iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** I **Month of publication:** January 2021

DOI: https://doi.org/10.22214/ijraset.2021.32787

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue I Jan 2021- Available at www.ijraset.com

Distributed Profile Evaluation Approach to Prevent DDOS Attack in MANET

Vinita Kushwaha[1], Kailash Kumar Patel[2]
[1]*M. Tech. Scholar,* [2]*Assistant Professor, Department of Computer Science Engineering, Technocrats Institute of Technology Advance, Bhopal, India*

Abstract: ***In the Mobile Ad-hoc Network (MANET), nodes connect with each other in the absence of any centralized authority on the grounds that stability is one of the big problems (MANET). Due to the peculiar features of MANETS, the protective architecture of MANETS poses a variety of consequential problems. The DDoS attack is not easily identified in network. In order to resolve the obstacles, a security system has to be placed in place that achieves both extensive safety and desirable network efficiency from attacks. In mobile ad hoc networks where network topology varies animatedly, straight approaches cannot be used effectively. Various DDoS protection schemes improve the performance of the network in the presence of an intruder to disable misbehavior operation and one of the recent is NTRS. In this research, proposes the Distributed Profile Evaluation Approach to Prevent (DPEAP) DDoS attack effect in the network that throws out compromised packets in the network outside the capability of the network. The NTRS was a recent research technique and the proposed DPEAP is a newly propose technique. The DPEAP identifies the attacker's actions by comparing the attacker's profile to the usual nodes on the network if the node profile is normal in the foam of the right data distribution on the network, then the DPEAP announces that the network has no threat, so if the attack is detected, the DPEAP would be aware of the attacker node on the network and will therefore retain the attacker's profile and count the information. The DPEAP scheme is secure and reliable as compare to NTRS scheme in MANET.***

Keyword: DDoS Intruder, MANET, DPEAP, AODV, NTRS, Routing

I. INTRODUCTION

The Mobile Ad-hoc Network (MANET) is made up of a temporary network, without the need for central management or traditional support equipment available in a conventional network, thereby forming an infrastructure-free network.[1] [2]. Popular uses of MANET are in military or police networks, industrial activities such as oil drilling platforms or mining operations, and emergency response operations such as flooding, tornadoes, hurricanes and earthquakes [3]. Due to multi-hop routing and an open operating environment, MANETs are vulnerable to attacks by greedy or malicious nodes, such as packet drop (blackhole) [4] attacks and flooding DDoS attacks [5]. Wormhole attack is a form of attack that acts as the route between the sender and the recipient, except if the sender has initiated data transmission [6].

Intuitively, intrusions in an information system that violate the system's security protocol, and the mechanism used to classify intrusions is intrusion detection. For about 20 years, intrusion detection has been researched. It is founded on the premise that the behavior of an attacker will vary greatly from that of a legal person and that several illegal acts will be observable. As a second level of protection that defends information infrastructure, intrusion detection systems (IDSs) are typically implemented along with other protective security measures, such as access control and authentication [7]. There are a variety of reasons for making intrusion detection a necessary aspect of the whole defense mechanism. First without protection in mind, many conventional systems and applications have been developed. In other instances, systems and applications have been designed to run in a particular context, and when implemented in the current environment, they may become vulnerable. (For example, when it is inaccessible, a device may be completely safe, but when connected to the Internet, it becomes susceptible.) Intrusion detection provides a way to recognize and thereby facilitate responses to attacks against these systems. Second, operating systems and applications which have design vulnerabilities or glitches that may be exploited by an attacker to target the systems or applications due to the shortcomings of information technology and software engineering experience [8]. Some prevention measures cannot be as successful as planned (e.g., firewalls).

II. IDS OVERVIEW

Detection of attack complements these defensive measures to increase the protection of the device. In addition, even though information networks can be effectively secured by preventive protection measures, it is also desirable to know what intrusions have arisen or are occurring, so that we can identify the security challenges and risks and therefore be properly prepared for possible attacks [7].

