iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improved Performance by Trusted Path Under Various Attacks in Mobile Ad Hoc Network

Bishnu Kumar Sharma[1], Manish Khule[2]
[1] M. Tech, CSE, GITS College, [2] Asst. Prof. of CSE dept., GITS College

Abstract: ***MANET is self-configuring, autonomous and dynamic infrastructure in which the nodes can acts as hosts as well as router in the network. MANET is having an open-source, decentralized, and dynamic infrastructure which means that it does not have any monitoring node to configure and monitor the network which makes it less secure and makes it easy for the attackers to break the network or come in between the transmitting. In the existing work they have executed an IDS system to identify black hole and gray hole attack under AODV protocol. They have been defined DTQ (Data Transmission Quality) which is being considered, if the value of the DTQ is greater than threshold then if the DTQ is not greater then voting will be done and if not the node will get prepared for the communication. Voting is done on the basis of number of positive and negative nodes. If the amount of positive nodes are more than the node will stay in the network otherwise marked as blacklisted and each node will get message and it will be cut off from the network. We performed the trust calculation of the nodes in the network which established the secure path for the transmission of data from source to destination.***
Keywords: Manet, IDS, IDS technique, black hole attack, Grey hole attack.

I. INTRODUCTION

As the importance of computer increases it also build up the connectivity demand. Wired solutions are utilized from a very longest period, but the demands for wirelessly solution are growing for linking to the Internet, exchanging data, transmit and obtain mail messages and so forth. Mobility Ad-hoc community (MANET) is a totally done studies place. MANET is a wirelessly advert hoc community. A MANET can be linked to web or outside network and can be a standalone network. MANET is a Latin word that means “for this,” or “for this purpose only”. In a MANET, nodes within their wireless transmitter can communicate with each other directly while nodes outside the range have to rely on some other nodes to relay messages. When a multi hop situation arises, the packets directed thru the sender multitude are relayed thru many middle hosts earlier reaching the endpoint host. The success of communiqué based on the different nodes cooperation [1].

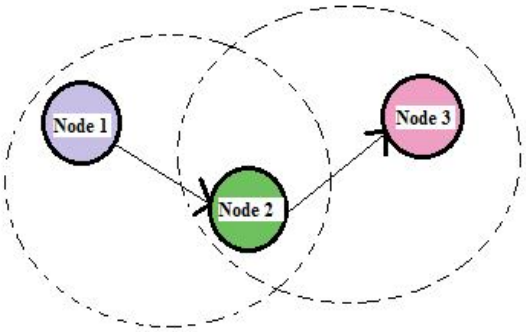


Fig. 1 Example of mobile ad-hoc network

II. INTRUSION DETECTION SYSTEM (IDS)

Intrusion is any group of actions which attempt to contain the confidentiality or availability, integrity. IDS are software or tool which observers site visitors community and if any suspicious hobby determined then it signals the device or n/w administrator. There are three major element of IDS are Analyses, Response and Monitoring. The Monitoring Module is responsible for controlling the collection of data. Analyses Module is responsible for deciding if the collected data indicated as an intrusion or not. Response Module is responsible for manage and using the response actions to the intrusion.

Due to the constraints of maximum MANET routing protocols, nodes in MANETs suppose that other nodes usually cooperate with every other to relay facts. This supposition leaves the attackers with the chances to attain important impact on the n/w with just one or two compromised nodes. To triumph over this difficulty, IDS should be put in to decorate the safety level of MANETs. If

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

MANET recognizes how to the detect the attackers as soon as they arrives in the n/w, we will able to wholly eliminate the potential damages caused thru compromised nodes at the major time. IDS typically info as the second layers in MANETs. it's a great accompaniment to present proactive method. So IDS is very significant aspect of defending the cyber substructure from attackers.

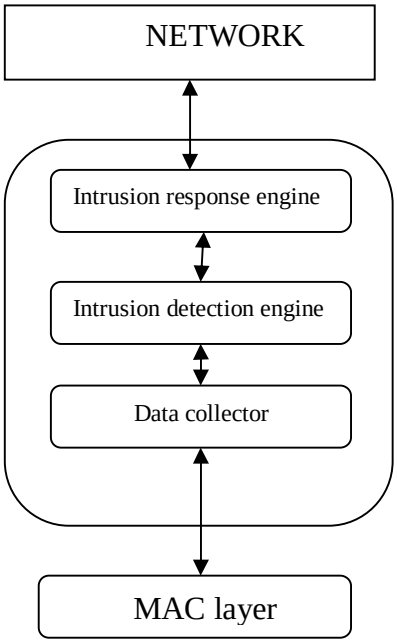


Fig 2. Intrusion detection system [2]

