Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

Asian Journal of Scientific Research 7 (2): 199-207, 2014
ISSN 1992-1454 / DOI: 10.3923/ajsr.2014.199.207

A Dynamic Knowledge Method In Opposition To Anomaly Host in AODV Based MANET

[1]T. Kumanan and [2]K. Duraisamy
[1]Research Scholar, Anna University of Technology, Coimbatore, India
[2]Dean/Academic, K.S.R. College of Technology, Tiruchengode, India

Corresponding Author: T. Kumanan, Research Scholar, Anna University of Technology, Coimbatore, India

ABSTRACT

A mobile *ad hoc* network (MANET) is an infrastructure less network. MANET contains collection of mobile devices those are connected by wireless. Each node in a MANET is liberated to move autonomously in any direction and will hence change its links to other devices repeatedly which may lead to network performance degradation as well as some security issues. As the MANET has no centralized host, the node in the MANET deviates from what is normal behavior of the node in MANET. That kind of node is called as Anomaly node which may perform some malicious actions against whole network. The Anomaly node could not be detected easily due to the dynamic topology of the MANET. To overcome this issue, propose an ADAODV (Anomaly Detective AODV) which uses Dynamic knowledge method to detect the anomaly node present in the MANET. The Simulation is done by using NS2 Simulator, which shows, the ADAODV detect that Anomaly node present in the network and also improves the overall performance of AODV in the presence of malicious node.

Key words: MANET, anomaly detection, dynamic knowledge method, AODV

INTRODUCTION

Mobile *ad hoc* networks (MANETs) can initialize as a cluster of huge number of mobile nodes form short-term network without any existing infrastructure network or central access point. Every node acts as host as well as router in the network and it must hence is enthusiastic to forward packets to some other nodes. The MANET has some personalities: Node mobility, dynamic topology, self organizing capability and provides large degree of freedom to make it completely different from other network.

MANETs have different security goal, they are:

- Authentication
- Integrity
- Confidentiality
- Non-Repudiation

MANETs faces additional problems and challenges during routing when compared to traditional wired network routing with fixed infrastructure. In such environments routing is motivated by restrictive factors such as continuously changing topologies, high energy consumption, low

bandwidth and elevated error rates. Mostly existing routing protocols follow two special approaches to deal with inherent uniqueness of *ad hoc* networks, namely the table driven and source initiated on-demand approaches.

The routing protocols for MANET are classified into two main categories. They are reactive and proactive protocols (Raj and Swadas, 2009). Routing protocols under the category of proactive protocol, exchange routing information with other nodes for the purpose of each node always have a valid route to all other nodes in MANET. On the other hand, reactive protocol exchanges its routing information only when required. By using this kind of reactive protocol, a node tries to find the route to the intended destination, only when it has the packet to send to that destination (Perkin s and Royer, 1999). According to the MANETs researcher, designing and progress of secure routing is difficult task in distributed communication environments.

Mobile *ad hoc* networks are susceptible to various attacks includes black hole attack, Reply attack, location disclosure attack and Denial of service attack (Raj and Swadas, 2009). In this study, to design a method for detect anomaly or misbehaving node: ADAODV which separates malicious node from the network. In this each and every node stores the destination sequence number in the incoming RREP packets and calculates the threshold value (Kurosawa *et al*., 2007) to evaluate the dynamic training data in every time intervals. By using proposed technique, the nodes participating in the transmission recognize that, one of its neighbors is anomaly node. Then that node is not allowed to participate in packet forwarding.

AODV (*AD HOC* ON-DEMAND DISTANCE VECTOR)

Ad hoc On-demand Distance Vector Routing (AODV) is an enhancement on the DSDV algorithm. Creating routes in AODV, it minimizes the amount of broadcasts though on-demand as opposed to DSDV (Perkins and Bhagwat, 1994) that maintain the entire routes list.

In this study identify a path to the destination; the source node broadcast a route request packet to its neighbors in turn broadcast till it reaches an intermediary node that has recent route information about the destination (Fig. 1). Already seen node discards a RRP (Route Request Packet). During path conformation the RRP send sequence numbers to make sure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, that reply with only the latest information.

