iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** I **Month of publication:** January 2019

DOI: http://doi.org/10.22214/ijraset.2019.1088

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: 6.887
Volume 7 Issue I, Jan 2019- Available at www.ijraset.com

Secure Routing Architecture for Mobile Ad Hoc Network

Ankita Dandge[1], Dr. Vilas Thakre[2]
[1, 2]*SGBAU, Amravati Maharashtra, India.*

Abstract: ***Mobile Ad-hoc networks (MANET) is self-configuring, multi hop wireless network. Security in mobile ADHOC network is huge challenge as a result of situation like there's no centralized authority which might supervise the individual nodes operational within the network. Additionally, the look of most Manet routing protocols assumes that there's no malicious node within the network. Hence, many efforts and researches are created toward the look of a secure and sturdy routing protocol for circumstantial networks. In this paper, the system is proposed for attacks that may target the operation of circumstantial routing protocol. An in depth survey of the well-known secured circumstantial routing protocols for mobile circumstantial networks is carried out. So as to investigate the existent solutions for securing circumstantial routing protocols in an exceedingly structured manner to hide the wide selection of intrusion detection Techniques in MANETs. In this paper proposes the technique for detection of attack on dealings of file, packet and paper tends to discover harm node and harm file.***
Keywords: Ad-hoc Network, Routing, Security, Attacks, MANET, MD5 algorithm.

I. INTRODUCTION

A mobile ad-hoc network (MANET) include a collection of mobile hosts that perform basic networking functions like packet forwarding, routing etc. while not the assistance of a longtime infrastructure. Nodes of associate degree ad-hoc network place confidence in one to a different in forwarding a packet to its destination, thanks to the restricted vary of every mobile host's wireless transmissions. Security in Edouard Manet is an important part for basic network functions like packet Forwarding and routing [1]. So as to supply property in an exceedingly mobile unintentional network all nodes need to perform routing of network traffic. though varied unintentional routing protocols are projected like Destination-Sequenced Distance-Vector (DSDV), Optimized Link State Routing Protocol (OLSR), Dynamic supply Routing (DSR) and unintentional On Demand Distance Vector (AODV), that assumed associate degree surroundings wherever all the nodes ar utterly cooperative and trustworthy and no security mechanism has been thought-about [2]. Intrusion detection (ID) in MANETs is additional advanced and difficult than in fastened networks, due to the issue in fulfilling the wants of IDS [3] (namely the power to gather audit information from the network, and apply ID techniques to notice intrusion with an occasional rate of false positives and an efficient response to intrusion) and since some characteristics of MANETs produce operational and implementation complexities. Further challenges for IDSs in MANETs ar as follows:

A. MANETs lack concentration points wherever watching and audit information assortment are often performed
B. MANET routing protocols need nodes to collaborate and act as routers, making opportunities for attacks
C. Due to the nodes' quality, the topology is dynamic and unpredictable, creating the method of intrusion detection difficult
D. IDSs in MANETs are additional advanced due to the restricted machine ability of most of the nodes [4]

To cover the big selection of intrusion detection Techniques in MANETs, during this paper tendency to propose the technique for detection of attack on dealing of file, packet [5]. Papers have a tendency to notice harm node and harm file.

II. BACKGROUND

In MANET there are different types of routing protocols for routing the packets. Each routing has own rule to packet transfer method. In mobile ad-hoc network in different circumstances different protocol [1]. There exist several proposals that attempt to counter the security threats mentioned in the previous section, and provide protection against malicious attacks and selfish behaviors. These proposed solutions are either an integration of security mechanisms into existing protocols (e.g. AODV and OLSR) [2]. The goals of any secure routing protocol square measure to produce some or all of the properties like Authentication, Access management, Confidentiality, Privacy, Integrity, Authorization, Anonymity, No repudiation, Freshness, accessibility, Resilience to attacks. Of these, accessibility especially targets denial of service (DoS) attacks and has the flexibility to sustain the