III. IDS TECHNIQUE IN MANET

One of the distinctive form of misbehaviours a node may also show is selfishness. A selfish node wants to preserve its own resources while using the services of others and consuming their resources. There are two approaches for dealing with selfish nodes. The first one gives a motivation for participating in the network function. The second approach detects and excludes misbehaving nodes. Most existing systems belong to the second type. These systems use extra facilities or specific algorithms to detect misbehaving (selfish) nodes in MANET and exclude them from the routing path.

A. Mitigating Routing Misbehaviour in MANET: Watchdog / Pathrater

The Watchdog/Pathrater is a result to the issue of selfish nodes in MANET. The device offers two extensions to the DSR algorithm to mitigate the consequences of routing misbehaviour: The Watchdog, to locate the misbehaving nodes and the Pathrater, to reply to the intrusion via isolating apart the selfish node from the n/w operation.

Watchdog runs on every node. When a node forwards a packet, the node's watchdog thing verifies which the following node in the path also forwards the packet. The Watchdog does this with the aid of listening in promiscuous mode to the following node's transmissions. If the next node does now not ahead the packet, then it's miles taken into consideration to be misbehaving and is said.

This is done by sending an alarm message to the other nodes on its friends list. When those nodes receive the alarm message, they evaluate it and change the reputation of the accused node only if the alarm source is fully trusted or the same node was accused thru many partially trusted nodes.If the Watchdog module that detected the misbehaving node is not in the same node that is acting as source node for the packets, then it sends a message to the source recognizing the misbehaving node.

The Pathrater module makes utilize of the data generated by using Watchdog to select a better path to supply the packets, heading off the selfish nodes [3].

IV. BLACK HOLE ATTACK

Black Hole Attack, is one of the security attacks in which malicious node promotes itself as a node which has shortest path from

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

source to destination. Black Hole Attacks are classified into: Single Black Hole Attack and Cooperative Black Hole Attack.

A. Single Black Hole Attack

These are the attacks in that handiest one node act as malicious node in entire n/w.

B. Cooperative or Collaborative Black Hole Attack

these are the attacks in which multiple nodes as a group act as malicious nodes. Its define that once a node requirements to transmit facts to any distinctive node in n/w, it transmit a RREQ message to each its nearby that can contain the malicious node as well. If any node has fresh route from itself to destination, it responds to RREQ message. If the reply from regular node reaches the supply node first, entire transmission works nicely, but if respond from malicious node reaches source first, it makes supply node think that the route discovery technique is entire and it starts of evolved sending messages thru malicious node. As a outcome, each the packets transmit thru despatcher to endpoint thru the malicious node get lost. The complete scenario of black hole attack is shown in Figure 1 and explained below.

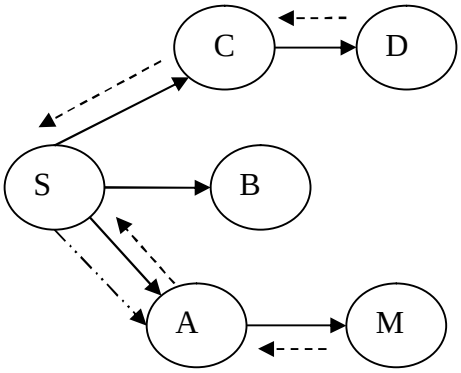


Fig 3 Black hole attack

RREQ-
RREP
DATA

C. Here M is the black hole

Here node S is the source node which wants to have communication with node, D considered as destination. Thus, node S will first ship a RREQ message to all its nearby namely A, B and C. If node A has a direction to D, it'll dispatch a RREP message to S. But node M being the malicious node will send a fake RREP thru A with very high destination collection. As a result, S will assume that path from S to D via A is the shortest and it will indirectly send data to Black Hole node (M) thinking that there exists a path to D via A. Because of which the whole data gets trapped instead of reaching to destination [4].

V. GREY HOLE ATTACK

Grey Hole attack is a unique case of Black Hole Attacks in MANET. As we have already discussed in the previous section that in a black hole attack, the, malicious node creates an illusion that it has the shortest path from source to destination and attracts all the packets towards it, thereafter it drops those packets. So it is certain that it will drop all the packets, however in a grey hole attack it may or may not drop all the packets. It does not have a uniform behavior, at one point it may drop certain packets and send some to other nodes. In another situation it may behave maliciously and then suddenly it might switch to normally behaving node. Grey hole attack detection turn out to be more dangerous when both the above described possibility is combined.

Existing Solution to avoid Grey Hole Attack: one of the solutions to avoid this type of attack is that suppose a node is behaving in a malicious manner, there is messaging criteria where all the other nodes apart from the malicious nodes will be notified about the malicious behavior of the node. In this manner we are able to isolate this node from other normal nodes and disallow this node to use networks resources.

A. To execute this solution, we will be requiring four sub tasks

1) Neighborhood data collection – in this task DRI(Data Routing Information) table is maintained containing the data forwarding information pertaining to neighboring nodes.
2) Local Anomaly detection- This is triggered by a node if it comes across a suspicious node by cross checking its DRI table.
3) Co-operative anomaly detection module – this task improves the detection criteria by reducing the false detection of local anomaly detection procedure.
4) Global Alarm Raising Module- This task send alarming messages across the network about the grey hole node in the network. This also makes sure that the malicious nodes are isolated from the network and cannot use any network resources.[5]

VI. LITERATURE SURVEY

Koichi Hirai(2017)et al presents about building a social MANET with the terminals of the member of the same SNS group using a community token to identify the group members. The community token has been defined, and the methods of generating, updating and sharing a community token have been presented. The paper has also proposed a routing method that takes account of the amount of resource usage that can be tolerated by relay nodes [6]

Kiyotaka Kaji (2017)et al presents about an algorithm and a routing scheme to compute and utilize detour paths adaptively according to the network traffic conditions. Through evaluation, we show that the proposed scheme improve the communication performance by using the detour paths in practical network scenarios. a method to adaptively reroute packets to detour congestion area in MANET. Our method detours packets when they meet congested area using only one additional routing table and an additional header field. The detour routing table is computed from the 2-hop neighbor information so that we can add the detour function to any type of shortest-path-based routing protocol via periodical hello message exchange. Simulation results shows that the proposed method improve the communication performance in multiple practical scenarios. [7]

El Mostapha (2017) et al presents about the impact of certain alerts generated by IDS on the security status of an information system, also improve the detection of intrusions using snort by classifying the most critical alerts by their levels of risk, thus, only the alerts that presents a real threat will be displayed to the security administrator, so, we reduce the number of false positives, also we minimize the analysis time of the alerts. The model was evaluated using KDD Cup 99 Dataset as test environment and a pattern matching algorithm [8].

Xiaonan Wang (2016) et al presents an ancyast-depend contentcentric MANET (ACCM) to decrease the content acquisition cost and to recover the content acquisition success rate. In ACCM, sources form an any cast set and a customer can obtain the chosen contents from the nearest anycast member in the unicast way. ACCM based on addresses to return the requested contents to a customer, so the content acquisition failure caused thru reverse-path disturbances is circumvented. Finally, ACCM is analyzed and evaluated, and the data show that it reduces the content acquisition cost and improves the success rate [8]

Sachi N. Shah (2016) et al presents about a new secure trust based routing scheme which is combination of social and QoS trust. The primary goal of our proposed scheme is to mitigate nodes performing various packet forwarding misbehaviors. We calculated four parameters for trust which are control forward ratio, data forward ratio, intimacy and residual energy. We present adversary model of the packet dropping attack against which our trust-based scheme is evaluated. Simulation outcomes in NS-2 illustrate which the define method recovers performance of PDR [9].

Seemita Pa (2016) et al presents online mechanism for discovering gray-hole attacks in real-time. The define device utilize the timing data inherent in the PMU info for discovering packet drop attacks, and doesn't impose any overheads or necessitate any support from the network infrastructure. Outcomes are presented to confirm the accuracy effectiveness and of the define detection mechanism below dissimilar network circumstances [11].

Pooja (2015) et al. presented that, Here Hint-depend Probabilistic routing protocol is utilized to define a local utility function depend method to detect black hole nodes. Then evaluation of the network performance in the presence of a black hole and in the nonexistence of black hole utilizing dissimilar performance metrics as packet delivered throughput and overhead ratio and packet drop in the network. ONE simulator is utilized to simulate Black Hole attacks [12].

VII. PROPOSE WORK

In the existing work they have executed an IDS system to identify black hole and grey-hole attack under AODV protocol. They have been defined DTQ (Data Transmission Quality) which is being considered, if the value of the DTQ is greater than threshold then if the DTQ is not greater then voting will be done and if not the node will get prepared for the communication. Voting is done on the basis of number of positive and negative nodes. If the amount of positive nodes are more than the node will stay in the

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

network otherwise marked as blacklisted and each node will get message and it will be cut off from the network.

But the problem with this approach is that if the amount of votes came out to be positive due to any cause like fault in the network or the malicious node incorrectly votes then it will stay in the network. So to overcome this drawback we have proposed another technique which is applied when the true positive results come.

We performed the trust calculation of the nodes in the network which established the secure path for the transmission of data from source to destination. Initially flood the network with route request packet which should be received by each neighbour node. We find the multiple routes for the data transmission but the path should be shortest. Then send the data by finding the secure and trustful path which makes them more efficient and reliable for data transmission.

A. Proposed Algorithm

Step:1 initialize the network
Step:2 broadcast Route Request packet in the network
Step:3 then wait for the response
Step:4 destination send Route Reply packet to the source with shortest available paths
Step:5 select 3 shortest routes between source and destination
Step:6 calculate the trust value of each node
Step:7 find the trust average of each path
Step:8 send the data from the highest trusted path
Step:9 exit

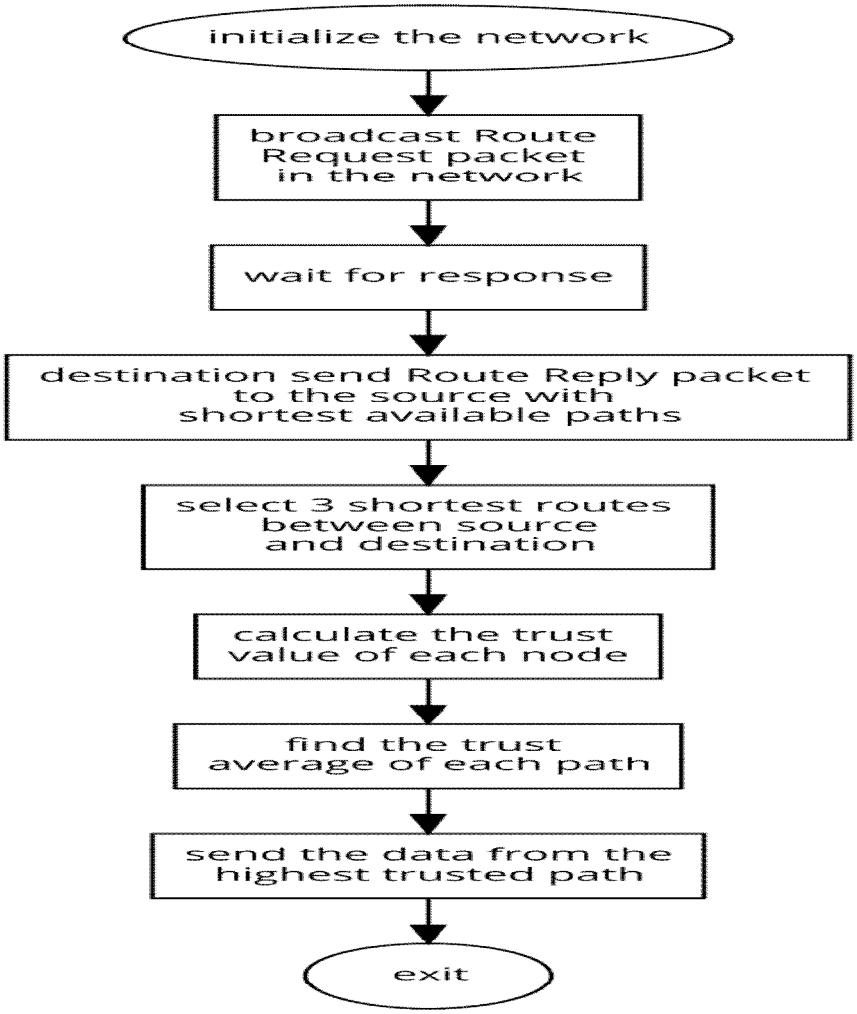


Fig.3 Flowchart of Proposed Algorithm

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VIII. RESULTS

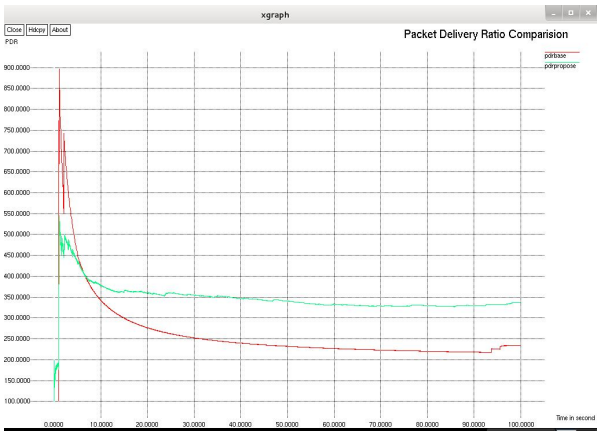


Fig. 4 PDR

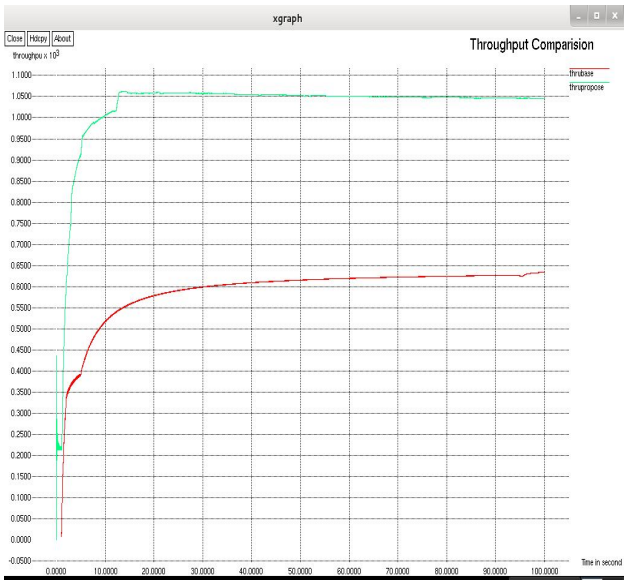


Fig. 5 throughput

Fig. 6 Routing overhead

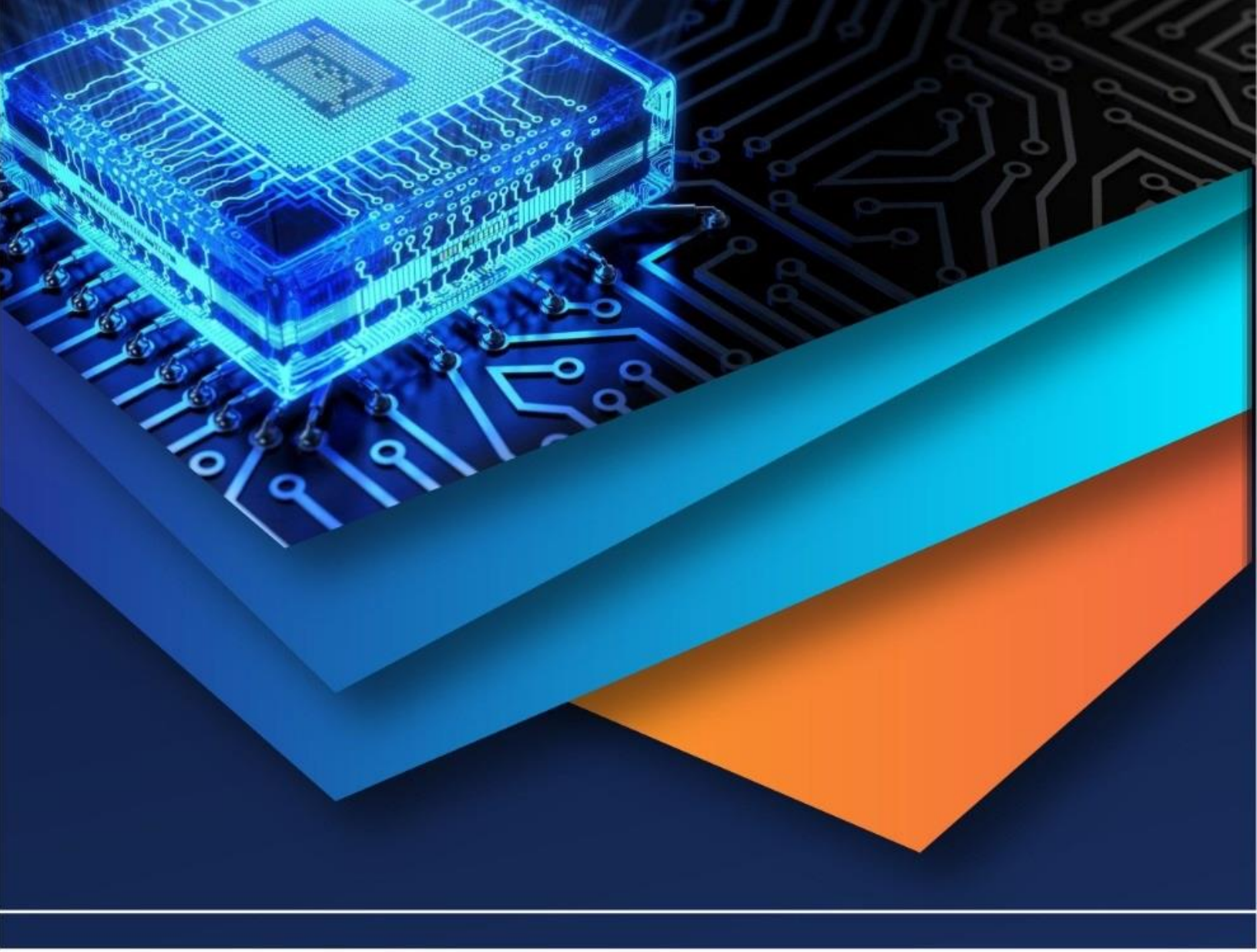
IX. CONCLUSIONS

Manets are of enormous use in today's world. In many situations where the wired networks or even the straightforward wireless networks could not be used, but manet due to its various significant properties are useful in those situations. But as it is having adaptive environment it is more likely to be vulnerable by amount of attacks. Some of them are black hole attack, modification, gray hole attack, flooding attacks etc. I have considered various approaches in detail for the detection and elimination of black hole and gray hole attack and proposed a explanation which is proficient and secure for both types of attacks. In the proposed work we have given a secure and efficient way for the discovery and deduction of gray hole attack in (manet). The algorithm for this is mainly implemented in aodv protocol. We have proposed an algorithm for the calculation of trust for each nodes of all path. Then transmit the packets from source to destination from the secured path.

In the future work, we can use other techniques which provide the more efficiency and security in the network.

REFERENCES

[1] Meenakshi Yadav , Nisha Uparosiya, " Survey on MANET: Routing Protocols, Advantages, Problems and Security", International Journal of Innovative Computer Science & Engineering,@2014
[2] Ranjit j. Bhosale, Prof. R.K.Ambekar, "A Survey on Intrusion detection System for Mobile Ad-hoc Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7330-7333
[3] Charlie Obimbo, Liliana Maria Arboleda-Cobo, "An Intrusion Detection System for MANET", CISME Vol.2 No.3 2012 PP.1-5 www.jcisme.org ○C 2011-2012.
[4] Neha , Manmohan Sharma, "A Survey on Black Hole Attack Detection and Prevention Techniques" , ©IJRASET 2015
[5] Vishnu Sharma, Akansha Vij, "rity Issues in Mobile Adhoc Network: A Survey Paper" , ISBN:978-1-5090-1666-2/16/$31.00 ©2016 IEEE
[6] Koichi Hirai, Kazumasa Takami, "Building A Social MANET based on An SNS Community Token" , 978-1-5090-6231-7/17 $31.00 © 2017 IEEE
[7] Kiyotaka Kaji ,Takuya Yoshihiro, "Adaptive Rerouting to Avoid Local Congestion in MANETs" , 978-1-5090-4183-1/17/$31.00 ©2017 IEEE
[8] El Mostapha CHAKIR, Mohamed MOUGHIT and Youness IDRISSI KHAMLICH, "An Effecient Method for Evaluating Alerts of Intrusion Detection Systems", 978-1-5090-6681-0/17/$31.00 ©2017 IEEE
[9] Xiaonan Wang and Xiaojian Zhu, "Anycast-Based Content-Centric MANET" , 1937-9234 © 2016 IEEE.
[10] Sachi N. Shah , Rutvij H. Jhaveri , "Trust-Based Scheme against Packet Dropping Attacks in MANETs", 978-1-5090-2399-8/16/$31.00 c 2016 IEEE
[11] Seemita Pal, Biplab Sikdar, "Online Mechanism for Detection of Gray-Hole Attacks on PMU Data" , 1949-3053 (c)2016IEEE
[12] Pooja, Dr. R. K. Chauhan, "AN ASSESSMENT BASED APPROACH TO DETECT BLACK HOLE ATTACK IN MANET", ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY