maliciously uses a specific routing protocol of the MANET, prevention becomes remarkably difficult. In such a case, it is almost impossible to recognize where and when the malicious node appears. Thus, the attack detection at each node becomes necessary.

The two techniques for finding malicious attack are classified as misuse detection and anomaly detection. Misuse detection techniques are signature-based analysis where attacks are identified by comparing their input traffic signature with signatures extracted from known attacks at the network routers. Whereas anomaly detection technique quantitatively defines a base line profile for a normal system activity, and any deviation from base line is treated as a possible system anomaly. If the traffic signature is known, attack detection can be done by misuse detection technique. But for certain attack for which the type or the traffic signature is not known this technique becomes inadequate. Thus, such kind of attack can be detected by the later method. In anomaly detection, even when the traffic signature is not known, if the base profile of a network is delineated a priori, then the abnormalities can be recognized [8]. The effectiveness of such detection methods has been tested via various experiments for wired network.

For MANET, since the network condition keeps changing, pre-extracted network information or state may not correctly represent the state of current network. This indeed influences the accuracy of anomaly detection. Thus, an anomaly detection scheme based on Antnet algorithm is been proposed. Antnet algorithm works on the principle of Ant Colony Optimization (ACO). ACO is a paradigm for designing meta-heuristic algorithm for combinatorial optimization problems. This was initially proposed Marco Dorigo in 1992 aiming to search for an optimal path in a graph based on the behavior of ants seeking a path between their colony and source of food. The remaining paper is organized as follows-Conventional Detection Scheme, Overview of AODV, Proposed detection scheme.

2. Conventional Detection Schemes

2.1. Secure schemes for Routing Procedure

To enhance the security in MANETs various secure ad hoc routing protocols have been proposed.For example, the secure AODV (SAODV), which uses signed routing messages, is proposed to add security to AODV and A-SAODV is a mild implementation of SAODV that uses the RSA as an asymmetric cryptographic algorithm and the SHA1as a hash algorithm. A survey conducted by Yih-Chun and Perrig shows the various secure routing protocols and their drawbacks and advantages. They also proposed a secure on demand ad hoc network routing protocol (Ariadne)[3], prevents the compromises modes of tampering with the uncompromised routes, and the secure efficient ad hoc distance (SEAD),which is a secure routing protocol, using efficient one way hashing functions and not using asymmetric cryptographic operations. In addition, Zhou and Haas proposed a distributed certification authority mechanism in which the authentication uses threshold cryptography. In a MANET is divided into clusters, and a certification authority is appointed to each cluster. Here, a method called key pre-distribution (KPD) scheme is applied. In authenticated routing for ad hoc networks (ARAN) is proposed by using public-key cryptographic mechanisms bases on the AODV. These methods can only guard against external attacks. However, the internal attacks mounted by the malicious or compromised hosts may still have a severe impact on the network performance, as well as on the connectivity among the nodes in the targeted MANET.

2.2. Network monitoring based attack detection

In addition to the aforementioned techniques, attack detection by network monitoring, has also been proposed. Kachirski and Guha proposed a method that detects attacks by employing distributed mobile agents. Network monitoring nodes are selected to be able to collect all the packets within a cluster, and the decision agents in the nodes are used to detect and classify the security violations. The concern of this method is that the monitoring nodes will consume a large amount of energy. Vigna et al, detects attacks by placing AODV - based State Transition Analysis Technique (AODVSTAT) sensors within the network and by either observing solely contiguous nodes or trading information with other sensors. However it is necessary to deploy a large number of AODVSTAT sensors on the nodes for detecting a varied range of attacks. In addition a large number of UPDATE messages may cause an overwhelming congestion in the network.