networking functionalities with none interruption thanks to security threats [3]. To guard MANETs against region attacks many mechanisms are planned exploitation completely different ways. In Tseng et al. surveyed existing solutions for police investigation region attacks and classified these proposals as distinguishing either single (i.e. one assaulter launches the attack within the network) or cooperative region attacks (i.e. 2 or additional nodes collaborate to launch the attack)[4]. TOGBAD is AN example of a region detection mechanism. Variety of routing protocols are planned towards providing security in impromptu networks. a number of the foremost wide mentioned protocols square measure echt Routing for impromptu Networking (ARAN), Ariadne and Watchdog Path rater. There have additionally been varied secure routing techniques that use multipath primarily based routing wherever they break the info into completely different range of sub packets, cypher them so finally route them through completely different ways [5].
This paper is organized as follows. Section I contains Introduction of this paper. In Section II mentioned Background. Section III introduced previous work done. Section IV explains existing methodologies. In Section V mentioned existing framework and analyzed it. Section VI presents the planned work. Its outcome potential results square measure analyzed in Section VII. Section VIII concludes this paper. Finally Section IX presents future scope.

III. PREVIOUS WORK DONE

Ratul Dey, Himadri Nath Saha (2016), [1] classifies the secure routing protocol in Edouard Manet, and additionally discussing presently projected technique of mitigating those attack. within the routing protocol of the Edouard Manet whereas forwarding knowledge packets to different nodes, some intermediate node extract helpful info packets and can't forward the packet to following node. Some node might modify the content of packets throughout the information transmission session.
Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi (2016), [2] discuss the foremost attacks which will target the operation of circumstantial routing protocol. a close survey of the well-known secured circumstantial routing protocols for mobile circumstantial networks is bestowed. so as to research the existent solutions for securing circumstantial routing protocols in a very structured manner, classified them into 3 categories: solutions supported cryptography, solutions supported unidirectional hash chain and hybrid solutions. during this analysis additionally offers a short outline and comparison of varied protocols accessible for secured routing in Edouard Manet. Mohanapriya Marimuthu and Ilango Krishnamurthi (2013),[3] analyze the vulnerabilities of a pro-active routing protocol known as optimized link state routing (OLSR) against a selected style of denial-of-service (DOS) attack known as node isolation attack. Analyzing the attack, propose a mechanism known as increased OLSR (EOLSR) protocol that may be a trust based mostly technique to secure the OLSR nodes against the attack. This method is capable of finding whether or not a node is advertising correct topology info or not by corroborative it's how-do-you-do packets, so detection node isolation attacks.
Adnan Nadeem, Michael P. Howarth (2013), [4] reporting a survey of the most varieties of attack at the network layer, then review intrusion detection and protection mechanisms that are projected within the literature. And classify these mechanisms as either purpose detection algorithms that alter one form of attack, or as intrusion detection systems (IDSs) which will alter a variety of attacks. A comparison of the projected protection mechanisms is additionally enclosed. Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, Pushkar Gupta, and Pravina Dhurandher (2011), [5] propose this theme that has been drawn from a network of friends in real world eventualities. The algorithmic rule works by causing challenges and sharing friend Lists to supply a listing of trusty nodes to the supply node through that knowledge transmission finally takes place. The nodes within the friend list area unit rated on the premise of the quantity of information transmission they accomplish and their friendly relationship with different nodes within the network.

IV. EXISTING METHODOLOGIES

A. FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems

FACES algorithmic program is establish to secure routing in mobile networks. FACES that stands for Friend based mostly routing mistreatment Challenges to determine Security [5]. The FACES algorithmic program is split into four stages, viz. Challenge Your Neighbor, Rate Friends, Share Friends and Route through Friends. The primary 3 stages of the formula area unit periodic, whereas the fourth is on demand. The algorithmic program provides authentication of nodes by causing associate initial challenge. Nodes that have completed the challenge realize place within the friend list. Friend based mostly routing exploitation Challenges to determine Security (FACES) accomplishes institution of friend networks in MANETs within the same manner as in world situations. Apply a similar plan to develop the FACES formula. The projected FACES formula is split into the next four Stages as shown in Figure one shows the challenge neighbors, Rate Friends, Share Friends and Route through friends. The figure additionally depicts the link/flow between the various stages of the algorithmic program. The routing of knowledge within the protocol is on demand; that's whenever the necessity arises. However challenges, friend sharing and rating area unit periodic processes. This makes the FACES protocol a hybrid one.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue I, Jan 2019- Available at www.ijraset.com