Node forwards process a RRP to its neighbors; it also maintains record in its tables the node from which the original copy of the request came. This kind of data is used to build the turnaround path

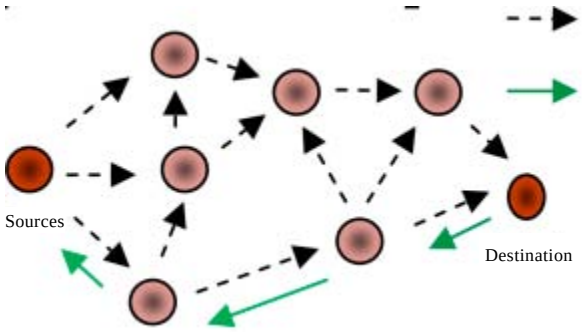

Fig. 1: Routing discovery in AODV

for the RRP. AODV uses symmetric links because the RRP follows the turnaround path of RRP. Because route replay packet traverses back to the sender (Fig. 1), the nodes along the path enter the forward route into their tables.

Any movement in source node then it reinitiate route discovery to the destination node. If only one intermediate nodes moves then they moved node's neighbor realizes the failure link and sends a failure notification for link to its upstream neighbors to till it reaches the source upon which the source can reinitiate route discovery if needed.

ANOMALY DETECTION

Anomaly detection, also related to outlier detection, it relate to identify patterns from the specified; data set that do not conform to recognized normal performance. Thus that type of detected patterns is called anomalies, frequently translates to critical and also actionable information in different functional domains. Anomalies are also referred to as outliers, aberrant, intruders, deviation, surprise, peculiarity, etc.

The framework of abuse and network intrusion detection, the interesting objects are often not rare objects particularly but unexpected bursts in activity. The outlier of this prototype doesn't hold to the general statistical explanation as unusual object, generally unsupervised methods has lot of outlier or anomaly detection methods will fail on such data, unless it has been aggregated properly. In place of CAA (Cluster Analysis Algorithm) may able to identify the some micro clusters frame by these rules. Already there are three broad categories for anomaly detection process. UADT (Unsupervised Anomaly Detection Techniques) identify the anomalies node in an unnamed test data or record set under the premises that the bulk of the instances in the data set are normal by looking for instances that seem to fit minimum to the remainder of the data or record set. SADT (Supervised Anomaly Detection Techniques) need a record set that has been named as "normal" and "abnormal" and requires training a classifier. Semi-supervised Anomaly Detection Techniques (SsADT) use normal training data or record set to assemble a representation as model of normal behaviors for nodes. Finally testing the possibility of a test instance to be generated by the learnt model many anomaly detection techniques create a model representing normal behavior from a given normal trained record set.

From the Fig. 2, in this study to know the concept of anomalies. In this context, the misbehaving nodes (i.e.,) the node which has abnormal behavior is called as anomaly. In this

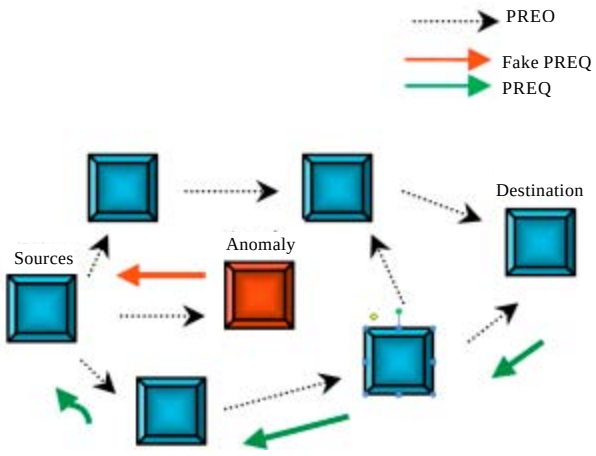

Fig. 2: Anomaly detection

study, Fig. 2 explains malicious node sending fake route reply itself as it have the shortest path to all other nodes in the environment. By doing this, the malicious node can divest the traffic from the source node.

ANOMALY DETECTIVE AODV (ADAODV)

AODV uses a destination seq_no for each route entry. It is set by destination node. If there exist two routes to the destination means, requesting node is required to select the one with greatest seq_no. Maintaining seq_no. is very much useful to avoiding routing loops.

The node which uses the ordinary AODV receives the RREP packet first check the sequence no in its routing table. The node accepts the RREP packet only it has the seq_no higher than the seq_no in its routing table. But in this proposed ADAODV the node additionally checks the seq_no is higher than the threshold value. Routing table have the threshold value, it's dynamically updated in every time interval. This technique is called as dynamic knowledge method.

As shown in Fig. 3. If the seq_no is higher than the threshold value, that node is suspected to be anomaly and add that node in to the anomaly list. When the node detected an anomaly, it immediately sends the warning ticket to its neighbors.

The warning ticket has the anomaly list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded.

Further, if any node receives the RREP packet, it checks the anomaly list to verify whether the RREP is from the anomaly node. If it is, no processing is done for the RREP. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the warning ticket. The malicious nodes send nonstop replies, so that kind of nodes are blocked, which outcome in less Routing overhead. Furthermore, unlike AODV, if the node is found to be malicious, the routing table for that node is not updated, nor the packet is forwarded to another node.

The threshold value is dynamically updated in the routing table by using the data collected dynamically for the particular time interval. The system could not adapt the changing environment when the initial training information or data were used. The threshold value is calculated by the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet. When a new node receives a RREP packet the threshold value is update according to the time interval. As a new node receives a RREP for the first time, it gets the updated value of the threshold. So the proposed design not only detects the anomaly node but tries to prevent the network further, by updating threshold which reveals the real changing

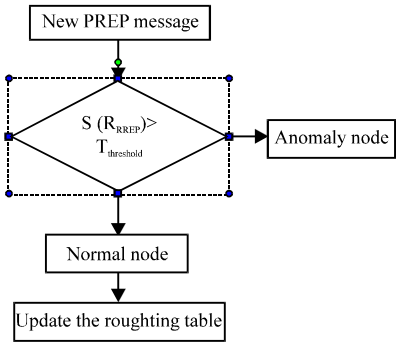

Fig. 3: Flow chart for ADAODV

environment. Other nodes are also updated about the malicious act by a Warning ticket and they react to it by isolating the anomaly node from network.

THRESHOLD VALUE CALCULATION

The mobile nodes in the MANET are participating in the transmission. For that it has discovered the route to reach the destination. Each and every node updates its routing table with the new route information as well as sequence no. The RREP sequence no is extracted from the routing table and stored into the list S (i):

$$S(i) = \{S_1, S2, S3 \ldots S_n\}$$

The originating node calculates the threshold value by selecting the greater value in the above list. It can be expressed as:

$$T_{threshold} = S(Ni), \text{ where } Ni=\max\{S(i)\}, i\_1 \text{ to } n$$

The source node discovers the route to its intended destination by broadcasting RREQ message. After that it receive RREP message with the route to reach the destination. The originator accepts the RREP after checking the seq_no in RREP is greater than $T_{threshold}$. If it is not a greater value, then it doesn't accept the RREP and add that corresponding node into the anomaly list. The $T_{threshold}$ value is dynamically updated for particular time interval.

Let $S(R_{RREP})$ be the sequence no in incoming RREP packet. Then the system will detect the anomaly node by following method:

- If $S(R_{RREP}) > T_{threshold}$: Normal
- If $S(R_{RREP}) < T_{threshold}$: Anomaly

By doing this, system can separate the anomaly node present in the network. System has to repeat the event for each incoming RREP to detect the anomaly in the MANET environment.

EVALUATION OF ADAODV SIMULATION ENVIRONMENT

The simulation parameters are given in Table 1.

In this study use NS2 simulator to show the simulation results. In that system used mobility model as the Random way point mobility model. And the system (example) has 40 nodes moving in an area of 1500×1500 m. Each node independently moving within the area specified area.

Table 1: Simulation parameters

Parameters	Value
Simulator	NS2 (Ver. 2.28)
Simulation time (m sec)	20
No. of nodes	40
Routing protocol	AODV
Traffic model	CBR
Mobility speed (m sce^{-1})	300
Simulation area	1500×1500
Transmission range (m)	250

SIMULATION ANALYSIS

The snap shots obtained by executing Anomaly Detective AODV in ns2 simulator are shown below.

Figure 4 shows the textual output of Anomaly Detective AODV. While running the tcl file, first it produces the textual output and also generates the nam file. NAM is abbreviated from Network Animator which takes the nam file as the input and converts the textual output into animated output. When the execution of nam file, the following output is obtained. Figure 5 explains the simulation result of Anomaly Detective AODV. In my simulation, I have taken 40 nodes which are distributed in 1500×1500 simulation area. I have taken the node 0 as a source and the node 39 as a destination. Initially, perform Route discovery. The Route Reply (RREP) is analyzed to detect the anomaly node. Figure 6 differentiates the anomaly node present in the network by red color. Then the node never route its packet through this anomaly node. In this simulation study, system taken 3 nodes (n0, n5, n16) for analysis. At the time of simulation starts, the delay at each node is zero. After that it gets increased gradually as time increased as shown in Fig. 6. If compare the delay at these three nodes, system can identify the total delay in the network. By seeing the graph, you come to know node 16 has minimum delay when compared with remaining nodes.

Data delivery ratio means that the ratio of packets delivered to a particular node at particular instant of time. The no. of packets received for the sample period is calculated. And then the graph is plotted for the node n0, n5 and n16 which are shown in Fig. 7. While compare the packet

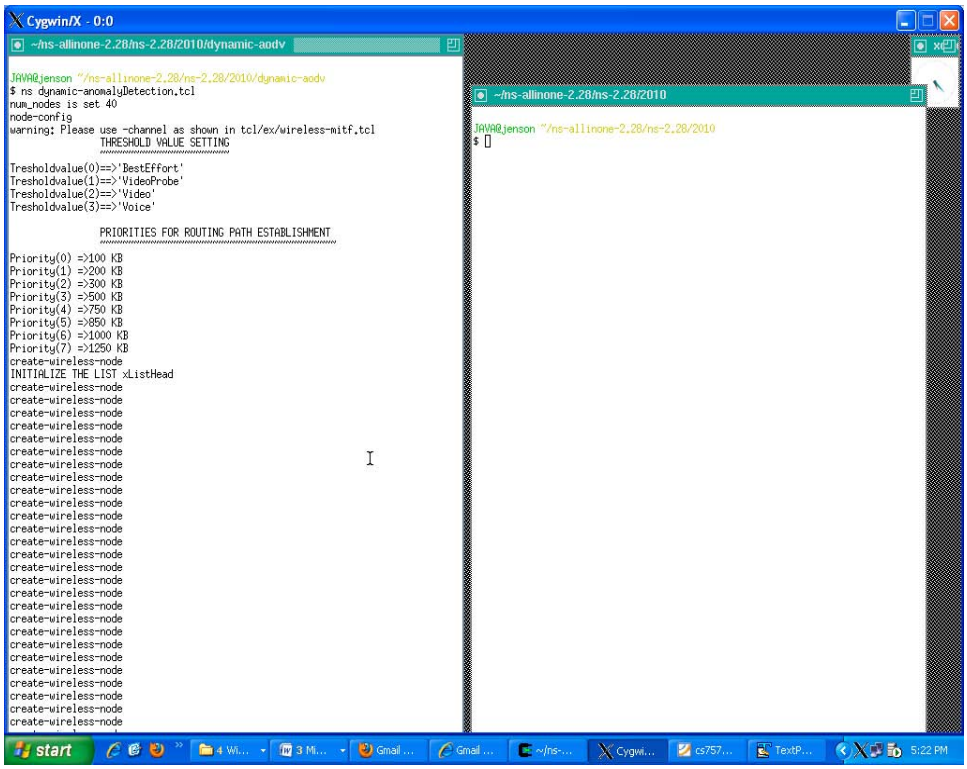

Fig. 4: Anomaly detection in dynamic AODV MANET

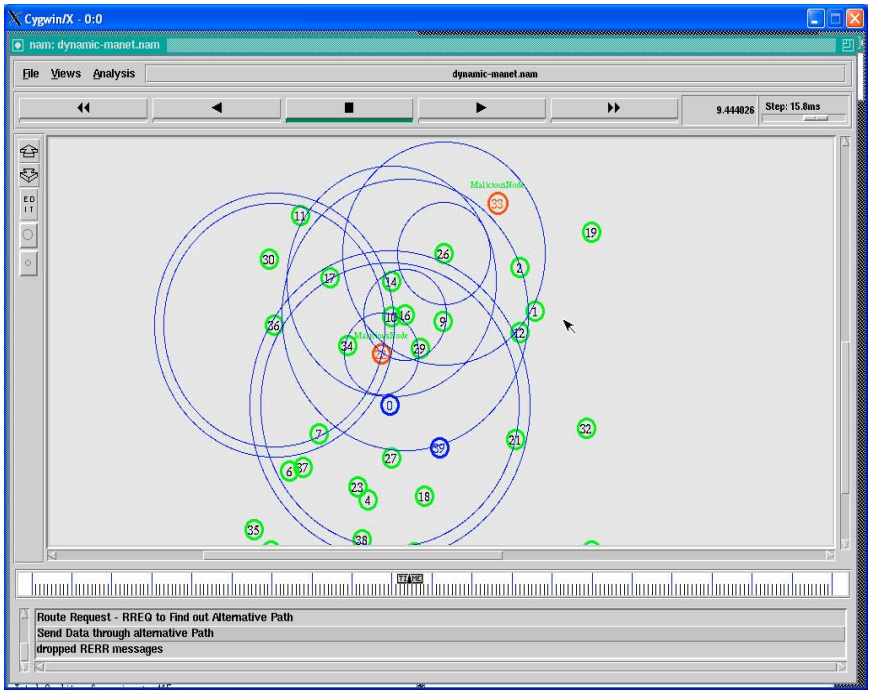

Fig. 5: Simulation result of anomaly detective AODV

Fig. 6: Delay at different nodes in anomaly AODV

delivery ratio for these three nodes network can identify the node 0 has the highest packet delivery ratio when compared with all other remaining nodes. Throughput is calculated by using the formula no. of packets received for the unit time. So, system analyzes the no. of packets received in particular time. Simulator take Time in X-axis and packets received in Y-axis. If system plot the graph between time and no. of packets received, system can examine the throughput of the Network. In this simulation the node n0 has highest throughput when compared with remaining nodes from Fig. 8.

Fig. 7: Data delivery ratio of anomaly detective AODV

Fig. 8: Throughput analysis of anomaly detective AODV

CONCLUSION

In this study, a new dynamic anomaly detection system for MANETs has been proposed. For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. The threshold value is dynamically updated in the routing table by using the data collected dynamically for the particular time interval. If the initial training data were used, afterwards the system could not adapt the changing environment. The proposed system demonstrates an effective performance in terms of high DRs and low FPRs against five simulated attacks, in addition to the scalability of the proposed scheme clarified by the simulation results obtained from two distinct network topologies of varying sizes.

FUTURE ENHANCEMENT

Future works will be focused on the various routing protocols in the MANET architecture. Although AODV is a major routing protocol in MANETs, new protocols are emerging, e.g., dynamic MANET on-demand protocol (DYMO). System will evaluate these protocols and give an analysis for the additional types of attacks to further improvement for the accuracy of the overall system. Yan *et al.* reported an interesting scheme with reference the context of studies on the intrusion detection system (IDS). The proposed IDS autonomic event analysis system that is represented by description logics allows inferring the attack scenarios and enabling the attack knowledge semantic queries. To cite a case, initially using this proposed system to detect attacks and then rigorously applying these IDS to analyze these attacks may bring about a reliable approach. Future works will comprise of feasibility studies on these more intelligent detection schemes in MANETs.

REFERENCES

Kurosawa, S., H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Network Security, 5: 338-346.

Perkins, C. and P. Bhagwat, 1994. Routing over multihop wireless network for mobile computers. Comput. Communi. Rev., 24: 234-244.

Perkins, C.E. and E.M. Royer, 1999. *Ad hoc* on-demand distance vector routing. Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., pp: 90-100.

Raj, P.N. and P.B. Swadas, 2009. DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. Int. J. Comput. Sci. Issues, 2: 54-59.