2.3. Anomaly Detection

Huang et al, proposed a method in which the packet flow is observed in each node. In this, method, 141 features that are both traffic and topology related are defined. Huang et al suggested an anomaly detection mechanism with interrelation between features. Moreover, they constructed an extended file state automation (EFSA) according to the specification of the AODV routing protocol, envisioned normal condition modeling, and detected attacks with both specification based and anomaly-based detection schemes. In specification based detection the attacks were detected as deviant packets from the conditions defined by EFSA. In addition, in anomaly detection, the normal conditions are defined as the baseline with which the condition of EFSA and also the amounts of transition statistics are compared.

The deviations from those conditions are used to detect the potential attacks. For determining the baseline profiles, in both methods the training data are extracted beforehand from the same network environment where the test data are applied. However, we note that the MANET topology can rather easily be changed and the difference in network states grows larger with time. Furthermore, these methods cannot be applied to a network where the learning phase has been conducted in another network.

Sun et al proposed an anomaly detection method in which mobility is considered. This method computes the recent link change rate (LCRrecent) and can select the training data, the link change rates of which have the smallest Euclidean distance to LCRrecent. However, the change of network states can be caused only by mobility; it may also occur due to the sudden participation and disappearance of nodes in a MANET. When the nodes in the current MANET differ from those in the training data, the defined baseline profile cannot express the current network state. As a result, these methods are rendered inadequate and considered difficult in a MANET environment. To solve this problem a normal state needs to be defined by using the data reflecting the trend of the current situation and this leads to the idea of updating the learning process within a time interval. By doing so the attack detection can adaptively be conducted even in changing network scenario.

3. Overview Of AODV

The AODV is a reactive routing protocol in which the network generates routes at the start of communication. Each node has its own sequence number and this number increases whenever a link changes. According to this sequence number, each node judges whether the channel information is recent. Figure.1 illustrates the route discovery process of the AODV. In this figure, node S attempts to establish a connection to destination D. First, the source node S refers to the route map at the start of the communication.

In the case where there is no route to destination node D, it sends a route node request (RREQ) message by using broadcasting. The RREQ ID increases by one every time, node S sends an RREQ message. Nodes A and B which has received the RREQ message, generate and renew the route to its previous hop. They also evaluate if this is a repeated RREQ message and accordingly discard it. If node A and B have a valid route to destination D, then they send an RREQ message using broadcasting. The exchange of route information will be repeated until an RREQ message reaches node D. When node D receives the RREQ, it sends an RREP message to node S. When node S receives the RREP message, a route is established.

In case of multiple RREPs received, a node selects an RREP message, the destination sequence number (Dst_Seq) of which is the largest among all the previously received RREPs. However if the Dst_Seqs were the same, then it will select the RREP message whose hop count is the smallest.

In Fig.2, when node B detects a disconnection of route, it generates route error (RRER) message and put the invalid message of node D into its list and sends RRER to node A. When node A receives a RRER message, it refers to its route map and the

current list of RRER messages. If there was a route to the destination of node D included in its map and the current list of RRER message to node S. This way, the RRER message can finally be sent to the source node S.

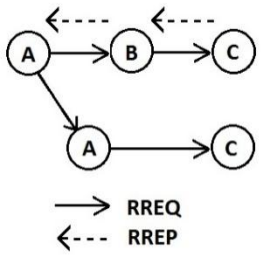

Figure-1: Route - discovery process on AODV

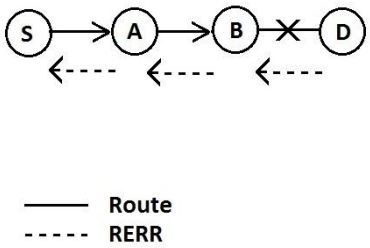

Figure-2: Transferring RERR messages on AODV

3.1 Routing Tables

Each routing table entry contains the following information:

1. Destination
2. Next hop
3. Number of hops
4. Destination sequence number
5. Active numbers for this route
6. Expiration time for this route table entry

Expiration time, also called lifetime, is reset each time this route has been used. The new expiration time is the sum of the current time and a parameter called active route timeout. This parameter is also called as route catching timeout, is the time after which the route is considered as invalid and so the nodes not lying on the route determined by RREPs delete their reverse entries. If active route timeout is big enough route repairs will maintain routes.

3.2. Control Messages

3.2.1. Routing Request

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains the following fields:

Source Address	Request ID	Source Sequence No	Destination Address	Destination Sequence No	Hop Count

The request ID is incremented each time the source node sends a new RREQ, so the pair (source address, request ID) identifies a RREQ uniquely. On receiving a RREQ message each node checks the source address and the request ID. If the node have already received a RREQ with the same pair of parameters the new RREQ packet will be discarded.

3.2.2. Routing Reply

If a node is the destination, or has a valid route to the destination, it unicast a route gets lost, a route error message (RERR) generated to notify the other nodes on both sides of the link of the loss of this link.

3.2.3. Hello Messages

Each node can get to know its neighborhood by using local broadcasts, so-called HELLO messages. Nodes neighbors are all the nodes that it can directly communicate with. Although AODV is a reactive protocol it uses these periodic HELLO messages to inform the neighbors that the link is still alive.

3.3. Sequence Numbers

3.3.1. Counting To Infinity

The core of the problem is that when X tells Y that it has a path somewhere, Y has no way of knowing

Whether it itself is on the path- as Tanenbaum notes. So if Y detects a link to Z is broken, but X still ha "valid" path to Z, Y assumes X in fact does have a path to Z. So X and Y will start updating each other in a loop, and the problem named "counting to infinity" arises. AODV avoids this problem by using sequence numbers for every route, so Y can notice that X's route to Z is an old one and is therefore to be discarded.

3.3.2. Time Stamping

The sequence numbers are the most important feature of AODV for removing the old and invaluable

Information from the network. They work as a sort of timestamps and prevent the AODV protocol from the loop problem. The destination sequence number for each destination host is stored in the routing table, and is updated in the routing table when the host receives the message with greater sequence number. The host can change its own destination sequence number if it offers a new route to itself, or if some route expires or breaks.

Each host keeps its own sequence number, which is changed in two cases:

- Before the node sends RREQ message, its own sequence number is incremented.

- When the node responds to a RREQ message by sending a RREP-message, its own sequence number becomes the maximum of the current sequence number and the node's sequence in the receivedRREQ message.

The reason is that if the sequence number of already registered is greater than that in the packet, the existing route is not up-to-date. The sequence numbers are not changed by sending HELLO messages.

3.3.3. Route Discovery

Route discovery process starts when a source node does not have routing information for a node to be communicated with. Route discovery is initiated by broadcasting a RREQ message. The route is established when a RREP message is received. A source node may receive multiple RREP messages with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. Fresh information.

3.3.4. Reverse Path Setup

While transmitting RREQ messages through the network each node notes the reverse path to the source. When the destination node is found the RREP message will travel along this path, so on more broadcasts will be needed. For this purpose, the node on receiving RREQ packet from a neighbor records the address of this neighbor.

3.3.5. Forward Path Setup

When a broadcast RREQ packet arrives at a node having a route to the destination, the reverse path will be used for sending a RREP message. While transmitting this RREP message the forward path is setting up. One can say that this forward path is reverse to the reverse path. As soon as the forward path is built the data transmission can be started. Data packets waiting to be transmitted are buffered locally and transmitted in a FIFO-queue when a route is set up. After a RREP was forwarded by a node, it can receive another RREP. This new RREP will be either discarded or forwarded, depending on its destination sequence number:

1. If the new RREP has a greater destination sequence number, then the route should be updated and RREP is forwarded.
2. If the destination sequence numbers in new and old RREP are the same, but the new RREP has a smaller hop count, this new RREP should be preferred and forwarded
3. Otherwise all later arriving RREP will be discarded.