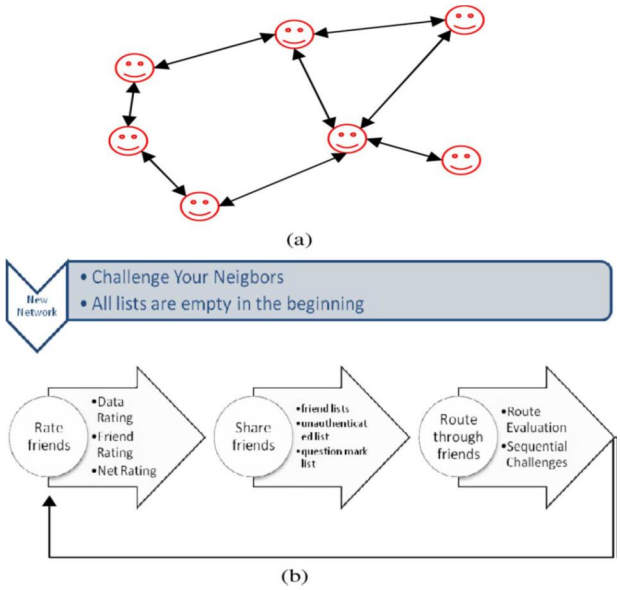


Fig 1: (a) Network of friends in a community. (b) FACES: Link/Flow between different stages.

B. Detection And Isolation Based Secure Routing Scheme

Develop a protocol for detection flooding, black hole, gray hole, wormhole and blackmail attacks. On detection the protocol takes immediate actions to blacklist these nodes from the network, thereby decreasing the quantity of malicious nodes during a network, therefore up the opposite QoS parameters [1]. This protocol detects and isolates misbehaving nodes in edouard Manet. It's AN improvement of DSR routing and supported choice of selfish and unselfish nodes. The advantage is that the trust and routing calculation method is evaluated by expertise, observation and behavior of different nodes, present within the network. This protocol will effectively discover self-serving nodes and isolate wormhole nodes that drop packets.

C. Secure Routing Protocol (SRP)

The Secure Routing Protocol (SRP) developed by Papadimitratos and Haas [2], the protocol designed to secure the on-demand routing protocols that utilize broadcasting as its route querying methodology. The authors mentioned which will be applied as AN extension of a large number of existing reactive routing protocols, particularly the DSR. A security association (SA) is needed between a supply node and a destination node. It's assumed that the SA are often established by employing a shared key between the 2 communication nodes. A SRP Header as shown in Fig. two is additional to the packet of the idea routing protocol. The supply node initiates the route discovery, by causing a route request packet that known by a question sequence variety (QSEQ), a random question symbol (QID), and also the output of a key hashed operate. The key hash operates takes information processing header, the header of the fundamental routing protocol, and also the shared key.

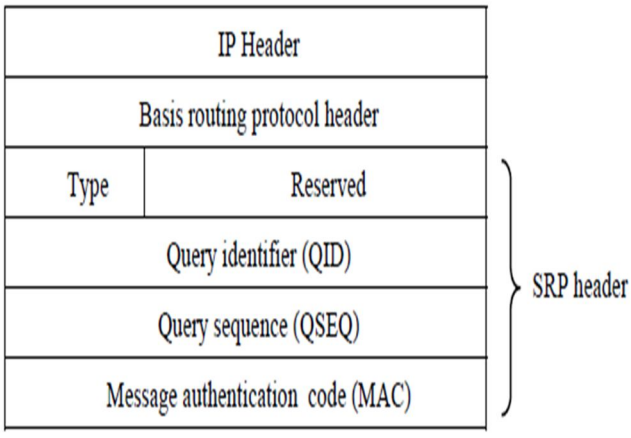


Fig 2. SRP Packet header

D. Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks

EOLSR is an improvement of the fundamental OLSR routing protocol [3], ready to} be able to discover the presence of malicious nodes within the network. This can be to eliminate any malicious node from giving the false info regarding any traditional node that desires to become MPR. Our resolution assumes that everyone the nodes square measure attested and may participate in communication i.e., all nodes square measure approved nodes.

In our approach, we tend to assume the authentication mechanism [3] is applied so as to spot the precise origin of every packet that prevents malicious node from causing cast reply packets exploitation spoofed address. Operating relies on confirming the correctness of the received how-do-you-do message from a neighbor node before designating it as MPR for this node. Protocol work on trust based mostly analysis to discover the malicious node is impressed from. In OLSR routing protocol, each node build its routing table and learn the constellation supported the how-do-you-do and TC messages it receives from its neighbors.