IDSs, despite their significance, are not substitutes for protective security measures, such as access management and authentication. IDSs themselves will of course, not have appropriate securities for information systems [8]. If an attacker erases all the data in an information system, detecting the attacks will not reduce the damage at all as a drastic example. Thus as part of a robust defense framework, IDSs should be deployed along with other preventive protection measures. Techniques for intrusion detection are generally divided into two methods: detection of irregularities and detection of misuse.

Detection of deviations is based on a subject's normal behavior (e.g., a person or a system); any action that deviates significantly from normal behavior is considered to be intrusive. In terms of the features of known threats or device vulnerabilities, exploitation detection captures intrusions; any behavior that conforms to the pattern of a known threat or susceptibility is called invasive. Alternatively, according to the origins of the audit information used by each IDS, IDSs can be categorized into host-based IDSs, dispersed IDSs, and network-based IDSs [9]. Host-based IDSs collect audit data from host audit trails and typically target attacks against a single host to be detected, distributed IDSs collect audit data from multiple hosts and probably the network connecting the hosts to detect attacks including several hosts. As an audit data point, network-based IDSs use network traffic, relieving the load on hosts that normally offer standard computing services.

III. LITERATURE SURVEY

Gurveen Vaseer, Garima Ghai, Dhruva Ghai, and Pushpinder S. Patheja [10] "A neighbor trust-based mechanism to protect mobile networks" This title addresses MANET, its numerous relevant problems, and selected solutions. A neighborhood trust-based protection framework that can stop malicious attacks in a MANET is explored in depth as a case study. The protection scheme defines the behavior of each node in the network in terms of collected and forwarded packets. Nodes are put in a suspect range and if malicious is detected by the protection scheme Acting constantly, it is then confirmed that the intruder in the network is the same node.

Divya gautam prof. Vrinda tokekar [11] “an approach to analyze the impact of DDOS attack on Mobile cloud computing" in this title also observes that resource drainage is completely independent and does not lie on routing protocol vulnerabilities." Denial of Service attack and Distributed Denial of Service attack is a kind of resource draining purposefully applied by exhausting the resource to degrade the output.

S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, A. Kannan,[12] “An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs” in this title that is energy efficient and uses cluster-based routing in which confidence scores on nodes are used to efficiently identify intruders. This routing algorithm minimizes DoS attacks more effectively by using intelligent agents to make optimal routing choices. It has been experimental from the studies performed with this confidence-based protected routing algorithm that this indicates that routing algorithm not only improves security, but also minimizes energy consumption and delay in routing.

Arathy K S, Sminesh C N,[14] “A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET” In this title, we propose a new method to detect single and collective black hole attacks with minimal routing and overhead computing. Black Hole Attacks in MANET By an additional route request with a missed target address, the future D-MBH algorithm recognizes single and multiple black hole nodes, determines a threshold ADSN, produces a black hole list and invokes the proposed D-CBH algorithm. The D-CBH algorithm generates a list of shared black hole nodes using the ADSN, black hole list and next hop information derived from RREP.

Gayathri Dhananjayan, and Janakiraman Subbiah[15] “T2AR: trust aware ad-hoc routing Protocol for MANET” This title indicates a trust-aware ad-hoc routing (T2AR) protocol to increase the degree of trust between the nodes in MANET. With the limitations of confidence rate, resources, mobility-based malicious activity prediction, the suggested approach modifies the standard AODV routing protocol. The matching packet sequence ID from adjacent node log reports specifies the confidence rate that prevents the generation of malicious reports. Moreover the overt and indirect consumption of trust observation schemes raises the level of trust. In addition, the use of the obtained signal intensity measure specifies that the trustworthy node is or is not within the contact range. The comparative study of the average end-to-end latency, throughput, false positives and packet distribution ratio between the suggest T2AR and current techniques such as TRUNCMAN, RBT, GR, FBR and DICOTIDS indicates the efficacy of T2AR in the stable MANET environment architecture, according to the author.

M. Poongodi, · S. Bose,[16] “A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET” In this title, the trust evaluation metrics are used to discuss a novel IDS. This is used for the identification in the networked architecture of flooding DDOS attacks. In the trust assessment-based setting, the proposed framework integrates the current Fire Cool-based protection procedures with the Dynamic Growing Self-Organizing Tree Algorithm.