3.3.6.Link Breakage

Because nodes can move, link breakages can occur. If a node does not receive a HALLOW message from one of his neighbors for specific amount of time called HALLOW interval, then

1. The entry for that neighbor in the table will be set as invalid.

2. The RRER message will be generated to inform other nodes of this link breakage RRER messages inform all sources using a link when a failure occurs.

4. Classification Of Attacks

The malicious nodes can misuse the AODV by forging source IP address, destination IP address, RREQ IDs, hop counts, Destination sequence numbers(Dst_Seqs), Source sequence numbers (Src_Seqs) and also by flooding the network with routing packets. According to prior works, we can classify the attacks against AODV into routing disruption attacks and resource consumption attacks.

1. Routing Disruption Attacks: These attacks interrupt the establishment of a route or destroy an Existing route. The most common attacks of this type are the modification of RREP (same as the Blackhole attack) and the modification of RREQ.

2. Resource Consumption Attack: This attack wastes resources of a specific node and the network as a whole. The most common attack of this type is malicious flooding.

4.1. Merits Of AODV

The AODV routing protocol does not need any central administrative system to control the routing process. Reactive protocols like AODV tend to reduce the control traffic messages overhead at the cost of increased latency in finding new routes. AODV reacts relatively fast to the topological changes in the network and updates onlythe nodes affected by these changes. The HALLOW messages supporting the routes maintenance are range limited, so they do not cause overhead in the network.
The AODV routing protocol saves storage space as well as energy. The destination node replies only once to the first request and ignores the rest. The routing table maintains at most one entry per destination. If a node has to choose between two routes, the up to date route with a greater destination sequence number is always chosen. If routing table entry is not used recently, the entry is expired. A not valid route is deleted: the error packets the error packets reach all nodes using a failed link on its route to any destination.

4.2. Drawbacks Of AODV

It is possible that a valid route is expired. Determining of a reasonable expiry time is difficult, because the nodes are mobile and sources, sending rates may differ widely and can change dynamically from node to node. Moreover, AODV can gather only a very limited amount of routing information; route learning is limited only to the source of any routing packets being forwarded. This causes AODV to rely on a route discovery flood more often, which may carry significant network overhead. Uncontrolled flooding generates many reluctant transmissions which may cause so-called broadcast storm problem.

The performance of the AODV protocol without any misbehaving nodes is poor in larger networks. The main difference between small and large networks is the average path length. S long path is vulnerable to link breakages and requires high control overhead for its maintenance. Furthermore as a size of network grows, various performance metrics begin decreasing because of increasing administrative work, so called administrative load.

AODV is vulnerable to various kinds of attacks because it is based on the assumption that all nodes will cooperate. Without this cooperation, no route can be

established and no packet can be forwarded. There are two main types of uncooperative nodes: malicious and selfish. Malicious nodes are either faculty and cannot follow the protocol, or are intentionally malicious and try to attack the network.Selfishness is non co-operation in certain network operations, i.e. dropping of packets which may affect the performance, but can save the battery power.

5. Proposed Method

5.1 Existing Scenario

The techniques for detecting the malicious attacks are usually classified into two categories, namely misuse detection and anomaly detection. In misuse detection, the method of using a signature-based analysis is widely implemented. In this method, the analyses are identified by comparing the input traffic signature with the signatures extracted from the known attack at the network routers. Anomaly detection is a technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable by using misuse detection, the method is rather inadequate. In such cases, those attacks can only be detected by using anomaly detections methods. In anomaly detection even when the traffic signature is unknown, if the baseline profile is pre-extracted and then applied to the same network. However, for MANET's, since the network conditions are likely to change, the pre-extracted network state may not correctly represent the state of the current network. This problem indeed influences the accuracy of the anomaly detection method.

5.2. Proposed Method

In this paper, we propose an anomaly detection scheme based on Antnet algorithm. The MANET hosts are mobile on their own so that the MANET environment is dynamically changing. A dynamic learning method is based on principle of Ant Colony Optimization (ACO). We conduct network simulations with different scenarios as a case study that concerns one of the most popular MANET routing protocols, i.e., the ad hoc on-demand distance vector (AODV). The simulation results (fig: 4& 5) of the network simulator2 (ns-2) demonstrate the effectiveness of the proposed technique, regardless of the number of nodes in the considered MANET.

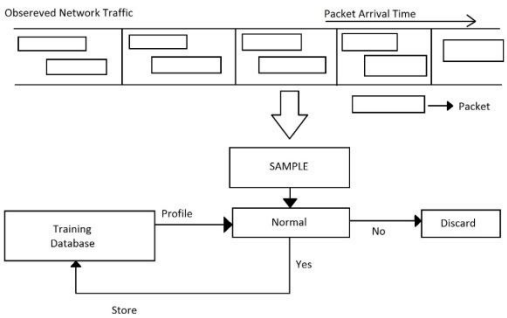

Figure-3: Flowchart showing learning and evaluation process

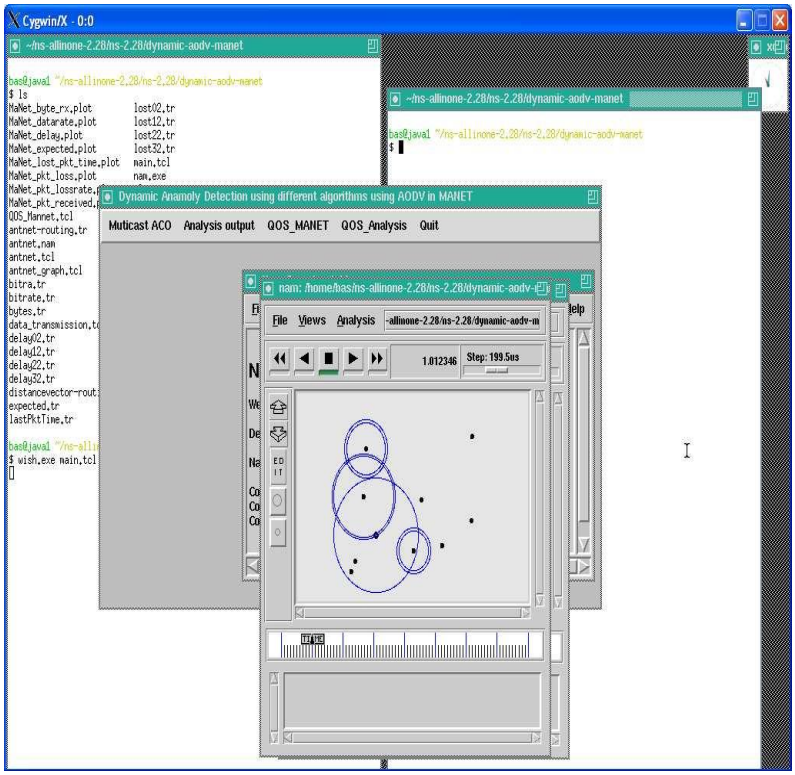

Figure-4: Quality of Service in MANET

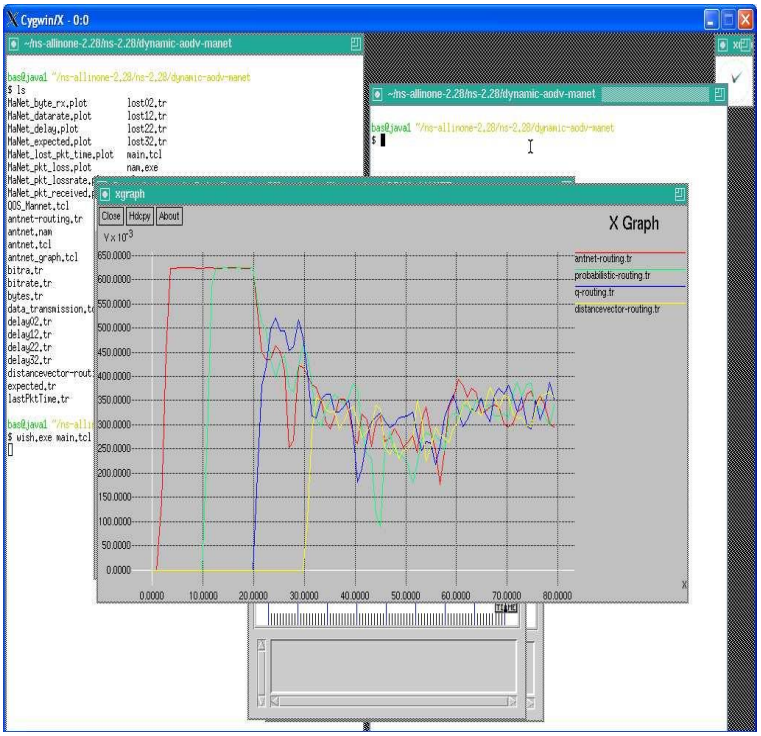

Figure-5: The algorithm performance analysis

5.3. Anomaly Detection

We first introduce the features that are essential for our anomaly detection scheme, and then delineate the module of the detection scheme based on the projection distances. A set of computational concurrent and asynchronous agents (a colony of ants) moves through states of the problem corresponding to partial solutions of the problem to solve. They move by applying a stochastic local decision policy based on two parameters, called trails and attractiveness. By moving, each ant incrementally constructs a solution to the problem. During the construction phase or on completion of a solution, ant evaluates the solution and modifies the trail value on the components used in its solution. This information will direct the search of the future ants

Definition of Features:

