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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

An Efficient Dynamic Anomaly Scheme Routing for Mobile Adhoc Network

B.Saranya[1], Dr.E.MaryShyla[2]

Research Scholar, Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, India

Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for women, Coimbatore, India

ABSTRACT: Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless ad hoc network. While observing a sequence of packet losses in the network, whether the losses are caused by link errors only, or by the combined effect of link errors and malicious drop is to be identified. In the insider-attack case, whereby malicious nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance. Because the packet dropping rate in this case is comparable to the channel error rate, conventional algorithms that are based on detecting the packet loss rate cannot achieve satisfactory detection accuracy. To improve the detection accuracy, the correlations between lost packets is identified. Homomorphic linear authenticator (HLA) based public auditing architecture is developed that allows the detector to verify the truthfulness of the packet loss information reported by nodes. This construction is privacy preserving, collusion proof, and incurs low communication and storage overheads. To reduce the computation overhead of the baseline scheme, a packet-block based mechanism is also proposed, which allows one to trade detection accuracy for lower computation complexity.

KEYWORDS: MANET, security, attacks, AODV.

I. INTRODUCTION

A mobile ad-hoc network (MANET) [1][2] is a collection of mobile nodes which uses wireless network to communicate with each other without any pre-defined fixed infrastructure. Fig 1 shows a typical architecture of a MANET. In such a network, the nodes are mobile and each node in the network plays a two-fold role: end-point of a communication session and intermediate router. They play an important role in the discovery and maintenance of the routes from the source to the destination or from a node to another one. During their lifetime, nodes enter or leave the network, and continuously change their relative position.

The routing protocols that have been designed generally assume that nodes are genuine and cooperative. But due to the dynamic nature of the network, malicious nodes enter in to the network and become a significant routing agent which disturbs the normal operation of the network by violating the protocol specifications [3][4][5]. Thus, the main intent of this paper is to enhance the performance of AODV protocol by identifying and circumventing malicious nodes. Here, anomaly detection scheme has been proposed to achieve the above mentioned objective. The anomaly detection scheme considers the traffic pattern of every node in the network to detect the malicious node.

II. RELATED WORK

In this section some of the security techniques that have been proposed to enhance the performance of the ad hoc routing protocols are discussed.

[6] Proposed a scheme to identify wormhole attacks in MANET. The author considered features such as number of incoming and outgoing packets and average route discovery time of every node in the network. If any abrupt changes take place in any of these features, it is found to have the presence of malicious node.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

[7] Proposed an approach in order to detect cooperative gray hole attack under AODV protocol. This approach detects the malicious node considering a common neighbor between the previous node and a suspected node. This common uses the distance information of the previous node and the suspected node to detect the presence the malicious node.
[8] Proposed a WPAODV to detect wormhole attacks in MANET. The WPAODV protocol uses neighbor node concept to detect the presence of worm hole attack node. If the route between the neighbor nodes and its succeeding nodes is greater than a predefined threshold it is declared to have worm hole in the path. The threshold is calculated by determining the path containing the more number of nodes and taking the average of the path with highest hop count.
[9] Proposed a fuzzy based intrusion detection system for detecting black hole and gray hole attack in MANET. Fuzzy logic employed here computes the number of packets dropped by a node. If the number of packets are dropped are significantly greater than a predefined threshold then it indicates the presence of malicious nodes. Here, for identifying black hole node the threshold value is set to 20% of the total packets and for the detecting gray hole attack the threshold is set to 5% of the total packets.
In [10] an approach based on intrusion detection system has been proposed for detecting cooperative black hole attacks. For this purpose the system maintains a predetermined list called audit data which comprises the normal activities of the system. For every time interval the activities of the users in the system is monitored and the collected data is compared with the audit data. If a collected is not found in the audit data, then it is the declared to have the existence of black hole attack node in the system.
In [11] an approach based on sequence number has been proposed for detecting black hole attack under AODV protocol. The difference between the sequence number of source and intermediate nodes or destination node is initially determined. If the difference is huge then it declared to have black hole node in the network.
In [12] the AODV protocol is modified so that it identifies the presence of black hole node in the network. Here, an additional information indicating the next hop node is included in the RREP packet and two control messages such as Further Route Request (FRREQ) and Further Route Reply (FRREP) are also employed. Once the RREP packet is received by the source it sends FRREQ to the next hop node in the RREP packet and after receiving FRREQ, the node replies with FRREP. If a node is black hole node it does not sent FRREP packet to the source.

III. PROPOSED METHODOLOGY

Dynamic Anomaly Detection Approach

Feature Definition of Dynamic Anomaly Detection

Each node determines its own traffic and exploits a time slot to store the total number of messages or packets that has been transmitted according to their types. In this time slot Δ_T, which is the network state's instantaneous value is represented by a n-dimension vector$[x1,x2. .\ xn]^T$, where x is the feature that is being measured.

In this study nine path finding features, four path abnormality features, and a single feature concerning a main characteristic of AODV are considered for detecting the abnormalities in the network.

Path finding features

The following path finding features are considered in this study:

Number of received RREQ messages
Number offorwarded RREQ messages
Number of outbound RREQ messages
Number of outbound RREP messages
Number of received RREP messages.

The number of RREQ messages that will be received is of three types, i.e., messages with their own source and the destination IP addresses, and messages without their own source and destination IP addresses. For an instance, when a node is under attack, a huge volume of RREQ messages will be received by it, and consequently, the number RREQ messages that is being received increases. This phenomenon signifies the presence of anomaly.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Path Abnormality features
These features are given as follows:

Number of received RERR messages
Number of dropped RREQ messages
Number of outbound RERR messages
Number of dropped RREP messages

When determining the number of RREQ messages that is being received, the packets with the same destination sequence number and destination IP address are noted only once for every time slot. For instance, when a node is under "Modification of RREQ" messages attack, a huge volume RREP packet cannot be successfully sent. Due to this, the dropping factor of RREP messages will increase, and this indicates the presence of abnormality.

AODV Characteristic Feature
The AODV characteristic feature that has been considered is the difference in the destination sequence number between the one present in the present in the RREP packet and the one contained in the list. Generally, while transmitting RREQ packets the source includes the destination IP address and sequence number in a list. Once the source receives the RREQ, it verifies the list for the destination sequence number. If the sequence number does not exists it indicates the presence of an abnormality.

IV. Learning of the States of the Network: Let T0 be the present time interval, and T1 be the initial time interval. By considering the data obtained in T1, the initial principal element is determined, and then the determined first principal element is employed in the subsequent time interval T0 for detecting anomaly. If the condition in T0 is identified as normal, then the corresponding data set will be used as the training data set. Otherwise, it will be treated as the data including attack, and it will consequently be discarded. This way, we keep on learning the normal states of the network. When updating the database, it is possible to use the most recent data set. But, as the current data set is easily influenced by the sudden network changes, it is significant to consider the time series model to preserve the database from the changes in the network topology. .

Authentication Technique for Path Finding Features
Homomorphic linear authenticator (HLA) cryptographic primitive which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients in routing pathfollows two steps. First public auditor should not be able to decern the content of a packet delivered on the route through the auditing information submitted by individual hops, no matter how many independentreports of the auditing information are submitted to the auditor. Second, our construction incurs low communication and storage overheads at intermediate nodes. This makes our mechanism applicable to a wide range of wireless devices, including low-cost wireless sensors that have very limited bandwidth and .memory capacities. This is also in sharp contrast to the typical storage-server scenario, where bandwidth/storage is not considered an issue. Write a separate function for encode and decode which will encrypt the data and give one digital signature is attached with request packet and as decode get an encrypted data as input then decrypt it. The encode function need two parameters which as data and the key in our project we used the node position as key. For decryption the key or digital signature will be matched with the node id as well as its position if matched the node is in routing process else attacker.

V. RESULTS AND DISCUSSION

In order to analyze the effectiveness of the proposed approach, simulations are performed using NS2. Table 1 shows the parameters that have been considered for configuring the network.

Simulation Parameters

Packet Size	1000
No. of Nodes	40
Protocol Used	DSR
Dimension	1000*1000

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Channel Type	Wireless channel IEEE 802.11
Queue Type	CMUPriQueue
Antenna	Omni Antenna
Protocol	TCP
Mobility	5 m/s
Traffic Type	CBR
Mobility Model	RandomWayPoint
Traffice interval	1.02

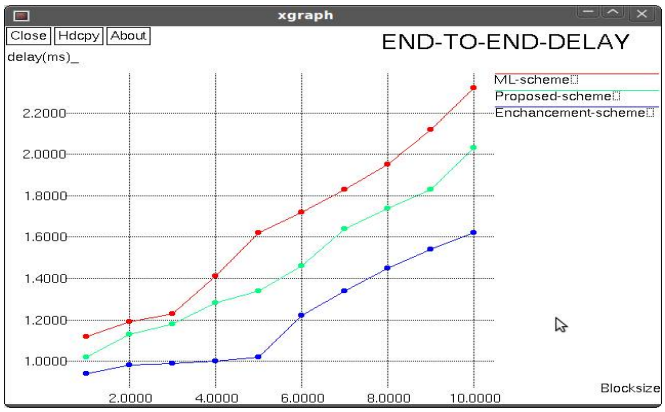
END-TO-END DELAY

Block Size v/sDelay

It is defined as the average time taken by the packet to reach the server node from the client node.
Delay = (Inter arrival of 1st pkt time and 2nd packe time) / (simulation_time)

END-TO-END DELAY (sec)		
ML Scheme	Proposed	enchanced
1.72	1.63	1.22
1.83	1.75	1.24
1.95	1.89	1.45
2.12	1.95	1.56
2.35	2.01	1.62

a)



b)

Depicts the time vs delay graph. The graph compares the end-to-end delay for both proposed and Enchancement. It is observed that, the end-to-end delay is reduced Enchancemnt method.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

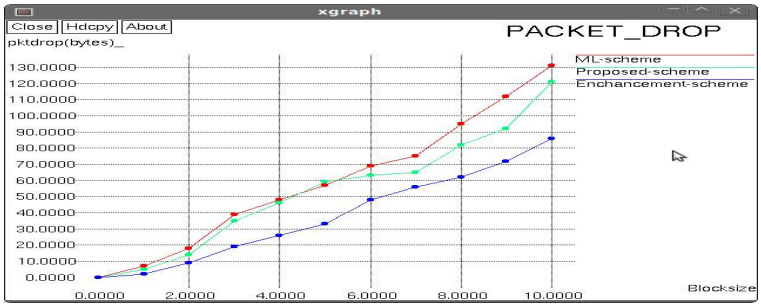
PACKET DELIVERY RATIO

Packet Delivery Ratio is defined as the average of the ratio of the number of packets received by the receiver over the number of packets sent by the source.

DeliveryRatio=(total_packets_received) / (total_packets_sent) *100

PACKET DELIVERY RATIO (%)		
ML Scheme	proposed	enchanced
7	5	2
18	14	9
39	35	19
49	46	26
57	52	33

c)



d)

From the above graph, it can be concluded that the miss detection probability of the proposed and their enhancement schemes are minimum when compared to the ML scheme. The packet drop factor which indicates the number of packets that has been dropped

FALSE ALARM PROBLEM

The false alarm will be differentiated from the overall selfishness alarm.

False Alarm		
ML Scheme	Proposed	Enchance
0.26	0.24	0.28
0.20	0.25	0.28
0.15	0.27	0.29
0.15	0.23	0.29
0.16	0.21	0.26

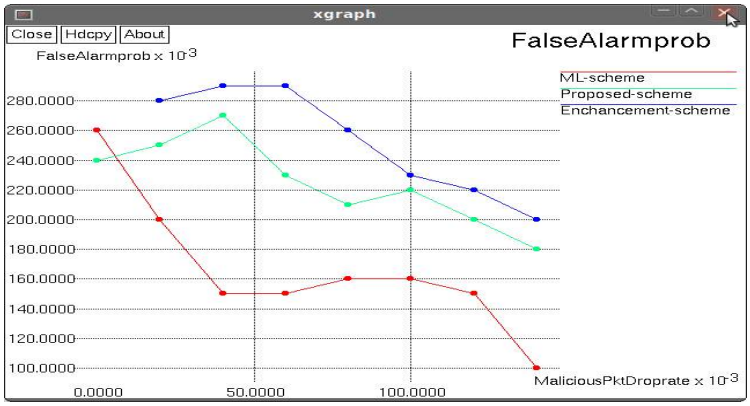
e)

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016



f)

The graph shows that the packet drop rate of the proposed and their enhancement scheme is low when compared to the ML scheme since the proposed approach considers thes traffic pattern of a node thereby effectively identifying malicious node than the ML scheme. The false alarm probability factor which indicates the dropping of malicious packets.

VI. CONCLUSION

Due to the dynamic nature of the network, malicious nodes enter in to the network and become a significant routing agent which disturbs the normal operation of the network by violating the protocol specifications. Thus, in this study dynamic anomaly detection approach has been proposed to detect the existence of malicious node that disrupts the normal operation of AODV protocol. This approach considers nine path finding features, four path abnormality features, and a single feature concerning a main characteristic of AODV for detecting the abnormalities in the network. Simulations have been performed to analyze the effectiveness of the proposed approach. The results indicate that the proposed scheme outperforms the ML scheme in terms of miss detection probability, packet drop, false alarm probability, detection error probability and end-to-end delay.

REFERENCES

1. K.S.Dinesh, “Routing Overhead Reduction and Selection of Stable Paths in MANET”, International Journal of Inventions in Computer Science and Engineering, 1(9), 2014.
2. G.Rajiv Suresh Kumar, K.M.Mohana Sundaram “Queuing Based Load Balancing Approach for Improving Network Performance in MANET”, International Journal of Inventions in Computer Science and Engineering, 1(8), 2014.
3. Ajay Jangra, Shivi Goel, “Biometric based Security Solutions for MANET: A Review”,I. J. Computer Network and Information Security,2013.
4. Anurag Kumar, Akshay Kumar, Anubha Dhaka and Garima Chaudhary, “Intrusion Detection against Denial of Service Attacks in MANET Environment”,International Journal of Emerging Trends & Technology in Computer Science, 2(4),2013.
5. Sneha A. Deshmukh, Monika Rajput, “Unwanted Activity Detection System in Wireless Network”, International Journal of Computer Science and Information Technologies, 5(2), 2014.
6. Saurabh Upadhyay and Aruna Bajpai “Avoiding Wormhole Attack in MANET using Statistical Analysis Approach” ,International Journal on Cryptography and Information Security,2(1),2012.
   Avenash Kumar , Meenu Chawla “Destination based group Gray hole attack detection in MANET through AODV”, International Journal of Computer Science Issues, 9(4), 2012 .
7. Vikaskumarupadhyay, Rajesh K Shukla, “WPAODV: Wormhole Detection and Prevention Technique”, WPAODV: Wormhole Detection and Prevention Technique, 5(3),2013.
8. E. Vishnu Balan , M.K. Priyan , C. Gokulnath , G. Usha Devi, “Fuzzy Based Intrusion Detection Systems in MANET”, International Conference on Cloud Forward: From Distributed to Complete Computing, 2015.
9. Alem, Y.F.,Zhao Cheng Xuan, “Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection”, International Conference on Future Computer and Communication (ICFCC), 2010.
10. S. Tamilarasan , “Securing AODV Routing Protocol from Black Hole Attack”, International Journal of Computer Science and Telecommunications, 3(7), 2012.
11.Romina Sharma, Rajesh Shrivastava, “Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network”, International Journal of Computer Science and Network Security, 14 (3), 2014.