E. Anomaly-Based Intrusion Detection

Anomaly-based intrusion detection (ABID) systems flag as abnormal discovered activities that deviate considerably from the traditional profile [4]. ABID systems are called behavior-based intrusion detection, during which the model of traditional behavior of the network is extracted, so this model is compared with the present behavior of the network to discover intrusion within the network. A diagram illustrating the fundamental ABID method is shown in Figure four. Anomaly detection systems usually accommodate 2 phases of operation: coaching and testing. Coaching is that the method of modeling the traditional or expected behavior of the network or of the users. The model conjointly acts as a profile of user or network behavior. For any anomaly based mostly IDS to be effective, it should thus have a uniform and stable profile that characterizes this behavior.

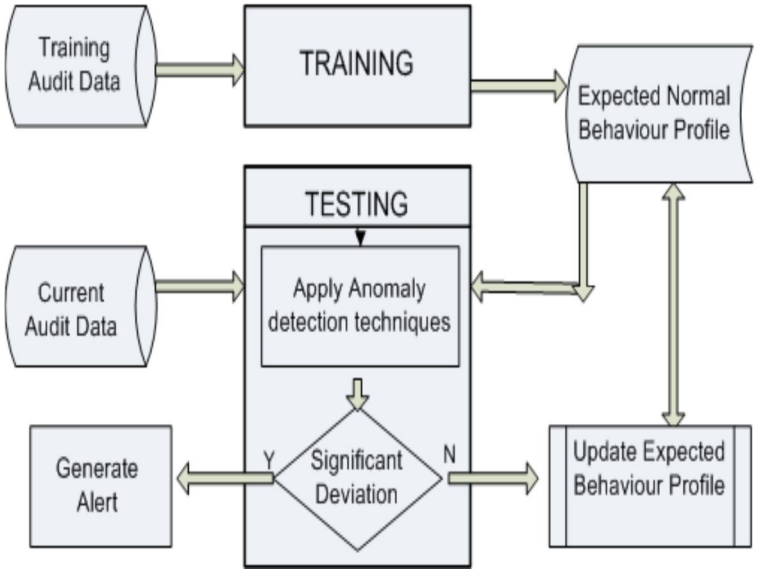


Fig 3: Anomaly-based intrusion detection process

V. ANALYSIS AND DISCUSSION

For the secure routing protocol 1st would like correct authentication ought to digital signature of every and each documented node [1]. It conjointly ought to mutable data of the management packets. It conjointly usually complemented with the employment of unidirectional hash functions. Establish whole and therefore the tunnel. These routing schemes offer authentication services that guard against modification and replaying of routing management messages and uses totally different cryptographical primitives for providing secure routing. This protocol takes advantage of the shortest path between the supply and therefore the destination. A modification of Dijkstra's algorithmic program is applied for this purpose. All nodes have positive weight.

Multipath and Message Trust primarily based Secure Routing (MTMR) [5] uses a trust assignment and change strategy which might be accustomed establish and isolate malicious nodes while not being exhausting on the resources of the network. It uses a parameter, the trust demand of the message such every message contains a sure level of importance supported its content and kind. This can be the trust demand of a selected message that decides however the message is routed. Therefore, solely methods with sure trust level are often used for its forwarding. This additional enhances the protection of the system.

Parameter for Comparison	Disjoint Multipath Routing	Trust based Multipath Routing	Message Trust based Multipath Routing
Routing	Multipath	Multipath	Depends on the trust of the message.
Message	Message broken into 4 parts	Message broken into 4 parts	Depends on the trust of the message (not always broken).
Checking employed	No check	No check	Cyclic Redundancy Check used
Encryption/Decryption	XOR	XOR	Cipher block chaining
Reliability	Non trust based	Trust based	Trust based
Route selection	Route selection is difficult, as disjoint paths may not be always found. Larger number of paths needed for routing	Takes more time in route selection as it is trust based. Lesser number of paths may be needed for routing	Easier in route selection as mostly lesser paths may be needed for routing, since the number of paths to be selected is based on the trust of the message.
Trust based updating	Not available.	Not available.	Available.
Mode	Non-promiscuous mode	Promiscuous mode	Promiscuous mode

Fig 4 : Comparison of Multipath Routing Protocols

VI. PROPOSED METHODOLOGY

A. Secure Routing Architecture

We propose architecture for security routing of mobile network. There are some key points of propose system. Fig:5 shows the architecture of proposed system.

