Providing Intrusion Detection and Preventing System by using DTMO Protocol in MANET

V. Nikhil Srivatsav, D. Veeraiah

Vignan University

***Abstract*: - Recent days wireless communication have become wide spread all over the world. In wireless communications, Mobile Ad-hoc NETwork (MANET) is one of the applications, i.e. mostly used. MANET is decentralized system architecture, i.e. architecture is dynamic in nature and changes according to the situation. In MANET each and every act as a transmitter and receiver. Each and every node can communicate with other nodes directly or indirectly. In indirect communication, source nodes rely on intermediate nodes for transferring the packets to destination nodes. Simply MANET has become very popular due to self configuring of nodes. MANET is used in military applications, emergency services like earth cakes, disasters, personal Area Network (PAN).Due to open medium and dynamic infrastructure of MANET, MANET has become vulnerable to malicious attacks. For overcoming this nature, Intrusion Detection System (IDS) is proposed. Present days this IDS is used in MANET for providing security. In this paper, I going to purpose the new technique called DYNAMIC MANET ON DEMAND (DYMO) Routing Protocol and it is implemented in this paper.**

***Index Terms*: - Digital signature, Diffie Hellman Key Exchange, DYMO Routing Protocol,Mobile Ad-hoc NETwork (MANET)**

1. INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is a self configuring infrastructure network of mobile devices connected by wireless. Ad hoc is derived from Latin and the meaning is “for this purpose”.

Each device in a MANET is free to move independently in any direction and it will change the links with other devices dynamically. Each and every mobile node has a tendency to transmit and receive the packet from other mobile nodes. Communication

can be taken place in two ways. They are:

1) Single Hop
2) Multiple Hop

1) **Single Hop: -** In single hop, a node can communicate with other nodes within the network range without relying on other nodes or intermediate nodes.
2) **Multiple Hop: -** In this multiple hops, a node can communicate with destination nodes by relying on other nodes or intermediate node, which are outside the range of source node. Simply, destination node is not within the range of source node.

Due to Dynamic Topology and decentralized system architecture, MANET is more vulnerable to attacks. Two types of attacks are present in MANET. They are:-

1) INTERNAL ATTACKS
2) EXTERNAL ATTACKS

1) INTERNAL ATTACKS: - This type of attacks can be done by the internal nodes of a network. Simply, external nodes will not participate in this type of attack. Internal attacks cannot be detected easily because

a) Internal node are more trusted nodes
b) It can generate wrong routing information and it can be send to all other nodes which are present in the network.

2) **EXTERNAL ATTACKS: -** This type of attacks can be done by the external nodes of a network, i.e. nodes does not present in a network. Congestion can occur due to these external attacks.

External attacks are of two types. They are :-

a) Passive attack
b) Active attack

a) Passive attack: - In this type attack, modification of packets cannot be taken place but intruder watches traffic between source to destination and study the data in packets. This type of attacks cannot be identified by authorized

users because data in packets are not modified by an intruder.

b) Active attack: - Modification of packets can be done by a intruder.

This type of attacks can be easily identified by delaying of packets from source to destination or by checking the authentication, confidentiality and integrity. Again Active attacks are classified in to four types. They are:

1) Dropping Attacks

2) Modification attacks

3) Fabrication attacks

4) Timing attacks

1) **Dropping Attack: -** Dropping of packets can be taken place between source to destination by a selfish node or compromise node. Due to this destination node cannot reach the packets**.** Simply end-to-end connection between source and destination is lost. There is no mechanism in routing protocols to detect whether packets are forwarded by a source node or not.

2) **Modification Attack: -** In this type of attack, modification of packets can be taken and disrupt overall communication between the network nodes. SINKHOLE ATTACK is the best example for this modification attack. In Sinkhole attack, compromising node advertises itself as the shortest path from source to destination and captures the routing information. From this routing information, modification of packets Can be taken place.

3) **Fabrication Attack**:- In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

4) **Timing attacks: -** In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.
For overcoming this attack, Intrusion Detection System (IDS) is introduced.

2. BACKGROUND

2.1 DIFFIE HELLMAN KEY EXCHANGE

This algorithm is proposed by Diffie and Hellman, so it is referred to as Diffie Hellman Key Exchange. The purpose of this algorithm is to enable the two users to exchange the secret key securely. That can be used for encryption of messages. This algorithm is limited to the exchange of the keys. Their two publicly known numbers: a prime number q and an integer α. suppose user A and B want to exchange the keys. This Diffie Hellman Key Exchange algorithm is explained in the following way.

Global Public Elements

Q Prime number a
a<q and 'a' a primitive root ofq

User A Key Generation

Select private key X_A

$$X_A < q$$

Calculate public key Y_A

$$Y_A = a^{X_A} \bmod q$$

User B Key Generation

Select private key X_B

$$X_B < q$$

Calculate public key Y_B

$$Y_B = a^{X_A} \bmod q$$

Generation of secret key by User A

$$K = (Y_B)^{X_A} \bmod q$$

Generation of secret key by User B

$$K = (Y_A)^{X_B} \bmod q$$

2.2 IDS in MANET

Nodes in MANET assume that other nodes always cooperate to each other to relay data. This assumption leaves the attackers to relay on network. For overcoming this problem this problem, Intrusion Detecting System (IDS) is introduced.

An ID acts as a second layer to the MANET. An ID consists of three approaches. Namely Watchdog, Twoack and Adaptive ACK (AACK).

Watchdog: - For improving the throughput of a network in the presence of malicious node, watchdog

is very useful. Throughput means number of messages has been delivered to a communication channel over a period of time. Generally, Throughput is measured in Bits per second (bps).Watchdog consists of two parts namely: **Watchdog and pathrater.** Watchdog acts as IDS. It checks each and every node whether it is working properly or not. If a node is not unable to send the packet, watchdog increases the failure counter in hopcount. If the failure counter increases more than the threshold value, watchdog inform to the pathrather. Pathrather informs to the source node and destination node that this node in the path is not working properly. But watchdog is incapable of detecting the links rather than nodes. Watchdog is unable to detect to malicious behaviors with the presence of following:

1) Ambiguous collision
2) Receiver collision
3) False misbehavior report
4) Limited transmission power
5) Collision
6) Partial dropping

TwoAck: - TwoAck is proposed to overcome the two out of six defects in the watchdog. They are receiver collision and limited transmission power.TwoAck works on routing protocols such as Dynamic Source Routing (DSR) protocols. It detects misbehavior links by sending acknowledgement over three consecutive links for transmission of data packets. Working of TwoAck is shown below:

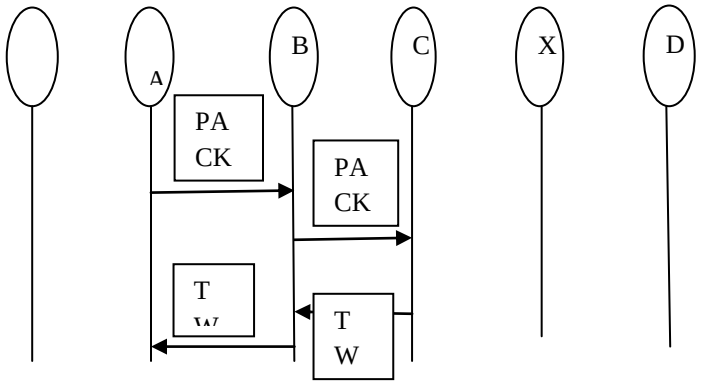

Fig 1 TWOACK scheme

Basically, TWOACK works on successive three nodes. Form above example Fig 1, packet 1 sent from node A to node B and then, node B forwards the packet 1 to node C. Node C sends TWOACK back to node B and then, node B sends back

TWOACK to node A. On successful retrieving of acknowledgement from node C to node A indicates that packet is successfully transmitted from node A to node C. If node A does not receives acknowledgment in predefined time, node A thinks that nodes B and C are malicious nodes. This process is continued for every consecutive three packets until it reaches the destination. But there will be a limited transmission power in MANET. Due to this, degradation of life span will be taken place in the network.

AACK: - AACK is a combination of TWOACK (TACK) and end-to-end acknowledgement scheme (ACK). When compared to TWOACK, there will no network overhead in AACK. Same as like of normal ACK, AACK sends packet from source to destination and receives the acknowledgement from destination to source. If acknowledgement is not received in particular period, AACK switches to TACK. But both TWOACK and AACK suffers from a problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgement packets.

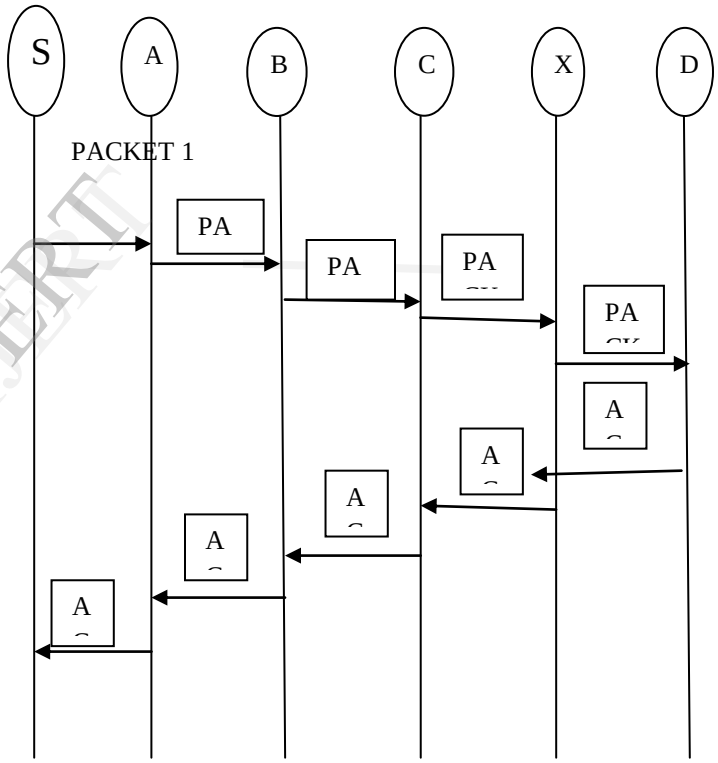

Fig 2: ACK Scheme

DIGITAL SIGNATURE: - Digital Signature is a mathematical scheme for demonstrating the authentication of document. A valid digital signature gives that message is created by a known sender. Digital signature came from cryptography. Cryptography is the study of providing security to the information while transmitting from source to destination. The aspects of providing security are authentication, integrity, confidentiality and non repudiation.

Digital Signature can be divided into two categories. They are:-

1) Digital signature with appendix
2) Digital signature with message recovery

1) **Digital signature with appendix**: For signature verification algorithm, original message is required.
   EX: - Digital Signature Algorithm (DSA)
2) **Digital signature with message recovery**: In this process, only signature is required in verification process. Simply, there is no need of any other information.
   EX: - RSA

In this paper, we proposed the both RSA and DSA

3. PROBLEM DESCRIPTION

In this paper, EAACK is proposed for handling weakness of WATCHDOG scheme. EAACK can handle three out of six weaknesses, namely,

FALSE MISBEHAVIOUR REPORT,

LIMITED TRANSMISSION POWER and

RECEIVER COLLISION.

In this section, explanation of these three weaknesses can be taken place.

a) FALSE MISBEHAVIOUR REPORT

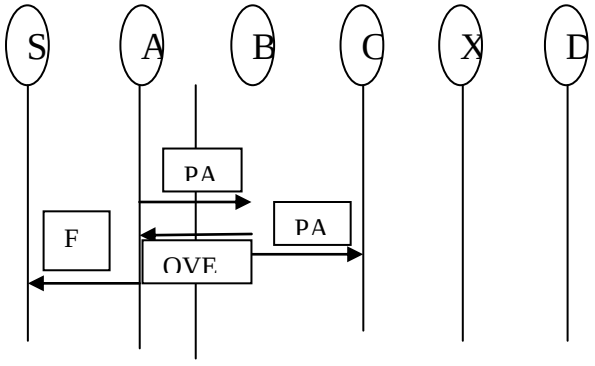

Fig 3: FRA

As the name suggests, FALSE MISBEHAVIOUR REPORT, as particular node working properly, another node reports has it is not working properly to main node or source node. For this FALSE MISBEHAVIOUR REPORT (FRA), example is explained in fig 3.

In fig 3, source node S sends a packet to destination node D via intermediate nodes A, B, C, and X. As node B sends packet to node C and node B gives reply to node A. As node A overhears the message of node B and gives a false report to source node S, i.e., node B is not working properly and node B does not sends the packet to node C. This process is known as FALSE MISBEHAVIOUR REPORT (FRA).

b) LIMITED TRANSMISSION POWER: A misbehavior node that can control its transmission power in a network for transmission of packets. Due to this data packets cannot reach the destination node D from source node S. A node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by the true recipient.

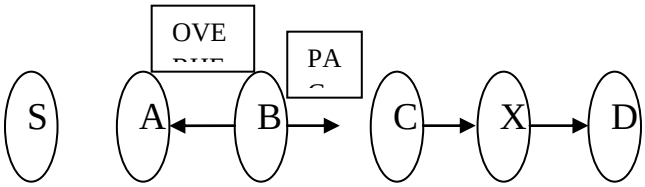

Fig 4: LRA

c) RECEIVER COLLISION

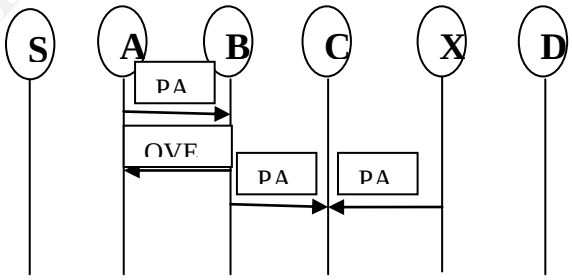

Fig 5: RC

IN this RECEIVER COLLISIONS, source node S sends packet 1 to destination node D and at the same time destination node D sends a packet 2 to source node S. Node B sends the packet 1 to node C and tells to node A that packet 1 is transmitted to node C but node B doesn't know that node X also sends a packet 2 to

node C. At node C, both the packets collide each other and both the packets are dropped at same time. This procedure is known as RECEIVER COLLISION.

4. SCHEME DESCRIPTION

To overcome the problems in watchdog, DYMO Routing Protocol is used.

DYMO ROUTING PROTOCOL:- Dynamic MANET On Demand Routing protocol is a combination of reactive and proactive routing protocol. It is extension of AODV and DSR. As like DSR, it also consists of RREQ and RREP. Every node forwards RREQ to other nodes for destination node. In this manner, each and every node learns about other nodes in the network. DYMO Protocol consists of two protocols. Route discovery and route maintenance.

Route discovery is to discover the route from source node to destination node. This process is done by flooding i.e., broadcasting the packet to all other nodes in the network. While transmitting the packet to destination node, intermediate node adds its IP ADDRESS to the packet header. Due to this RREP is possible from destination to source node in reverse path.

Each node maintains routing table with information about other nodes. Each entry in routing table consists of:

Destination Address: IP Address of the destination.

Sequence number: destination sequence number.

Hop Count: Number of hops towards the destination.

Next Hop Address: IP address of next node on the path towards the destination.

Next Hop Interface: Interface is used to send the packets towards the destination.

Route Maintenance is the process of responding the changes in the network that happens when a route is created. To maintain the path, nodes actively monitor the links between them. If destination node receives the packet without a valid path i.e., from source to destination,

then Route Error (RERR) has been occurred.

In RERR, nodes maintain the list of address and sequence number as unreachable node

REFERENCES:

1) Study of routing protocols and secure routing of MANET in AD HOC & SENSOR NETWORKS by DHARMA PRAKASH AGGRAWAL & CARLOS DE MORAIS CORDEIRO.

2) Study of routing protocols and MANET in MOBILE AD HOC NERTWORK FROM WIRELESS LANS TO 4G NETWORKS by GEORGE AGGLEOU

3) Nan Kang, Elhani M.Shakshuki and Tarek R.Sheltami."Detecting Forged Acknowledgements in MANET." Published in 2011 IEEE Conference on Advanced Information Networking ang Applications.

4) Aishwarya Sagar Anand Ukey and Meenu Chawla "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET." Published in International Journal of Computer Science Issues, Vol 7, Issue 4,No 1, July 2010.

5) Tarag Fahad & Robert Askwith "Misbehavior Detection Mechanism for Mobile Ad-hoc Networks."

6) Johann Lopez, Jose M.Barcelo, Jorge Garcia-Vidal "ANALYSING THE OVERHEAD IN MOBILE ADHOC NETWORK WITH A HIERARCHICAL ROUTING STRUCTURE"

7) Md Foyzer Mondal & Akshai Aggarwal "A REPORT ON STUDY OF MANET ROUTING PROTOCOLS BY GLOMOSI SIMULATOR"

8) Ashwini K.Pandey and Hiroshi Fujinoki "STUDY OF MANET ROUTING PROTOCOLS BY GLOMOSIM SIMULATOR." International Journal of Network Management

9) Tiranuch Anantvalee and Jie Wu "A SURVEY ON INTRUSION DETECTION IN MOBILE AD HOC NETWORKS"

10) Akash Singh, Manish Maheswari, Nikhil and Neeraj Kumar "SECURITY AND TRUST MANAGEMENT IN MANET."

11) Diffie Hellman Key Exchange algorithm in NETWORK SECURITY ESSENTIALS by WILLIAM STALLINGS

12) Elhadi M.Shakshuki, senior member of IEEE, Nag Kang and Track R.Sheltami, Member of IEEE"EAACK-A SECURE INTRUSION-DETECTION SYSTEM FOR MANET" IEEE Transactions on industrial Electronics. Vol 60 NO 3 march 2013

13) Priyanka Goyal, Vinti Parmar, Rahul Rishi "MANET VULNERABILITIES, CHALLENGES, ATTACKS, APPLICATIONS" published in International Journal of computational Engineering & Management. Vol 11 January 2011.

14) Vivek Arya and Charu " A SURVEY OF ENHANCED ROUTING PROTOCOLS FOR MANET" Published in international journal on AD HOC NETWORKING SYSTEM Vol 3 No 3 July 2011.

15) Meenakshi Patel and Sanjey Sharma"DETECTION OF MALICIOUS ATTACKS ON MANET A BEHAVIOURAL APPROACH."

16) Hariom soni, Asst.prof. Preeti Varma "A SURVEY ON PERFORMANCE BASED SECURE ROUTING PROTOCOLS IN

MANET." Published in International Journal of Advanced Research in Computer Science & Engineering. Vol 2 ISSUE 1, January 2013

17) Bounpadith Kannhavong, Hidehisa Nakayama, Yokhiaki Nemoto, And Nei Kato" A SURVEY OF ROUTING ATTACKS IN MOBILE ADHOC NETWORKS."