Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 11, November -2017

Enhancement of Trust and Security using Cryptography in Mobile Ad Hoc Network

[1]Poonam Yadav, [2]Dr. Shivnath Ghosh

[1]*Dept. of CSE, Maharana Pratap College of Technology Gwalior*

[2]*Associate Professor, Computer Science & Engineering Maharana Pratap College Of Technology Gwalior*

Abstract— *Mobility ad hoc network (MANETs) is less- infrastructure network in which nodes communicate to each other wirelessly. MANET can be attacked easily as compared to wired network. So many methods have been implemented for improving the security of the network. These methods provide confidentiality, non-repudiation. In existing approach, author applies Received Signal Strength technique. In this, node calculates the trust on the basis of signal strength but it has some issues. In our approach, we propose a trust management scheme that improves the security in MANETs. We used multipath and cryptography techniques to effectively detect and eliminate the malicious nodes from the network.*

Keywords— *MANET, Trust, Trust in routing*

I. INTRODUCTION

MANET is a set of mobility devices communicating with every some other without use of any centralized administration. The devices in MANET can circulate freely with seamless connectivity and form a self-structured network. MANET is useful in military communication and other specialized fields e.g. emergency services, and environment monitoring [1] etc. Military applications can't depend on fixed infrastructure based communiqué services in battlefield but MANET is utilized to rapidly self-organize the network and communicate with different node.

There are several elements like scarcity of network resource, dynamic nature applications, topology, etc., which affect MANET's performance. In a dynamic environment like a mobile wirelessly network, Communication is difficult than communicating with a static channel because the link reliability, delay and packet loss aren't determined.

Hence, providing QoS in ad-hoc network is considerably problematic at the receiver, as an outcome degrading consumer experience [2].

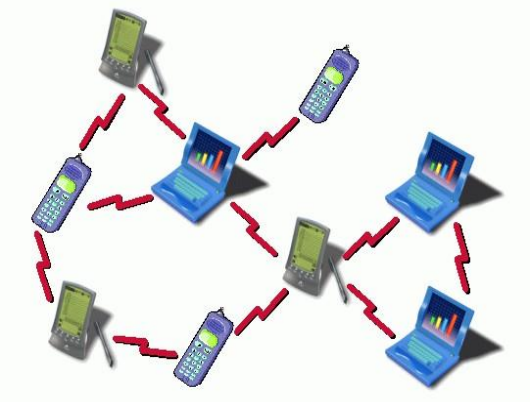

Fig .1 Mobile Networks

II. TRUST

A common place definition considers believe to be a measure of subjective notion that one man or woman or celebration makes utilize of to examine the chance one or more can participate in a good action before the chance presents itself to observe whether or not that activity has occurred. Once an individual is taken into account trustworthy, it's meant that there's a high chance that the actions they're expected to perform are done in a way that's favorable to trusted. In MANET believe shall be outlined as a degree of belief in line with the conduct of nodes, the chance price of believe is variable from zero to at least one where zero represents completely distrust and one represents fully trust. Providing trust model in ad hoc networks is primary so it gains greater protection level and improves efficiency inside the community. The dynamics of this has contributed to three fundamental evaluation areas within the discipline of trust administration for allotted ad-hoc networks. This includes work focusing on trust Propagation, trust Aggregation and believe Prediction [3].

III. TRUST IN ROUTING PROTOCOLS

Author needs that receiver nodes obtaining data packets respond to the source node with a signed acknowledgement. This acknowledgement consists of the packet's unique identifier, concatenate with the receiver node's address. If the no. of unacknowledged packets exceeds a threshold, then a fault detection protocol is utilized, just like the Secure Trace path protocol defined via Simon and Padmanabhan. In any next data packets, the source transfer at the identical path, it consists of a „probe listing"; this carries the addresses of the intermediate nodes from which the originator require an acknowledgement, with the receiver node's address as last entry. The list consists of a HMAC which is recursively produced, all round utilizing a secret key shared among the source node and the intermediate node being „probed", this is a method additionally called to as „onion encryption. When a probed middle node receives the probe listing, it decrypts a layer of the onion encryption and confirms the HMAC prior to forwarding the packet, so that the next intermediate node inside the probe listing can affirm that it is appropriate to the list.
After forwarding, a probe list, a middle node delays for an acknowledgement from the subsequent node on the probe list. If one isn't obtained with a selected timeout interval, then the node must initiate an acknowledgement chain through making an acknowledgement. The timeouts are calculated in such a way that the last probed node that fully obtains the packet will always start the chain of acknowledgment. Thus, when the route is working, this will be the receiver node. This acknowledgement chain is forwarded towards the initiator node.
The originator node decrypts each layer of the final acknowledgement packet, verifying the HMAC within each layer to confirm that the corresponding intermediate node received the packet. The originator can use this probe protocol to perform a binary search by adding the intermediate node in the middle of the route to the probe list of successive data packets, halving the route being searched after every iteration. A broken link is discovered when an expected acknowledgement isn't accepted from a middle node at position *i* in the probe list, but an acknowledgement is accepted from the middle node at position *i* - 1. [4]

IV. TRUST METRICS

Trust is evaluated on different metrics and dissimilar ways. Some schemes use continuous or discrete values to measure the level of trust. For Example, trust is described by a continuous value in [0, 1] or measured as discrete cost. Threshold primarily based procedures are also utilized to measure agree with. Trust metrics comprise opportunity primarily, mobility, fuzzy, similarity, context depend factors like signal power, strength etc.

V. PROPERTIES OF TRUST

A trust decision framework must now not paintings underneath the aim that each one node is helpful for MANETs. Trust must be determined in a highly customizable way without communicational load and excessive computation.

- Trust isn't static, it's dynamic.
- Trust is depending on context [5]

VI. LITERATURE SURVEY

Shimmi Singh Rathour [6] et al. presented that they apply the trust approach which is calculated via dempsters shafer theory, after calculating trust they apply SVM to categorize nodes behavior. On the basis of categorization we detect malicious behavior of nodes. The simulation is performed on NS-2.35; with the aid of these techniques we improve network efficiency in the form of throughput or PDR.

Raihana Ferdous [7] et al. presented that secure routing is a vital issue in MANET as mobility nodes are prone to attacks from malicious nodes and the overall performance of the n/w depends on it. Three routing protocols have been study and equated: OLSR, AODV and DSR. The metrics being utilized are Delay, Throughput and PDR. NS2 has been utilized as tool for the experiments. The performance study of those protocols is also compared for power utilization using believe-based model: TLEACH and Node based Trust Management (NTM) Scheme. Simulation outcomes show that OLSR protocol performs well compared to AODV and DSR

Sapna B Kulkarni [8] et al. presented that a trust based clustered algorithm in which for every movable devices in the network the trust value is evaluated and the devices with least trust value are rejected as malicious nodes. The nodes are inserted to the friend list depend on the calculated trust level. The friends having a highest trust level are qualified to become CH. The nodes with least trust values are considered as malicious and are eliminated from the friend list. The algorithm employees the following step: a) Challenge your neighbors b) Rate your friends c) Share friends and Route through friends**.**

Rahul Talreja [9] et al. presented that the approach define the thought of Trust Variable Factor (TVF) that enables to identify mischievous nodes in MANET. Utilizing TVF, a number of data transmitted to discover misbehaving nodes may be decreased to an extra extent. The method can adapt to varying QoS needs and would result in good throughput and

performance.

Arvind Kushwaha [10] et al. presented that, a novel solution way to transmission server load from one server to different server. Energy efficiency is an element for operation of ad-hoc n/w. Define algorithm will divert the load from lowest energy node to highest energy node. The complete proposed solution will work to find multipath routing for and congestion control and load balancing for MANET.

Siddhant Dodke [11] et al. presented that, assessment between ordinary general execution of DSR and AODV is executed. They have also analyzed the routing protocol AODV as well as DSR utilizing NS-2 simulator; the obtained results show that DSR consume 40% less energy as compared to AODV.

V. Sameswari [12] et al. In this paper, the MANET plays a significant role in networking research environment for sharing information from one to others. MANET is a mobile, which is formed via radio signal without any desirable base stations. The main issue of DSDV is routing overhead continuously, because it maintains the update information during data transmission. The DSR protocol's drawback is route creation delay during route building and end-to-end delay during transmission. To explain the above issue, this paper proposed an inventive approach called Hybrid of Destination Sequenced and Dynamic Source routing protocol (HDS2) in MANET. The novel method of HDS2 improves the PDR & throughput and minimizes route creation and end-to-end delay. The defined approach has been tested and implemented in NS2 simulator and finally it"s compared with existing DSDV routing protocol.