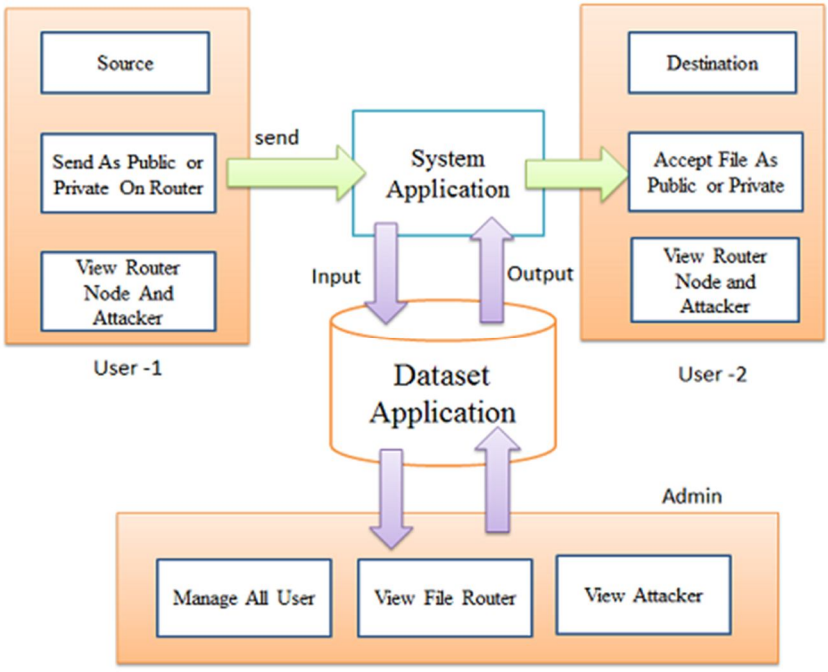


Fig 5: Secure Routing Architecture

1) Comparison of security dimension coverage point of all sender and receiver.
2) Number of communication events required to secure communications between all nodes.
3) Number of bytes required to secure communications between all nodes.
4) Overhead of securing communication required for route generation
5) Overhead of securing communication required by using MD5 algorithm (Message digest algorithm)

For data security we used MD5 Algorithm as describe as followes:

B. MD5 Algorithm (Message-digest algorithm)

Steps

1) The file authentication will be check by MD5 algorithm
2) Input file
a) convert file in 512 blocks
b) compress all data in 128 bit
c) Divides the data in 4 blocks of 32bit
d) apply binary shifting to each block
e) Convert each block in hex value
f) combine all blocks and create a hash value of 128 bit
3) MD5 generate a hash value for each document. The hash value is generated two times. First time when user send a file. Second time when another user received the file. Both hash value must be same, if they are different that means the file has been modified.

VII. OUTCOME AND POSSIBLE RESULT

The proposed an architecture for security routing of mobile network. In this architecture we can detect the damage packet and node on which it damages packets. We can also detect the number of packet loss in between transaction. Find out the attacker path in transaction. And successfully transfer the file from source node to destination node. Dataset application is used for manage the all users, view file router, and view attackers.