IV. PROBLEM STATEMENT

Security is an important part for any communication, in recent scenario heterogeneous environment uses for communication, where mixed network (wired/wireless), hybrid topology and centralize as well as decentralize controller are utilize. Due to those factors involves the some unavoidable misbehavior in network which gain the network resource and disrupt the network. In the communication numerous threats are present which access the network resource so that in this dissertation our aim to secure the mobile ad hoc network from distributed denial of service and increase the network reliability.

V. PROPOSED DPEAP SCHEME

Distributed security system evaluate the neighbor profile and action taken based on its behavior, while security system found that any neighbor spread unknown packet in network then block permanently else only watch their activity every discrete events and take decision collaboratively. In this section describe formal description of proposed work, where routing protocol taken as dynamic protocol such as ad hoc on demand distance (AODV) which useful to find the shortest path form source to destination. Algorithm implement underneath the network simulator -2 which secure the mobile ad hoc network from distributed denial of service attack and improve the reliability for communication. The communication between the nodes play an important role since they are all working collaborative form or based baseline path, that provide one measure issue is security, so here we build the detection and protection denial of service attack algorithm under nodes communication, first we initialize all variables and check the behavior of the Distributed Denial of Service Attack, if any node sends an undefined type packets in large amount with high speed, that confirms the attacker presence. The historical research base identification and potential real-time defense would give the communication network power in the form of a security problem. The DPEAP identifies the attacker's actions by comparing the attacker's profile to the usual nodes on the network. If the node profile is normal in the foam of the right data distribution on the network, then the DPEAP announces that the network has no threat, so if the attack is detected, the DPEAP would be aware of the attacker node on the network and will therefore retain the attacker's profile and count the information.

Algorithm: Distributed profile evaluation to prevent network by DDOD attack

A. Set the Initial Network Parameter

Mobile Node Sensor = N;
Layer MAC = 802.11
Route = AODV
Attacker nodes = DDoS
Demand Protection = Distributed Profile Evaluation Approach to Prevent (DPEAP)
Inter time of arrival = IAT (Control Rate at Different Time)
/Attacker launches a negation-attack
Attacker-node (capture of insecure node information && send = = fake_packet && rate = 10^{10}*0.1s)
If (Receiver data == Susceptible) // DDoS confirmation
{
Infected
Call DDoS Attack Module
}
Phase to create a trace file for further evaluation
Phase review monitor for identification
If (packet_type == DDOS & Rate >= Normal) // higher data rate
{
Packet is category DDOS
Find the ratio of infection
}
Step:2 Call the DPEAP Protector
It's though (DPEAP-Check vulnerable node && total packet receives && rate && sender)
{
If (rate >= Usual && Packet =DDOS)
{

Submit a rate management response at various arrival time
if (control rate = true) // Usual data flooding
{
Unable to obstruct
}
{Block the attacker node}
}
}

VI. SIMULATION PARAMETERS

Table 1 shows the simulation parameter and on the basis of that all three scenarios are designed. The DDoS Attack and recovery through NTRS and propose DPEAP scheme having the same scenario of communication. The routing protocols, grid layout, number of nodes, Antenna and other are also mention to measures the performance of all three scenarios.

Table: 1 Network Input Parameters.

Parameters	Configuration Value
Routing Protocol	AODV
Simulation Area	800m*800m
Network Type	MANET
Number of Nodes	50
Physical Medium	Wireless, 802.11
Mobility Speed	Random
Mobility Model	Random Waypoint
Attack Type	DDoS
Secure Protocol	DPEAP
Simulation Time (Sec)	100Sec
Transmission Range	550m
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground

A. Comparative Analysis of Packet Delivery Ratio

The number of packets send and receive ratio is measures through Packet Delivery Ratio Analysis (PDR) or is the percentage ratio of packets received to send. The PDR in case of an attack is only evaluated up to 95 seconds but after applying DPEAP PDR is enhanced and it is better than the previous NTRS security scheme against DDoS attack. The protection scheme increases performance and provides an effective PDR in the network. In the event of an attack, the PDR is about 72% percent at the time about 95 seconds, but in the case of the DPEAP system, the PDR output is 98% up to the end of the simulation.

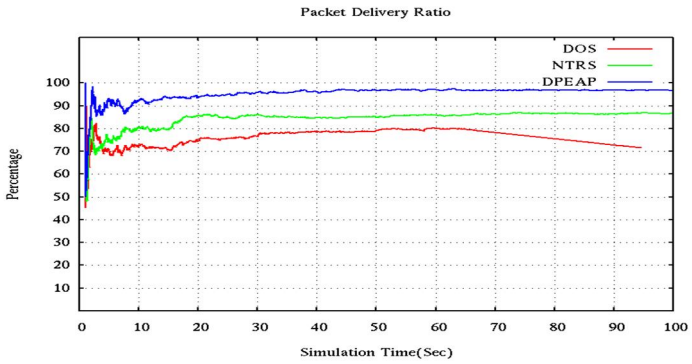


Fig. 1 Analysis of Packet Delivery Ratio.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue I Jan 2021- Available at www.ijraset.com

B. Comparative Analysis of Throughput [Kbps]

The performance of Kbits received at destination in unit time is measures through throughput performance. This graph reflects a throughput study in the case of, DDoS attack, previous NTRS scheme and DPEAP approach. The throughput tests the amount of data received per second at the destination. At the time of attack, the throughput decreases due to intense packet routing flooding in the network. It can also only be measured up to 95 seconds in the network. But after implementing the DPEAP scheme, the throughput is really high and reaches to 2700Kbps/second.

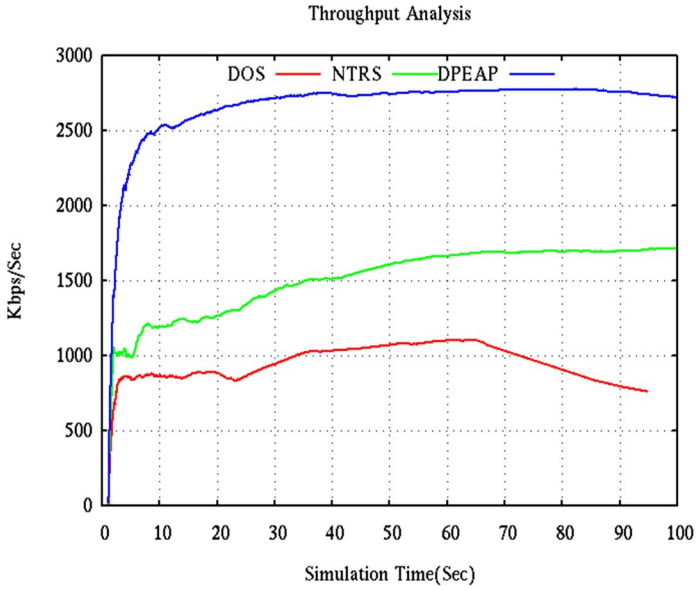


Fig.2: Analysis of Network Throughout [Kbps].

C. Comparative Analysis of Normal Routing Load

The DDOS intruder is constantly flooding the large amount of packets in the network (about more than $50*10^3$) that means consuming the bandwidth in the network so that nodes are not verified with each other about this kind of misbehavior. This graph reflects the routing load in the event of an attack being very heavy, which is the key cause for congestion in the network. After implementation of the DPEAP the routing load is under control and also less than the NTRS routing scheme.

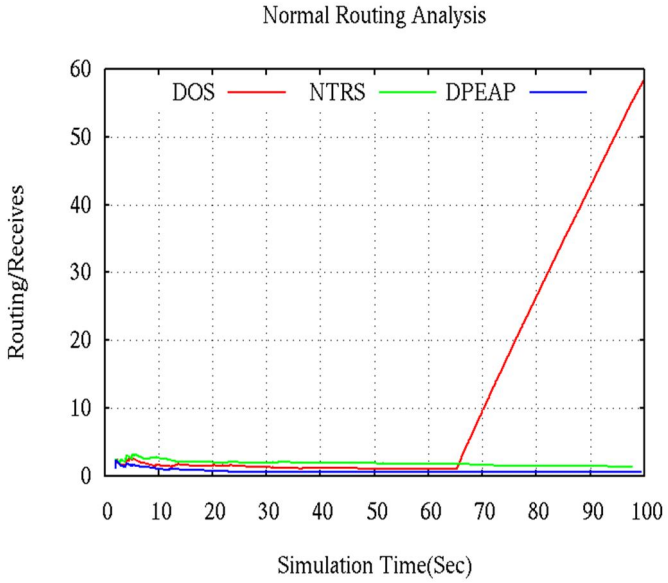


Fig.3: Analysis of Normal Routing Load.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue I Jan 2021- Available at www.ijraset.com