Safaa LAQTIB [13] et al. In this paper, they have studied the performance of many mobility replica specifically: Gauss Markov Mobility replica and Random Direction having changeable amount of nodes and Random walk. The empirical outcomes recommend that OLSR protocol using Random Waypoint mobility replica has better outcomes for dissimilar number of nodes.

VII. PROPOSED WORK

In our proposed work, we used multipath and cryptography techniques to effectively detect and eliminate the malicious nodes from the network. Firstly, we select source and destination nodes and if the source has a data to send then it finds the multipath by applying multipath source routing protocol. Then at each path, we calculate the reputation value of nodes and MD5 algorithm used for every communication. This ensures the integrity data and also provides the security to the network by ensuring that only authenticated nodes can communicate. If the reputation is greater than threshold value then it"s considered as reputed node else it is a malicious node and it can be removed from the network.

Proposed Algorithm

Step 1: initialize network
Step 2: select source S and
destination D nodes Step 3: if S
had data
Then find multipath by using multipath
source routing Else
Wait for data
Step 4: generate hash value of every message by using
MD5 algorithm Step 5: if nodes are authentic then
{
Calculate confidence value every of
their neighbours $CV_{ij} = f_{ij} - d_{ij}$
Where f_{ij} = No. of packets forward from node j
to other nodes d_{ij} = No. of packets drop by node
j
Step 6: if CV > threshold
{
Find reputed node from all neighbours
$rep_h^{(n)} = \max(rep_1^{(n)}, rep_2^{(n)}, \ldots\ldots, rep_m^{(n)})$
Step 7: If reputation value > threshold
Reputed node
Step 8: Else
Malicious node and eliminate
from network Exit
}
Step 9: Else
Exit
}

Step 10: Else
Non-authentic node
Exit

VIII. RESULT ANALYSIS

Network Simulator version 2 (NS2) is a tool which is utilized to implement the proposed approach to demonstrate the performance of the work. We compare the base technique with the proposed method to illustration the efficiency of the work.

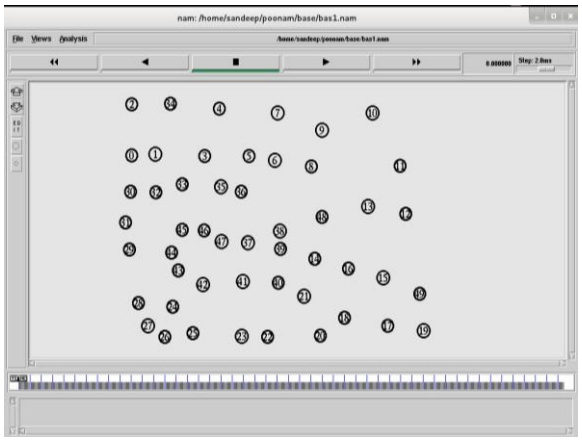

Fig.4 Initialization of network

The figure below shows that all source nodes search the path for the transmission of data towards the receiver and transmit data between the nodes.

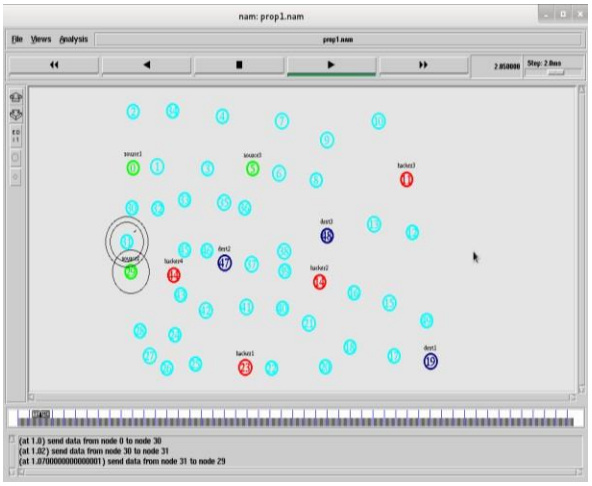

Fig.5 Data transmission start

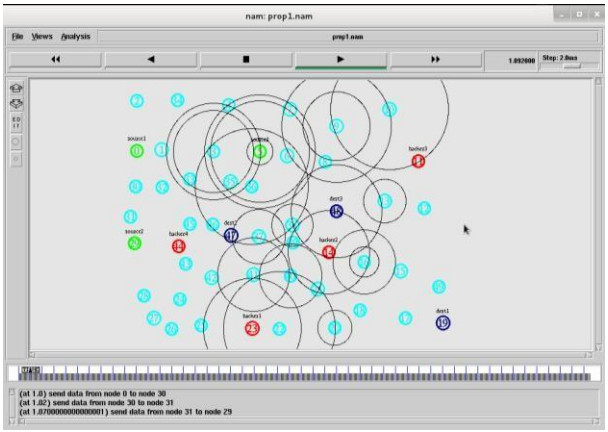

Fig.6 All source start data sending

We have described the parameters table with their values to show the default values for the simulation:

Table 1: Parameter Table with their Values

Parameters	Values
Simulation Used	NS2
Network Size	1526m x 135m
Number of Nodes	50
Simulation Time	50s
Antenna Used	Omni directional Antenna
Packet Size	1500 bytes
MAC Protocol	IEEE 802.11

Packet Delivery Ratio (PDR):
It outlines the proportion of packets transport from supply towards destination. The graph show a PDR graph among base approach as well as proposed approach. This PDR rate is best in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

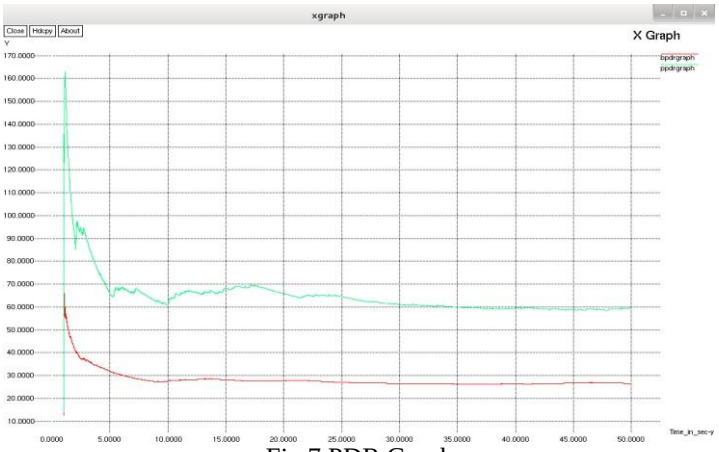

Fig.7 PDR Graph

Packet Drop:
The difference in quantity of packets received than the no. of packets sent is known as packet drop. From the graph, it is shown that the proposed work is improved than the existing work as the no. of packets drop is less in the proposed work.

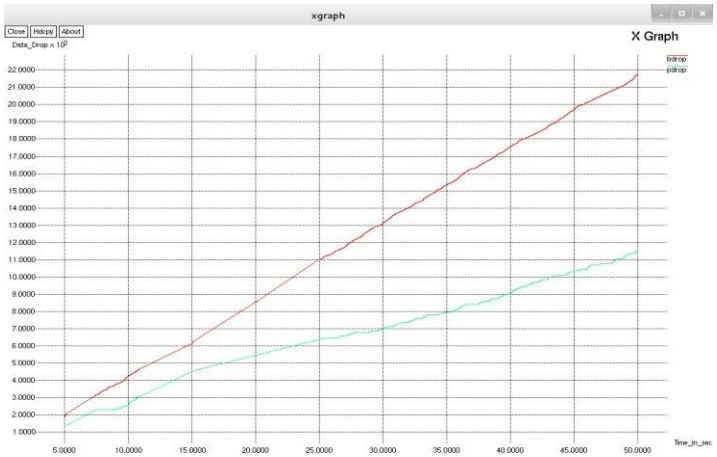

Fig.8 Packet Drop Graph

Throughput:
The rate of successful data packet delivery from one node to another over a communiqué channel is known as throughput. The graph represents an output graph among base approach moreover as projected approach. The output of the projected approach is better than the present approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

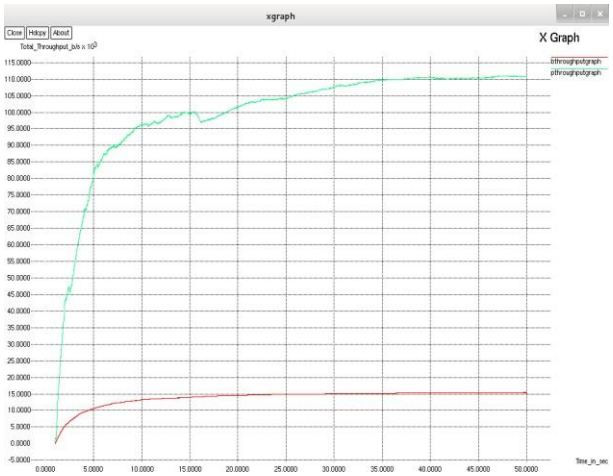

Fig.9 Throughput Graph

IX. CONCLUSION

A MANET is a type of ad hoc n/w which can communicate by the nodes and forwards the data when they have data to send . Because MANETS are mobility, they use wirelessly connections to link too many networks; there are various security vulnerabilities which can be attacked by malicious users. These type of attacks are basically unfeasible to detect, so making it difficult to produce security for such attacks. In MANET, believe is the degree of perception about the behaviour of dissimilar entities (or agents). i.e. The trust that node A places in a node B is the strength of node A's belief that node B will behave without malicious intent, and the service that node B provides will be according to node A"s expectation. The degree of Trust is the perception possibility varying from 0 (complete distrust) to 1 (complete trust). So we eliminate the malicious nodes from the network which aid in achieving the security for the nodes.

References

[1] I. Chlamtac *et al*., "Mobile ad-hoc networking: Imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13-64, 2003.

[2] V. T. Raisinghani and S. Iyer, "Cross-layer design optimizations in wireless protocol stacks," *Computer Communications*, vol. 27, no. 4, pp. 213-217, 2006.

[3] Mrs. S. Geetha, Dr. G. Geetha Ramani, "Survey of Trust Based Routing Protocols in MANET", ISSN: 2277 128X/ Volume 4, Issue 10, October 2014

[4] Shane Balfe, Po-Wah Yau and Kenneth G. Paterson, "A Guide to Trust in Mobile Ad Hoc Networks",911NF-06-3-0001.

[5] Vijayan R, Jeyanthi N. "A Survey of Trust Management in Mobile Ad hoc Networks" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 4 (2016) pp 2833-2838.

[6] Shimmi Singh Rathour, Nitin Manjhi, Trust Base Hybrid Approach for detection and Prevention MANET from Attacks", 978-1-5090-2080-5/16/$31.00 ©2016 IEEE

[7] Raihana Ferdous, Vallipuram Muthukkumarasamym, "A Comparative Performance Analysis of MANETs Routing Protocols in Trust-based models", 978-1-5090-5510-4/16 $31.00 © 2016 IEEE

[8] Sapna B Kulkarni, Dr. Yuvaraju BN, "Rating and Friend sharing algorithm of Trust based clustered routing algorithm in MANETS", 978-1-5090-4620-1/16/$31.00 ©2016 IEEE

[9] Rahul Talreja, SriPradha Sathish, Kamlesh Nenwani, "Trust Variable Factor A Trust based method to detect Misbehaving Nodes in MANET" 978-1-4673-9939-5/16/$31.00 ©2016 IEEE

[10] Arvind Kushwaha, Prof. Nitika Vats Doohan "M-EALBM: A Modified Approach Energy Aware Load Balancing Multipath Routing Protocol in MANET" 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[11] Mr.Siddhant Dodke, Dr. P. B. Mane and Mrs. M.S. Vanjale "A SURVEY ON ENERGY EFFICIENT ROUTING PROTOCOL FOR MANET" 978-1-5090-2399-8/16/$31.00 ©2016 IEEE.

[12] V.Sameswari, E.Ramaraj "An Innovative Approach of HDS2 Routing Protocol In MANET" 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).

[13] Safaa LAQTIB, Khalid El YASSINI, Meriem HOUMER Moulay Driss EL OUADGHIRI, Moulay Lahcen HASNAOUI "Impact of Mobility Models on Optimized Link State Routing Protocol in MANET" 978-1-5090-3837-4/16/$31.00 ©2016 IEEE.