Each node observes its own traffic and uses a time slot to record the number of packets (messages) according to their types. The statistics for a time interval define a state in the network are as follows:

- Path Finding Features
- Path Abnormality Features
- AODV Characteristics Feature

These features are implemented in an Ant-colony optimization (ACO) Algorithm for MANET Environment which is the proven method for identification, detection and efficient routing. The AODV parameters are simulated using ACO in MANET Environment.

5.4. Defining Normal And Malicious Behaviour Of A Node

The vulnerabilities discussed in previous section provide intruder a way to compromise legitimate nodes and make them malicious in nature. In this section, an attempt has been made to define a normal and malicious behavior of a node. And the normal and the malicious behavior of a node described can be easily understood by the algorithm shown in figure 6.

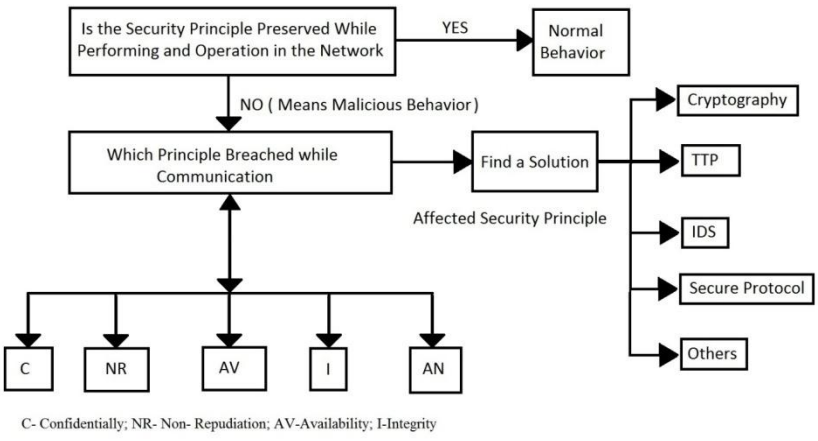

Figure-6: Defined Algorithm for Normal & Malicious Behavior of a node

5.5. Antnet Algorithm

The goal of every routing algorithm is to direct traffic from sources to destinations optimizing at the same time several measure of network performances as throughout (correctly delivered bits per time unit), packet delays and resources utilization. The general problem of determining an optimal routing algorithm can be stated as a multi objective optimization problem in a non-stationary stochastic environment. Information propagation delays, and the difficulty to model the whole network dynamics under arbitrary traffic patterns, make the general routing problem intrinsically distributed. Routing decisions can only be made on the basis of local and approximate information about the current and the future network states.