VIII. CONCLUSION

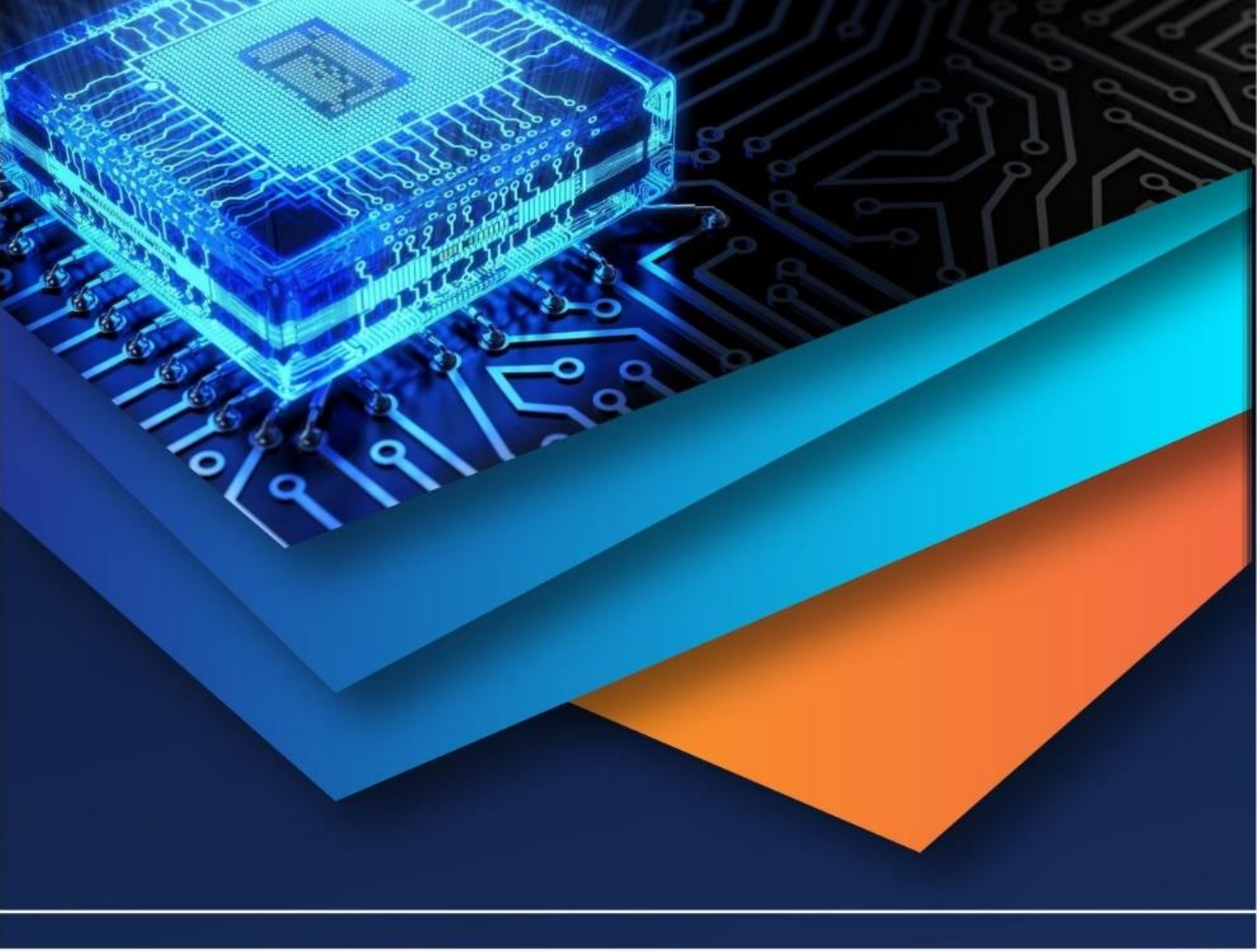
During this paper, discuss the attacks that may target the operation of circumstantial routing protocol. An in depth survey of the well-known secured circumstantial routing protocols for mobile circumstantial networks is bestowed. so as to investigate the existent solutions for securing circumstantial routing protocols in an exceedingly structured manner to hide the wide selection of intrusion detection Techniques in MANETs, during this paper propose the technique for detection of attack on dealings of file, packet. Paper tend to discover harm node and harm file.

IX. FUTURE SCOPE

In this paper proposed the system for detecting the attacker node, on which path attack is placed on which node and calculate the packets lost. In future proposed system for prevention the attacks there should be the developing the algorithm. Means prevent the transaction of file transformation from same attack in future.

REFERENCES

[1] Ratul Dey, Himadri Nath Saha, “Secure Routing Protocols for Mobile Ad-Hoc Network (MANETs) –A Review” INTERNATIONAL JOURNAL OF EMERGING TRENDS & TECHNOLOGY IN COMPUTER SCIENCE (IJETTCS), Volume 5, Issue 1, January - February 2016.
[2] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, “Secure Routing Protocols for Mobile Ad Hoc Networks” IEEE, 2016
[3] Mohanapriya Marimuthu and Ilango Krishnamurthi,” Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks”, JOURNAL OF COMMUNICATIONS AND NETWORKS, Vol. 15, No. 1, February 2013.
[4] 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.
[5] Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, Pushkar Gupta, and Pravina Dhurandher,” FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems”, IEEE SYSTEMS JOURNAL, Vol. 5, No. 2, June 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY