International Journal of Engineering & Scientific Research
Vol.4 Issue 10, October 2016,
ISSN: 2347-6532 Impact Factor: 5.900
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

SECURE DATA TRANSFER IN MANETS BY USING HYBRID PROTOCOLS

Raman Manocha*

Ravinder Choudhary*

Er. Sunil Panjeta(Research Supervisor)*

Abstract :

Wireless networks are gaining popularity day by day, as users want wireless connectivity irrespective of their geographic position. MANETs consist of mobile nodes that are free in moving in and out in the network. Mobile Ad hoc Network (MANET) is a collection of mobile nodes in which the wireless links are frequently broken down due to mobility and dynamic infrastructure. Routing is a significant issue and challenge in ad hoc networks. Many routing protocols have been proposed like IAODV and IDSR so far to improve the routing performance and reliability. ***Current work we are going to present Efficient and Secure Data transfer with hybrid of DSDV and MDSR protocol based on the performance metrics like packet delivery fraction, end–to–end delay, throughput. Simulation is done in NS2 (Network Simulator version2).***

* Dept of Electronics and Communication Engineering, YIET, Gadholi, Yamuna Nagar Haryana

1. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any challenging and interesting research areas.

2. MANETs Routing Protocols

Mobile Ad-Hoc Network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide efficient better end-to-end communication. MANETs works on TCP/IP structure to provide the means of communication between communicating work stations. Routing protocols in MANETs are a challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area.

Routing protocols in MANETs are classified as:-

A. Reactive protocols
B. Proactive protocols
C. Hybrid protocols

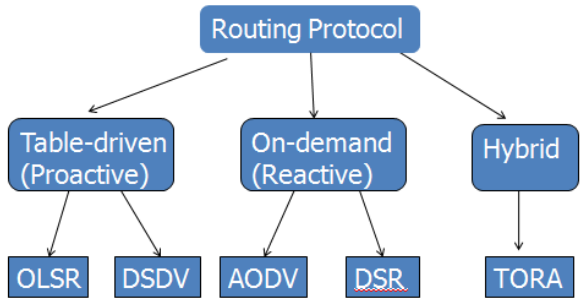


Fig. 2.1 MANETs Routing Protocols

A. Reactive Protocols

Reactive protocols are also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route.

B. Proactive protocols:

In proactive protocols, each node maintains individual routing table containing routing information for every node in the network. Each node maintains consistent and current up-to-date routing information by sending control messages periodically between the nodes which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbours. Some of the existing proactive routing protocols are DSDV and OLSR.

C. Hybrid Routing Protocol:

Hybrid routing protocol combines the advantages of both proactive and reactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some of the existing hybrid protocols are ZRP and TORA.

3. Proposed Methodology

Our IDS model is based on the following assumptions.

(a) All the nodes are identical in their physical characteristics. If node A is within the transmission range of node B, then node B is also within the transmission range of A.

(b) Also our solution assumes that all the nodes are authenticated and can participate in communication, i.e., all nodes are authorized nodes.

(c) The source node, destination node and IDS nodes are taken as trusted nodes by default.

(d) All the IDS nodes are set in promiscuous mode only when needed, and an IDS node will always be neighbour to some other IDS node.

(e) Since there are multiple routes from a source to destination, the source node has to cache the other routes to mitigate the overhead incurred during new route discovery process.

4. Protocol Description

According to DSR protocol, the source node has to broadcast the RREQ packet to find a path to reach the requested destination.The requested destination, or any intermediate node having

the path, can send back the reply to the source node. The malicious nodes which perform gray hole attack participate correctly in the route discovery process. They forward the RREQ packets as any other normal DSR nodes. When the route is selected through this malicious node to reach the destination, it selectively drops the data packets .To mitigate gray hole attack, when the destination nodes receive data packets from the source node, it starts the process of discovering the presence of any gray hole nodes in the path. In our approach, when the source node has data packets to send to the destination, it divides the data to be transmitted into different blocks and sends one block of data at a time to the destination. It also intimates the number of data packets it sends in a block to the destination before the actual transmission of the data using a different route (2nd shortest path to reach destination).

We denote the number of packets forwarded by source node S to destination node D in a block be NS. Let nodes a0, a1, a2, a3, . . . , an represent the source route or data forwarding route between source node S and destination node D. Any node ai in the path has to keep count of the number of packets it forwards to its downstream node ai+1 as NFPai, ai+1. When the destination node receives the data packets from the source, it starts a counter and keeps count of number of data packets it receives in a block. Let N_D denotes the packets received at the destination node, and then the probability of packets received at the destination node is calculated as follows:

$P_{D=}N_D/N_S$

If $P_D > T_{PL}$, then the destination node starts the process of detecting whether any malicious node is present in the route. If not, then the destination node sends the positive acknowledgement back to the source node. Here T_{PL} represents the packet loss threshold value and takes values between 0 and 0.2. In our approach, the destination node starts the gray hole detection process, when the data packet loss exceed 20% of the total packets sent by the source node. The source node starts transmitting the next block of data only after receiving the positive acknowledgement from the destination or receiving ALARM packet from the neighbour IDS node. Procedure 1 shows the action of the source and destination nodes during the transmission and reception of data packets.

4.2. Gray hole attack discovery process

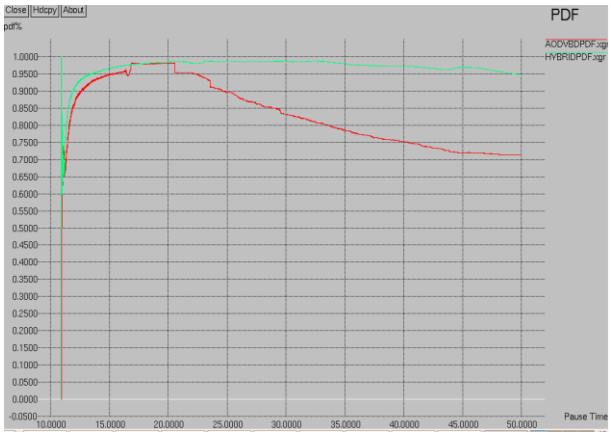
When the destination node discovers that the actual number of data packets it receives from its previous hop node is significantly less than the number of data packets the source node sends, it starts the gray hole node discovery process. First it sends a QUERY REQUEST

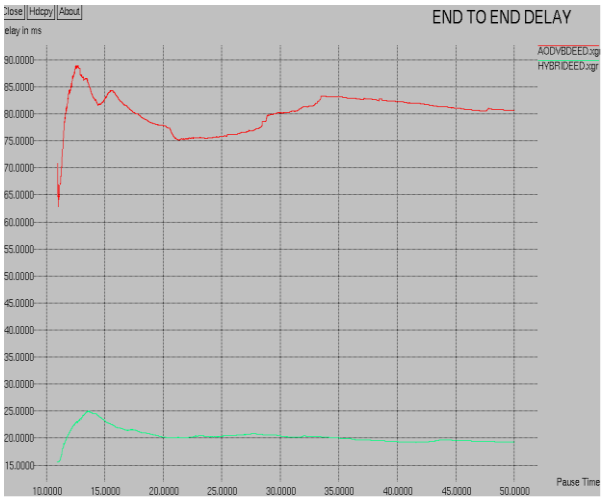
(QREQ) packet to the node in the source route (data forwarding path) at a 2-hop distance from it. If S, a0, a1, a2, . . . , an_3, an_2, an_1, an, D represents the source route, then node D sends a QREQ packet to node an_1 which is at 2-hop distance to node D.

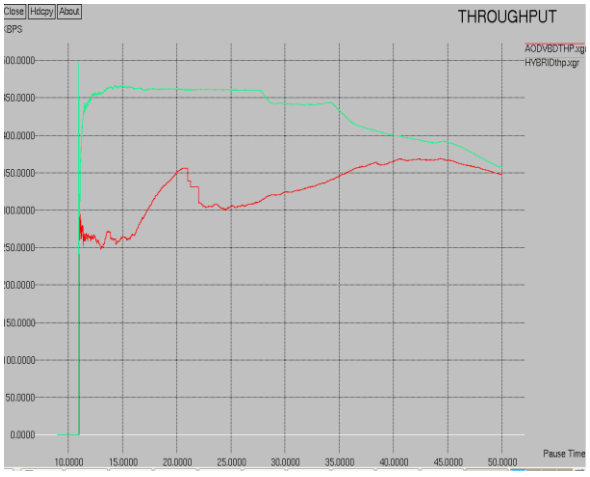
if source node
Intimate to the destination, the count of data packets in a block of data
Send one block of data through the path selected through route discovery process
else if destination node
Compare the data packets received with the data count intimated by the source.
Calculate the probability of packets received at the destination node as PD.
if PD < TPL (the value of TPL is between 0 and 0.2)
Send positive acknowledgement back to source node.
Else
Initiate Gray Hole Attack Discovery Process
end if

The QREQ is used for finding the number of data packets forwarded by that node, to its next hop node. The node an_1 sends back a QUERY REPLY (QREP) packet to the destination node D. The QREP contains the number of data packets a node forwarded to its next hop neighbour in the source route. From the QREP it receives, the destination node verifies whether it's previous hop neighbour (say node an) is correctly forwarding all the data packets it receives from its previous node (node an_1). If not correct, the destination node moves both nodes an_1 and an to the suspected list. If correct, it means that those two nodes are participating correctly in data forwarding. So the destination again sends a new QREQ to the node an_3 which is at 2-hop distance from the node an_1 in the source route. From the QREP it receives, the destination node verifies whether those two nodes an_3 and an_2 are forwarding all the data packets they received. This process continues until the QREQ reaches the node which does not have a previous hop node at 2-hop distance in the source route.

Results and Discussions







5. Conclusion :

We proposed a light weight solution methodology which is a simple acknowledgement scheme to detect gray hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed algorithm, the destination node detects the presence of malicious nodes in the source route and with the help of intrusion detection system the malicious nodes are isolated from the network. Also our IDS nodes will turn into promiscuous listening only in the presence of suspected nodes resulting less energy loss, which makes our method suitable for the resource constrained characteristics of MANET. The simulation results show that the percentage of data packet loss in our proposed work is better than DSR in presence of multiple gray hole nodes.

6. RFERENCES :

[1] Parul Sharma, Arvind Kalia and Jawahar Thakur, "Performance Analysis of AODV, DSR and DSDV Routing Protocols in Mobile Ad -hoc Network (Manet)", Journal of Information Systems and Communication Volume 3, Issue 1, 2012.

[2] Meenakshi Mehla, Himani Mann, "Sbpgp Security Model Using Iodmrp", International Journal Of Computational Engineering Research IJCER May-June 2012 Vol. 2

[3] Ashwini V. Biradar, Shrikant R. Tandle, Veeresh G. Kasabegoudar, "Detailed Performance Analysis of Energy based AODV Protocol in Comparison with Conventional AODV, and DSDV Protocols in MANET", International Journal of Computer Applications Volume 49– No.10, July 2012.

[4] Biswaraj Sen, Sanku Sinha, " A Simulation Based Performance Analysis of AODV and DSDV Routing Protocols in MANETs", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.4, July-Aug. 2012.

[5] Jashanvir Kaur and Er. Sukhwinder Singh Sran, "SBPGP Security based Model in Large Scale Manets", International Journal of Wireless Networks and Communications Volume 4, Number 1 (2012).

[6] Adel.S.El Ashheb, "Performance Evaluation of AODV and DSDV Routing Protocol in wireless sensor network Environment", 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012).

[7] Sachin Kumar Gupta & R. K. Saket, "Performance Metric Comparison of AODV and DSDV Routing Protocols in Manets using NS-2", IJRRAS 7 (3) June 2011.

[8] Akshai Aggarwal, Savita Gandhi, Nirbhay Chaubey, "Performance Analysis of AODV,DSDV and DSR in Manets", International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, Nov 2011.

[9] Abdul Hadi Abd Rahman, Zuriati Ahmad Zukarnain, "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks", European Journal of Scientific Research Vol.31 No.4 (2009).

[10] Maqsood Razi, Jawaid Quamar, "A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET" IEEE 2008.

[11] Shubhranshu Singh, Ashutosh Bhatia, " A DHCPv6 Based IPv6 Autoconfiguration Mechanism for Subordinate MANET", IEEE 2008.

[12] Geetha Jayakumar and Gopinath Ganapathy, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol", International Journal of Computer Science and Network Security (IJCSNS), Volume 07, November 2007.

[13] G Varaprasad and P. Venkataram, "The Analysis of Secure Routing in Mobile Ad Hoc Network", International Conference on Computational Intelligence and Multimedia Applications, IEEE 2007.