The adaptive routing algorithms proposed in this paper, called ANTNET, are distributed and mobile multi-agent systems well matching the above characteristics of the general routing problem. Real ants have been shown to be able to find shortest paths using a stochastic decision policy based only on local information represented by the pheromone trail deposited by other ants. Algorithms that take inspiration from ants' behavior in finding shortest paths have recently been successfully applied to several discrete optimization problems. In ant colony optimization each one of a set of concurrent artificial ants makes use of a stochastic local search strategy to build a solution to the combinatorial problem under consideration. The whole set of ants collectively search for high quality solutions by a cooperative effort mediated by indirect communication of information on the problem structure they collect while building solutions. Similarly, in ANTNET, artificial ants (agents) collectively solve the routing problem by a cooperative effort in which stigmergy, mediated by the network nodes, play a prominent role.by using a stochastic routing policy based on local (public) and private information ants concurrently and asynchronously explore the network and collect useful information. While exploring, the ants adaptively build probabilistic routing tables and local models of the network status using indirect and non-coordinated communication of the information they collect.

5.5.1. Process Algorithm

Step 1: Initial Path Discovery using AODV

Step 2: Anomaly Detection using ANTNET Algorithm (ACO) Step 3: Rediscover Path Based on ACO

6. Conclusion

For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. Thus, in this paper, an anomaly detection system based on Antnet algorithm which works along with AODV routing protocol for MANET has been suggested. And during simulation to differentiate an attack state from normal state, we have defined features based on the characteristics of these attacks. As most of the relations among these nodes are fixed, this project shows that it is possible to define generic network rules aimed to automatically detect selected network anomalies.

7. References

[1] " A network based anomaly detection system using multiple network features" Y Waizumi, Y Sato and Y Nemoto, in 3rd Int. Conf. WEBIST, Mar 2007

[2] " Cross - feature analysis for detecting ad- hoc routing anomalies" Y huang, W Fan, W Lee and P Yu in Proc. 23rd ICDCS, May 2003

[3] "A Survey of Performance based Secure Routing Protocols in MANET "HariomSoni, Asst. Prof. PreetiVerma, IJARCET, ISSN: 2278 - 1323, Volume 2, Issue 1, Jan 2013

[4] "Performance Comparison of Secure Routing Protocols in Mobile Ad-Hoc Networks" AshwaniGarg, VikasBeniwal, IJCAIT, ISSN: 2278-7720, Vol. I, Issue II, Sep 2012.

[5] "Routing security in wireless Ad-Hoc networks", Hongmei Deng, Wei Li, Dharma, P. Agarwal, IEEE Communications Magazine, Oct 2002.

[6] "A Self-adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks", Satoshi Kurosawa†, Hidehisa Nakayama†, Nei Kato†, Abbas Jamalipour‡, and Yoshiaki Nemoto†Graduate School of Information Sciences, Tohoku University Aoba 6-3-09, Aramaki, Aoba-ku, Sendai, Miyagi, 980-8579 Japan

[7] "Intrusion Detection Techniques for Mobile Wireless Networks" Yongguang Zhang, Wenke Lee, Yi-An Huang, Mobile Networks and Applications,(2003) 1-16

[8] "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Yih-Chun Hu∗ And Adrian Perrig , David B. Johnson, Springer Science + Business Media, Inc. Manufactured in The Netherlands. 2005

[9] "Securing Ad hoc Routing Protocols", Manel Guerrero Zapata and N. Asokan.