Data Security using Packet Dispersion in MANET

Ramkrushna C. Maheshwar
Computer Science and Engineering,
Symbiosis Institute of Technology and Science.
Jawaharlal Neharu Technological University, Hyderabad,

Rohitkumar R. Wagdarikar
Computer Science and Engineering,
Symbiosis Institute of Technology and Science.
Jawaharlal Neharu Technological University, Hyderabad, India.

Anandrao G. Deshmukh
Computer Science and Engineering, BIGCE, Solapur.

Abstract— In real Growing world, Network Security is very necessary. To provide a secure, reliable network system, we are going to develop such an application which provides a high security in wireless network. The dispersion technique is very useful to provide high security in MANET. This project can be used in MANET as well as stationary node network. Dispersion technique ensures security. Many organizations require an application which provides the platform to hide the information from the hackers. So we provide such facility in our model. "Data Security using Packet Dispersion" provides facility to hide data from hacker and this is possible by dispersion of data. In this technique, the packets are forwarded to the nearest neighbor node and also checks nodes battery level to make process faster.

Keywords- Packet dispersion, security in MANET, Security in Wireless, Data Security using Packet dispersion.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as a routers. Network nodes in MANETs are free to move randomly[5]. Therefore, the network topology of a MANETs may change rapidly and unpredictably. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves either individually or collectively. Depending on its application, the structure of a MANET may vary from a small static network that is highly power-constrained to a large-scale highly dynamic network. There are two types of MANETs: closed and open. In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity [].

Packet dispersion in IP networks is a mechanism in which application packets are dispersed between parallel paths leading from the source to the destination, based on a predefined dispersion strategy[10]. Packet dispersion can be implemented by the source application or by nodes in the network. There are two types of Packet Dispersion techniques: Packet Pair Dispersion, Packet Train Dispersion. In a Packet Pair Dispersion, Two equal sized packets are sent back to back through the network. In a Traffic Train Dispersion, multiple back to back probe packets are sent through the network.

Packet dispersion can be implemented through a variety of strategies, which of these are following:

I. Deterministic scheduling dispersion

a. Periodic dispersion – session packets are dispersed in a periodic schedule manner over the routes repeatedly. For example, if the schedule is (i, i, i, j, j) then in every cycle 3 packets in a row are sent over path pi, and then the following two packets are sent over path pj, where this schedule repeats cyclically.

b. Deterministic round robin dispersion – a special case of periodic dispersion where packets are sent in a round robin fashion (cyclic schedule) over the paths.

Random packet dispersion – for each packet of the session, the dispersing device picks randomly one of the paths leading to the destination and sends the packet over it. The traditional delivery of packets over a single path is referred to as a no-dispersion strategy. We will assume that the packet dispersion strategies are executed in session context[10].

II. RELATED WORKS

The following list of papers shows the relative work carried out for Data security in MANET and Packet Dispersion techniques and possible solutions given.

I. Packet Dispersion in IEEE in 802.11 Wireless Networks: This paper focuses on packet dispersion in Wireless LAN (WLAN's) and types of dispersion[1].
II. Energy –Efficient Deployment of Intelligent Mobile Sensor Networks: This paper focuses on the battery levels of the nodes for faster processing of data transmission[2].
III. Cross-Layer Approach to Detect Data Packets Droppers in Mobile Ad-Hoc Networks: This paper gives you idea to find out the selfish nodes [3].
IV. Routing Misbehavior Detection in MANTETs Using 2ACK: scheme to detect and mitigate the effect of routing misbehavior in Manet's environment [5].
V. Study of Different attacks in MANET with its detection and mitigation schemes: This paper focus on what kinds of attacks occur on MANET and how to detect and mitigate them[6].
VI. A New Combination Approach to Secure MANET's Against attacks: identity and prevent the malicious nodes exhibiting different layer attacks[7].
VII. A Highly Secured Approach against attacks in MANETS: The approach effectively detects and prevents the selfish nodes and links in networking sessions[8].
VIII. Secure Data Transmission Model in MANET: data transmission using both reactive and proactive protocol[9].

III. PROPOSED SYSTEM

The Packet Dispersion technique divides data into sub packets and disperses those packets in network. Dispersion means the sending different packets to different nodes.

Past Trends:

Few years ago, encryption and decryption algorithm was used to provide security. Once a node is compromised, the hacker can always acquire the encryption/decryption keys of that node, and thus can intercept any information passed through it

.

Current trends:

Now days, organizations became large so they must require good application which manages the security of whole organization. This model gives flexible facilities to the network with better performance. We provide the facilities that needed for the organization.

Future Trends:

This model provides the facility that makes a flexible and reliable network system. We have to provide some future trends such give a powerful network system. Those give strong algorithm for dispersion technique.

Goals:

The goal of "Data Security using Packet Dispersion" is to secure the important data over the unreliable channel i.e. wireless channels in such a way that no one apart from sensor and sink can access the data.

Problem Definition:

Creating and maintaining the network and application that support the whole organization is a major concern. Without reliable network any organization cant increase their network performance. In MANET networks any node request for private data then network provide high security for that data. To ensure security we can have encryption algorithm but in this technique whole data present in one packet therefore it is easy for hacker to hack data, by knowing the key he will be able to get access to whole data directly. To remove this drawback we used dispersion technique.

3.1 SYSTEM MODEL

The modules are as follows: Data Module, Dispersion Module, Routing Module, and Network Module. The main focus of this is on dispersion Module i.e., divides data into small packets and disperses it in network.

Data Module: This module Sink Node will request to the sensor node for data and its details. Then Sensor node will receive acknowledgment from the Sink node with its details. Sensor node gather appropriate data required by the Sink node and get details about time to live and chunks.

Dispersion Module: This module is very important in our project. In this module sensor divides data into sub packets and disperses those packet in the network. Dispersion means sent different packets to different nodes.

Routing Module: This module is used to route packet in the network. This module decides that which packet to be send to which node and In this module it will find trusted and selfish nodes and make a group of trusted node and send the packets to the intermediate trusted nodes.

Simulator Module: This module maintains information of network. In this module we created simulator to show our output graphically.

In the existing system, there is a possibility that when a sender chooses an intermediate link to send some message to destination, the intermediate link may give problems such as the intermediate node may not forward the packets to destination, it may take very long time to send packets or it may modify the contents of the packet. In MANETs, as there is no retransmission of packets once it is sent, hence care is to be taken that packets are not lost. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. It will not be forwarded further. The nodes which do not forward the packets to neighboring nodes called as selfish nodes.

The node level modules are following:

Module 1: Sender module (Source Node/Sensor Node).

The task of this module is to read the message and then divide the message into packets, send these packets to receiver through the intermediate node and receive acknowledgement from the receiver node through the intermediate node.

Module 2: Intermediate module (Intermediate Node).

The task of this module is to receive packet from sender and send it to intermediate node toward the destination.

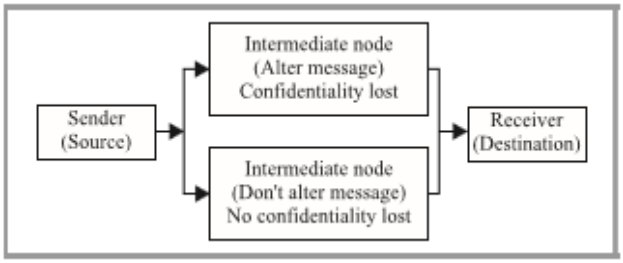

Fig1. Packet Dispersion Node level diagram

Module 3: Receiver module (Destination Node/Sink Node).

The task of this module is to receive message from the intermediate node, take out destination name and hash code and decode it. Compare the hash code of source node and destination node for security purpose.

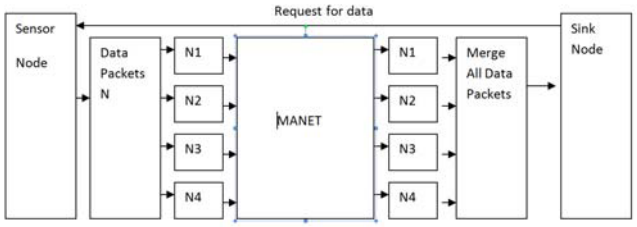

Fig.2 Packet Dispersion Technique

3.2. FUNCTIONING OF SCHEME:

It is used to safeguard the data transmission against arbitrary malicious behaviour of network nodes. The packet dispersion for secured data communication provides end to end secure and robust feedback mechanism. The technique uses an active path set comprising node disjoint paths, determined and deemed operational at the source for communication with a specific estimation disperses each outgoing message and dividing the resultant information into N pieces, which are transmitted across routes one piece per route. Even if the message pieces are lost or corrupted, successful reception of M out of N pieces allows the reconstruction of messages at the destination. The ratio r=N/M is termed the redundancy factor and we denote a dispersed message with redundancy r as an (M, N) message[9].

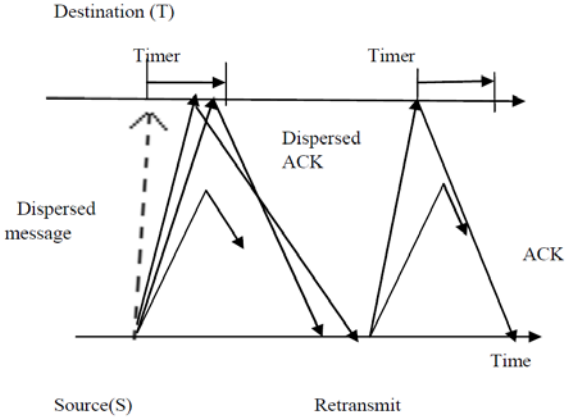

Fig.3 Dispersing the Messages in network

In Fig 4. we showed the sink node and sensor node. The sink node makes request to the sensor node for the data packets. The sensor node which receives the request from the sink node and add sink to the list, then it transmits whatever required data packets to sink on network using dispersion technique. Here the data packets divide into sub data packets and transmit to different intermediate nodes in the network towards the sink node. Whenever the packet receives the sink node it merges the all data packets which are dispersed on the network

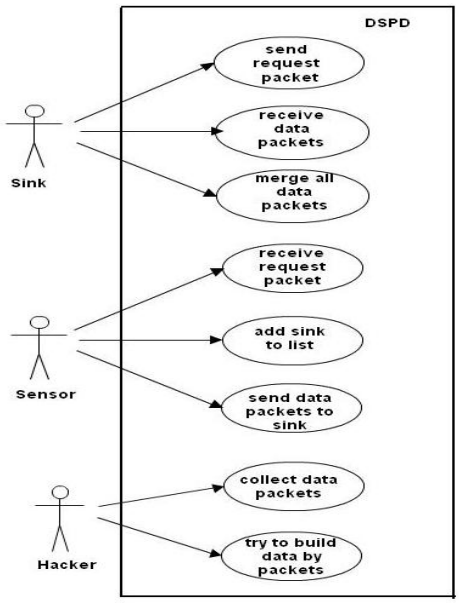

Fig.4 Use Case Diagram for Packet Dispersion

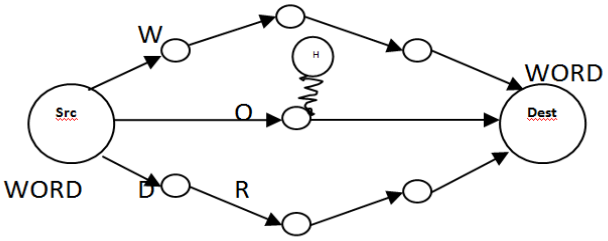

Fig.5 WORD Transmission on MANET using Packet Dispersion

In MANET networks any node request for very private data then network provide high security for that data. To ensure security we can have encryption algorithm but in this technique whole data present in one packet therefore it is easy for hacker to hack data, by knowing the key he will be able to get access to whole data directly. To remove this used dispersion technique. In this technique Divides the data packets into sub packets then transmits that sub packet to intermediate node towards the destination. After reaching at destination merges the all sub packet that will make as original data packet. Here will get the security from hacker, if hacker tries to access the router nodes in network he will get only sub packets so hacker cant access the whole data , we are getting the security on data transmission over the Manet.

IV. ALGORITHM FOR PACKET DISPERSION :

We have used the triplet of SENSOR_NODE -> INT_NODE -> SINK_NODE as an example to illustrate Packet Dispersion. Where SENSOR_NODE is assumed
as the source node, INT_NODE is the intermediate node and SINK_NODE is the destination node.

Nomenclature:
Pkt_Count = the number of the message packets sent,
Pkt_Miss = the number of the 2ACK packets missed,
d = the acknowledgement ratio,
WT = waiting time, i.e., the
maximum time allotted to receive 2ACK packet

DATA MODULE:

Sink Node: Request for Data to the sensor node.
Sensor Node: Accept the request from sink node. Extract the Sink Node details.
Gather the details of data , size of data, the time to live and details of chunk.

DISPERSION MODULE :

At node SENSOR_NODE

```
while (true) do
Read the destination address;
Read the message;
Find the length of the message.
Pkt_Miss=0, Pkt_Count=0, WT=20 ms, d=0.2,
2ACK Time=Current Time (Acknowledgement accepted time) – Start Time.

while (length > 64 bytes) do
Take out 64 message packet;
Length = length – 64;
Encode message using hash function;
Send message along with the hash key;
Pkt_Count++ ;

Receive 2ACK packet;
if (2ACK time > WT) then
Pkt_Miss++ ;
end
end

if (length < 64 bytes) then
Encode message using hash function;
Send message along with the hash key;
Pkt_Count++;
Receive 2ACK packet;
if (2ACK time > WT) then
Pkt_Miss++;
end
end
end
```

At node SINK_NODE :

```
while (true) do
Read message from INT_NODE;
Take out destination name and hash code;
Decode the message;
Rearranges all messages;
If (Pkt_Count==total_chunk)
Successfully Received the messages;
Else
Retransmission of messages ;
End
Send 2ACK packet to INT_NODE;
End
```

ROUTING MODULE :

At node INT_NODE

```
Find out Trusted nodes and Selfish nodes.
While (true) do
Send the request to all intermediate nodes.
```

```
If (Ack==true) then
Add it to trusted group nodes
Else
Declare it as a selfish node .
End if
End

while (true) do
Read message from source SENSOR_NODE
if (Alter) then
Add dummy bytes of characters;
Process it and forward to destination SINK_NODE;
Receive 2ACK from SINK_NODE and send it to SENSOR_NODE;
else if (Do not Alter) then
Process it and forward to destination SINK_NODE;
Receive 2ACK from SINK_NODE and send it to SENSOR_NODE;
end
end
```

Combination of SENSOR_NODE and SINK_NODE parallel:

```
while (true) do
if ((Pkt_Miss/Pkt_Count)>d and (hash code of source msg) != (hash code of destination msg)) then
Link is misbehaving and the confidentialityis lost;
End

if ((Pkt_Miss/Pkt_Count)<d and (hash code of source msg) ! = (hash code of destination msg)) then
Link is working properly and the confidentialityis lost;
end

if ((Pkt_Miss/Pkt_Count)>d and (hash code of source msg)= (hash code of destination msg)) then
Link is misbehaving;
end

if ((Pkt_Miss/Pkt_Count)<d and (hash code of source msg)= (hash code of destination msg)) then
Link is working properly;
end
end
```

V. GUI SNAPSHOTS

In this project, we have two graphical user interface (GUI) for providing user friendly environment. The first form is used to take input from user and the second form is used to show output on simulator.

In this simulator:

Yellow nodes = both in queue and out queue contain packets.
Green nodes = only in queue contain packets and out queue is empty.
Red nodes = only out queue contain packets and in queue is empty.

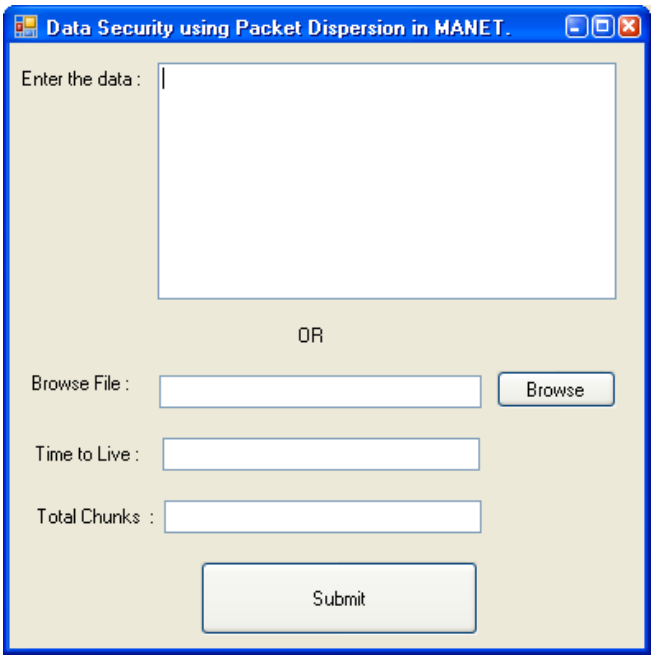

Fig.5 User Inputs Time to live and total no. of chunks

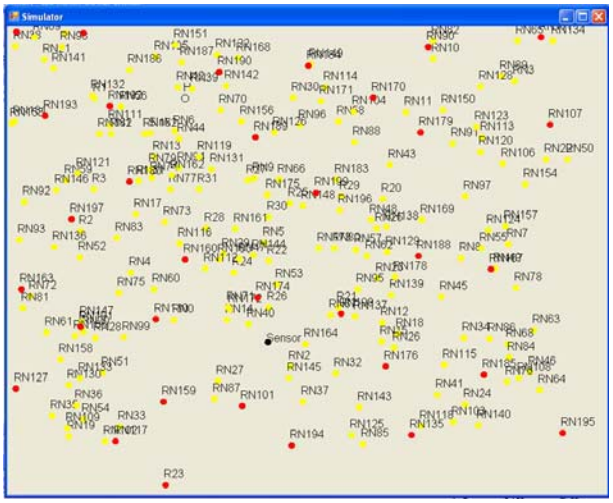

Fig.6 Initial state of network and movements of router nodes.

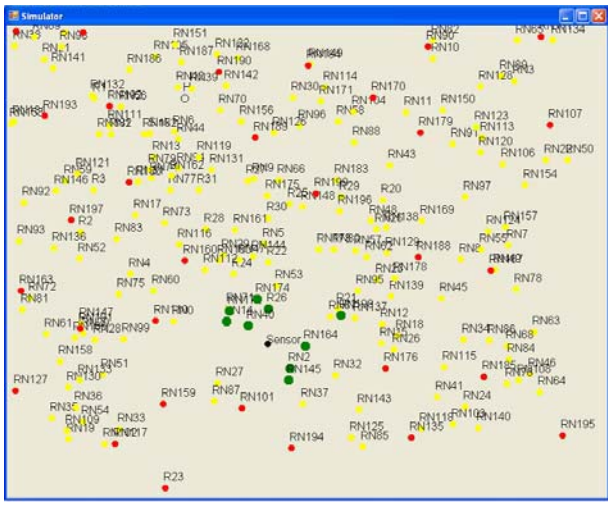

Fig.7 how packets are dispersed through nodes in network.

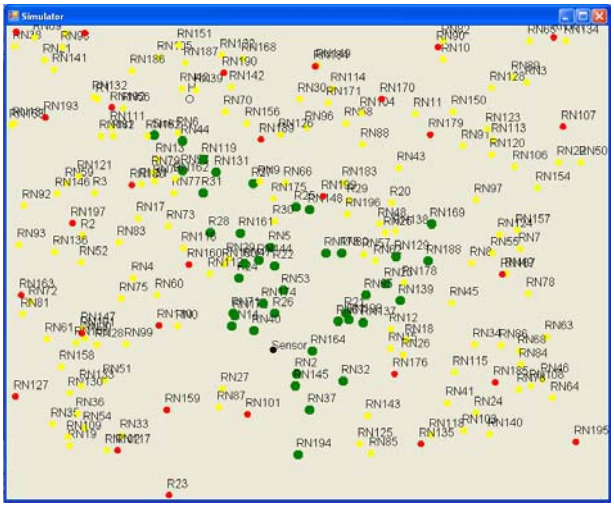

Fig.8 Fully dispersed packets throughout the nodes and all the packets are securely delivered to sink.

Approach	Link Staus	Packet Delivery Status	Routing Overhead
Packet Pair Dispersion	Proper	100%	Low
	Misbehaving	90%	Medium
Random Packet Dispersion	Proper	100%	Low
	Misbehaving	90%	Medium

Fig.9 Packet Pair Dispersion and Random Packet Dispersion

VI. ROUTING DETAILS:

:Sink Sending Request Packet
:Sensor:request payload received
:sending data packet
:R25: DataPayload 0 from RN148
:R25: Forwarding Data to :[0] R27
:RN40: RequestPayload
:RN40: Forwarding Request to : Sensor
:RN67: DataPayload 1 from R21
:RN67: Forwarding Data to :[1] R21
:RN71: RequestPayload
:RN71: Forwarding Request to : RN40
:RN73: RequestPayload
:RN73: Forwarding Request to : RN116
:RN77: RequestPayload
:RN77: Forwarding Request to : RN73
:RN94: DataPayload 2 from R31
:RN94: Forwarding Data to :[2] Sink
:RN112: RequestPayload
:RN112: Forwarding Request to : RN71
:RN116: RequestPayload
:RN116: Forwarding Request to : RN112
:RN162: RequestPayload
:RN162: Forwarding Request to : RN77
:Sink: GOT DATA PACKET : 3 from RN94
:Sink Sending Request Packet
:Sensor: request payload received
:sending data packet
:R27: Data Payload 0 from R25
:R27: Forwarding Data to :[0] RN131
--
--
--
--
--
--
:RN116: Forwarding Request to : RN112
:RN162: RequestPayload
:RN162: Forwarding Request to : RN77
:Sink: GOT DATA PACKET : 0 from RN44
:Sink Got Complete Packet
:Sink Sending Request Packet
:Sensor:request payload received
:sending data packet
:sending data packet

:H: GOT DATA PACKET : 0

VII. VALIDATION TESTING:

This phase of testing validates fields of the forms that are to be input by the user. This includes checking if necessary fields have been left empty and performing data type validation checks, e.g. detecting if users has input a string in place of an integer value.

Test case 1: Test for valid Request of Sink

Aim: Test for valid Request of Sink node
Method: Field which takes request.
Operation: sink node will wait for response.
Expected result: system request to Sensor node for TCP connection.
Actual result: same as expected.

Test case 2: Test for Sensor check for request

Aim: Test for Sensor check for request
Operation: find requested data into memory.
Expected result: Sensor accepts request, try to find requested data.
Actual result: same as expected

Test case 3: Test for Routing of data

Aim: Test for routing of data
Operation: router routes request from sink to sensor and data packet from sensor to sink.
Expected result: router forwards data to the correct neighbor node.
Actual result: same as expected

VIII. RESULT AND FUTURE SCOPE :

The project "Data Security Using Packet Dispersion" is to provide services for securing data in wireless network. The focus of our system is on providing reliable service to the needs and expectations of users. In our application the data is divided in number of chunks and the chunks are dispersed to different nodes present in network. So, Data Security Using Packet Dispersion is best suitable for the security purpose in Manet. In future we will reduce the time span between packet dispersion and re-union of packets. We may also encrypt a data while dispersing so that a single packet should not be viewed by any one. Further the scheme can also be extended for identifying and preventing more number of network layer attacks; so that the approach can be made more robust against the attacks.

IX. PERFORMANCE ANALYSIS:

We have considered the network parameters for evaluating the performance with the packet dispersion technique. Further it can be extended to a few more parameters based upon the node density in the network. The algorithm can also be extended to identify and prevent few more network layer attacks.

• Packet delivery ratio – the ratio of the number of packets received at the destination and the number of packets sent by the source.
• Routing overhead – The number of routing packets transmitted per data packet delivered at the destination.

X. CONCLUSION

The MANETS security issues new ideas and approaches as it has got potential widespread applications in military and civilian communications. In these networks there will be more dependence on the cooperation of all its nodes to perform networking functions. Thus, makes it highly vulnerable to malicious nodes. One such misbehavior is related to routing of packets. When such misbehaving nodes take part in the route discovery process, but refuse to forward the data packets, routing performance may be degraded severely. The performance degradation caused by such malicious nodes (misbehaving) in MANETS. We have proposed and evaluated a technique called, packet dispersion to detect and mitigate the effect of such routing misbehavior & to provide security for the data transmission. The packet dispersion technique to detecting the malicious node by sink node, isolation of malicious

node by discarding the path and prevention data packets and providing security for data packets. Our analysis and simulation have shown the effectiveness of the randomized dispersive routing in Manet.Through this simulation we showed that how data has been securely transmitted in Manet. At the same time , we verified that this improved security performance comes at a reasonable cost of energy.

REFERENCES

[1] Mingzhe Li, Mark Claypool and Bob Kinicki , Packet Dispersion in IEEE in 802.11 Wireless Networks , P2MNet Tampa, Florida, November 14, 2006

[2] Nojeong Heo and Pramod K. Varshney*, Fellow, IEEE* , Energy Efficient Deployment of Intelligent Mobile Sensor Networks , IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 35, NO. 1, JANUARY 2005.

[3] Djamel Djenouri and Nadjib Badache,Cross-Layer Approach to Detect Data Packets Droppers in Mobile Ad-Hoc Networks, IWSOS 2006, LNCS 4124, pp. 163–176, 2006.

[4] S.Dhanalakshmi, Dr.M.Rajaram , A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET, IJCSNS International Journal of Computer Sci 184 ence and Network Security, VOL.8 No.10, October 2008.

[5] Sunilkumar S. Manvi*a*, Lokesh B. Bhajantri*b*, and Vittalkumar K. Vagga, Routing Misbehavior Detection in MANTETs Using 2ACK, Journal of telecommunication and information technology 4/2010.

[6] Himadri Nath Saha # 1 , Dr. Debika Bhattacharyya # 2 , Dr. P. K.Banerjee *3, Study of Different attacks in MANET with its detection and mitigation schemes, IJAET/Vol.III/ Issue I/January-March, 2012/383-388.

[7] G. S. Mamatha and Dr. S. C. Sharma, A New Combination Approach to Secure MANETs Against attacks, International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010.

[8] G.S. Mamatha and Dr. S. C. Sharma, A Highly Secured Approach against attacks in MANETS, International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010 / 1793-8201.

[9] Panagiotis Papadimitratos *, Zygmunt J. Haas, Secure Data Transmission Model in MANET, Ad Hoc Networks 1 (2003) 193–209.

[10] Haim Zlatokrilov, Hanoch Levy , Packet Dispersion and the Quality of Voice over IP Applications in IP networks , School of Computer Science Tel Aviv University Tel Aviv, Israel