D. Analysis of Average End to End Delay [ms]

The UDP packet analysis is seen in this graph in the case of usual AODV routing, in the case of an attack and in the case of the IDS. Here we specifically visualized the failure of the packet in the event of an attack. In the event of an attack, marginal packets are transmitted in the network, but the efficiency of the network is the same as standard AODV routing after the IDS scheme has been implemented.

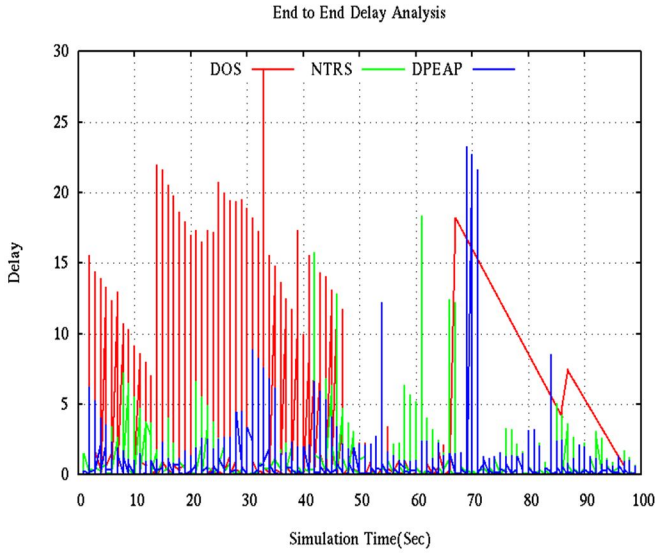


Fig. 4: Average End to End Delay [ms].

E. Percentage of Attack

This graph reflects the percentage study of the malicious actions in the event of an attack. Here we specifically visualized that 38 percent of the network is just infected by an DDOS attacker. Infection in the network is initiated from 1 second. But since implementing the DPEAP approach, the infection is negligible in the case of an attack, which implies that the protection scheme fully prevents the attacker's misbehavior operation.

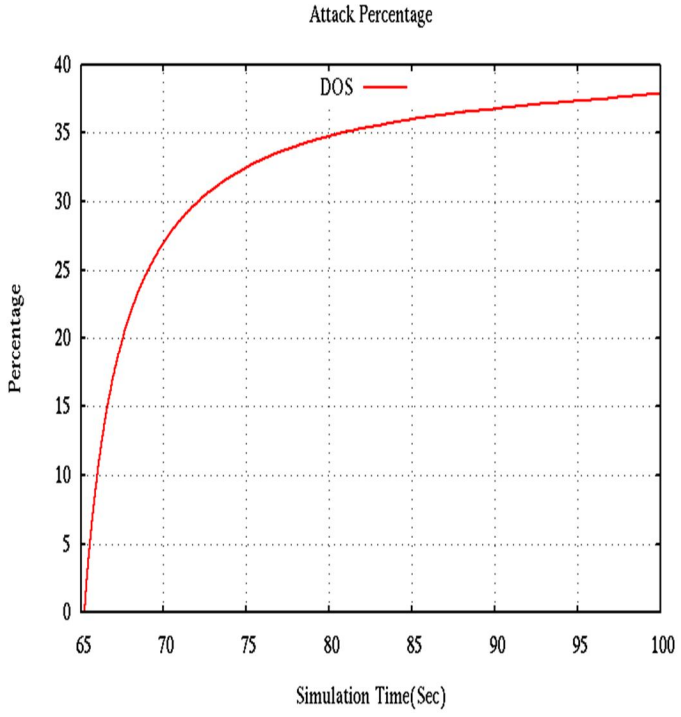


Figure 5: Percentage of Attack.

F. Summarize Performance Analysis

The cumulative output of the network as shown in Table 3. This table reflects all the summery efficiency metrics in the exact figure foam, which indicates how many packets are sent, received and lost on the network in case of NTRS routing, attack and DPEAP.

Table: 2 Summarize Analysis of Network.

Parameters	DOS Attack	NTRS	DPEAP
Packet Sends	4343	7010	10372
Packet Receives	3114	6065	10008
Packet Drop	1229	945	364
PDR (%)	71.70	86.52	96.49
NRL	63.94	1.36	0.54
Average Throughput[Kbps]	797.18	1552.64	2715.77
Average Delay[ms]	1.05	0.53	0.41

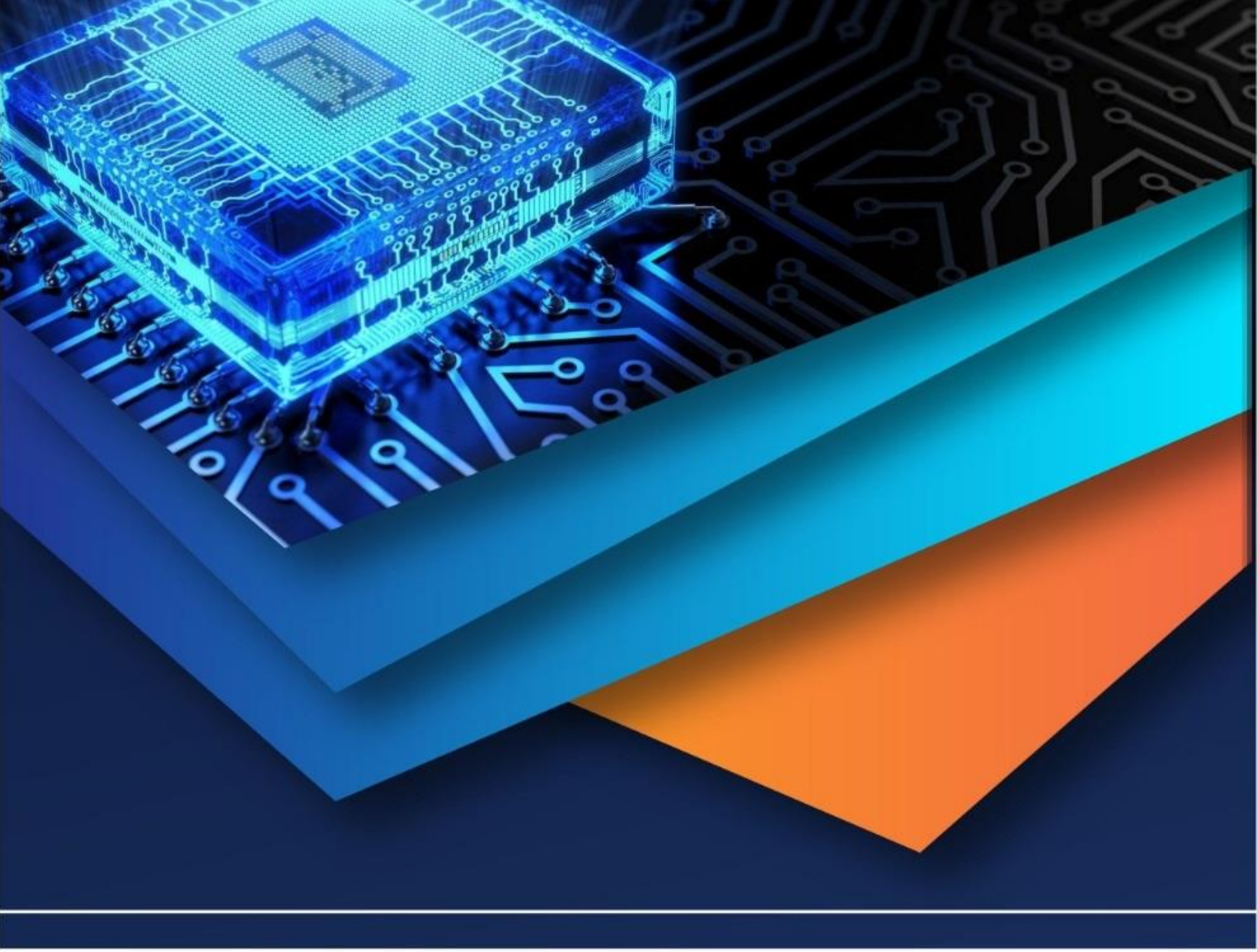
VII. CONCLUSION AND FUTURE SCOPE

In (Mobile Ad Hoc Network) MANET, nodes continuously share network knowledge. But the information is in the foam of a vast number of packets flooded into the network, in which case the network is affected by the DDoS attack. The proposed structure removes the need for a centralized authority which, due to its self-organizing existence, is not technically in the wireless sensor network. When route is establish and source want to transmit the data, meanwhile attacker are in active mode and generate huge amount of junk message during short period of time. While detection system found suspicious data as network relative issue than instantly call to network management protocol to take further action to resolve those problem. The attacker has compromised 38 percent of the network performance but is still impaired by the remaining network performance. The packet dropping is almost one-third of the previous scheme. The PDR is 10% more as compare to previous scheme and overhead is almost half as compare to the previous NTRS scheme. The proposed DPEAP scheme produces improved outcomes in the case of a DDoS intruder. Proposed security system use route protocol ad hoc on demand distance vector routing (AODV) which is dynamic routing suitable for ad hoc communication and established the route between source to destination with multi-hop link disjoint path. Other side if detection system found as unmatched protocol, it assume the behavior as attacker packet and record their identity for further decision. The performance of propose DPEAP scheme is measures with NTRS scheme and the performance of DPEAP is better.

In the future, measures the performance of grey hole attack and black hole attack. Other methods such as packet capture, false path forwarding, swapping source and destination addresses will still be used in the future for secure communication in MANET

REFERENCES

[1] M.M. Lehmus, Requirements of ad hoc network protocols, Technical report, Electrical Engineering, Helsinki University of Technology, May 2000.
[2] N. Asokan, P. Ginzboorg, Key Agreement in ad hoc Networks, Computer Communications 23 (17), pp.1627-163, 2000.
[3] G. C. Siva Ram Murthy, B. S. Manoj, " Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Low price Edition, Pearson Education, 2007.
[4] Dokurer, Semih."Simulation of Black hole attack in Wireless Ad-hoc Networks". Master's thesis, AtılımUniversity, September 2006.
[5] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.
[6] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communication, 14 (5), pp. 85-91, 2007.
[7] H.yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security In Mobile Ad Hoc networks: Challenges and Solutions. IEEE Wireless Communications, 11(1):38-47, Feb 2004.
[8] P. Yau and C. J. Mitchell, "Security Vulnerabilities in Ad-hoc Network", 2003.
[9] Adnan Nadeem, and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks, IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.
[10] Gurveen Vaseer, Garima Ghai, Dhruva Ghai, and Pushpinder S. Patheja "A neighbor trust-based mechanism to protect mobile networks" January/February 2019.
[11] Divya gautam prof. Vrinda tokekar "an approach to analyze the impact of DDOS attack on Mobile cloud computing" IEEE, International conference on information, communication, instrumentation and control (ICICIC), 2017.
[12] S. Muthurajkumar, S. Ganapathy, M. Vijayalakshmi, A. Kannan, "An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs" Springer Science Business Media New York 2017.
[13] Arathy K S, Sminesh C N, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET" Elsevier Procedia Technology 25, pp. 264 – 271 (RAEREST) 2016.
[14] Gayathri Dhananjayan, and Janakiraman Subbiah" T2AR: Trust Aware Ad-Hoc Routing Protocol for MANET" Springer Plus 2016.
[15] M. Poongodi, · S. Bose, "A Novel Intrusion Detection System Based on Trust Evaluation to Defend against DDoS Attack in MANET" Springer 24 sep 2015.
[16] Anuj Rana, Vinay Rana, Sandeep gupta "EMAODV: Technique to Prevent Collaborative Attacks in MANETs" Elsevier procedia computer science 70, 137 – 145, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY