iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41389

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: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

A Secure Approach to Autonomous Mobile Ad-Hoc Networks Using Superman Technique

A. Anne Linda
Department of Computer Science and Engineering, University College of Engineering, Nagercoil, India

Abstract: ***Mobile Ad-hoc Networks or MANETs are mostly found where any fixed facilities are not available and so it is dynamic. Secure transmission of data is an important aspect in MANET. They have unique characteristics like dynamic topology, wireless radio medium and lack of centralized administration. As a result they are vulnerable to different types of attacks in different layers of protocol. To protect these networks, various security protocols have been developed. To address these issues, a framework called Security Using Pre-Existing Routing for Mobile Ad-hoc Networks (SUPERMAN) [1] is proposed. This paper presents a security framework SUPERMAN which enables data confidentiality and prevention of data loss by using AES encryption. And a report is generated at the destination side to view user details, path details and attack node details.***

Keywords: mobile ad hoc networks, node authentication, data confidentiality.

I. INTRODUCTION

MANET has become one of the emerging part in our day-to-day life and they become a threat if security is not considered carefully before deployment. MANET communication is one of the wireless communication. Now-a-days evolution of wireless network plays a major role in the society. Mobile Ad-hoc networks has now become one of the most active field of communications and networks. It is one of the challenging areas of wireless networking.

MANET is a collection of mobile nodes with no pre-determined infrastructure. Each mobile node is accompanied with a wireless transmitter and a receiver with an antenna. They use radio broadcast medium for communication. Nodes in MANET have the capacity to move freely in the network and it is self organising. Each node in a MANET acts as a router that discover and maintain routes. The control of the network is distributed among the nodes participating in the network. The delivering of data packet is executed by the node themselves.

Any attack in routing phase may disrupt the entire communication. So routing has to done be in more secure manner. MANET is very useful to real world application where the topology changes rapidly.

Links in MANET has less bandwidth than the wired network. The inherent characteristics of MANET leads to some major issues like power constraints, routing protocols and radio inference. The main characteristics of MANET are limitations of infrastructure, self organization and dynamic changes of nodes.

The dynamic, self-configuring and infrastructure-less group of mobile devices are known as MANET. Number of devices in MANET are known as node. Each node act both as a client and a router. By the way of forwarding packets to a destination node communication has made across the network.

Routes are discovered dynamically by the mobile hosts. It is more susceptible to security attacks as communication takes place in open method. Nodes may join or leave the network dynamically. Due to dynamic nature of MANETs are highly vulnerable to various security attacks like Wormhole ,Blackhole, Grayhole, Sybil and Deniel of Service (Dos) attacks. Attacks can be reduced by implementing various security protocols.

MANETS are different from wireless IP networks because there is no base stations and wireless switches. Research in the area of Ad-hoc networking is receiving more attention from industry and government. Even though there are lot of security issues in MANET it is more wanted because of their usage. So security is an important in MANET. To overcome these security threats and attacks a framework has been developed named, Security Using Pre Existing Routing in Mobile Ad-hoc Networks(SUPERMAN) [1]. This protocol has been designed to address node authentication, network access control and secure communication. The existing system, provides only routing or communication security. In contrast SUPERMAN combine both routing and communication security at the network layer.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

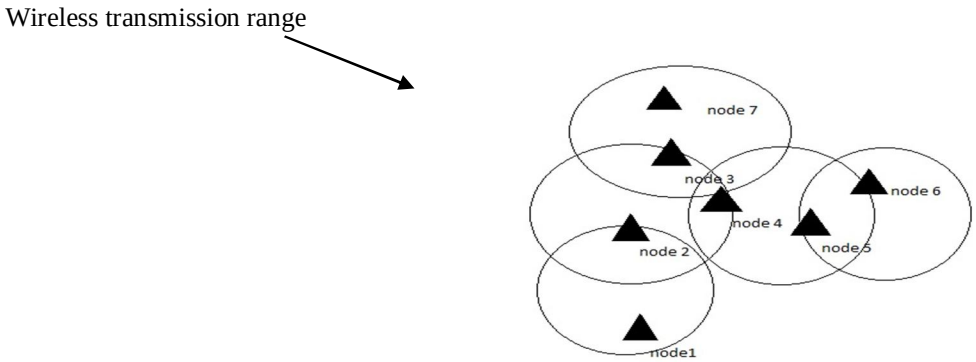


Figure 1: MANET Network

Fig.1 indicates the MANET architecture which is generally autonomous and frequent change of topology. The range is specified in the figure which symbolize the wireless transmission range between other dynamic nodes in the Ad Hoc networks. The transmission range depends on the intermediate nodes that the data packets are passed on to reach the destination node.

The remainder of this paper is organized as follows: Section 2 analyses the problem in the context of previously published work. Section 3 analyses the algorithms and design objective. Section 4 introduces the SUPERMAN framework. Section 5 gives the performance analysis between existing and proposed system. Section 6 draws conclusion from the research findings.

II. RELATED WORK

Recently several protocols have been proposed to improve security in MANET. Many security mechanisms are established in order to improve the secure transmission of packets in Ad-hoc networks. The emerging field of nomadic computing requires various security schemes to enhance the security services such as confidentiality, authentication, authorization and data integrity.

Rutvij H. Jhaveri et al [2] proposed a protocol to address some basic security concerns in MANET and it includes the operation of wormhole attack. It also provides the way of Securing the Ad-hoc On Demand Distance Vector routing protocol (AODV). It includes modification of sequence numbers and hop counts, source routing tunnelling, spoofing and fabrication of error messages.

Priyanka Goyal et al [3] proposes a scheme to describe the fundamental problems of ad hoc networks including the concept, features, vulnerabilities in MANET, and the study of routing protocols**.** It is based on some popular algorithms like Distance Vector Routing Protocol(DVR), Open Shortest Path First(OSPF), Ad-hoc On demand Distance Vector Routing Protocol(AODV), Zone Routing Protocol(ZRP). In this scheme it includes some more improvement in bandwidth and high capacity is required. There is also a need for higher frequency and better spatial spectral reuse.

Zaiba Ishrat et al [4] developed a scheme and that paper makes a discuss about the security issues, vulnerable nature of the mobile ad-hoc network, security criteria and the main attack types. It uses Intrusion Detection Technique to prevent the intrusion of malicious nodes, uses both message authentication primitives and digital signatures. In this fake messages can be injected into the network and to prevent this more number of security schemes must be known.

Kirti Gupta et al [6] presents the main vulnerabilities in the mobile ad-hoc networks and their security solutions. In this paper various attacks like modification attack , jellyfish attack , flooding attack and their issues were discussed. Existing proposals are based on one specific attack.. Here unanticipated or combined attacks remain undiscovered. So combined form of many attacks should be identified and their issues should be rectified in the overall networking system in MANET.

Gurjeet Singh Dhillon et al [7] clearly describes the vulnerabilities , challenges and applications in
MANET. The major attacks like man in the middle Attack , routing attack and Deniel of service attack
Were clearly examined and their preventive measuresare taken. Improvement in bandwidth and capacity is required for the nodes that are in the network. Large scale of Ad-hoc networks is a challenging issue. Certain preventive measures were taken to detect and rectify the possible attacks wereclearly specified.

Edwin Lawrence et al [8] establishes what routing information is exchanged, when and how routes are computed, their network structure, communication model, routing strategy. This paper describes the routing protocols such as proactive routing protocol, reactive routing protocol and hybrid protocol. It indicates that is difficult to choose the right routing protocol for routing process which should be in secure manner. So various security routing mechanisms are clearly discussed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

III. PROBLEM ANALYSIS

MANET's dynamically establishing mobile nodes in the networks. It has no fixed infrastructure. Due to the movement of mobile nodes in MANET the network topologies keep on changing. Mobile nodes communicate with each other through wireless links. The links in MANET have less bandwidth than the wired network. Due to the above characteristics it comes under some security threat and various attacks.

A. Security Threat

A threat refers to anything that has the potential to cause serious damage to the MANET. A threat is something that may or may not happen but has the potential to cause serious harm. A threat can be either intentional or accidental or the possibility of a natural disaster. The following security dimensions are identified:

Non-repudiation prevents the nodes from broadcasting of false information regarding of the previous transmission.

Integrity allows nodes to make ensure that the packets are received at the destination in the same form they were sent.

Confidentiality prevention of unauthorized nodes from capturing of packet payloads.

Authentication confirms the identity that the communicating nodes are legitimate nodes.

Privacy prevention of outside nodes into the network from deriving valuable information.

B. Attacks In Manet

Manet is a group of autonomous nodes which enables communication in wireless medium. As it is wireless medium it is open to a large number of attacks. The following security attacks are identified:

BlackHole Attack a malicious node that falsely replies for route request but it does not have an active route to the destination node and also advertise itself as having shortest route to destination and starts sending data through black hole node and becomes active element in the route.

GrayHole Attack The behaviour of a malicious node is unpredictable. It may drop certain packets while forwarding all other packets. It behave malicious for sometime and later changes like ordinary node.

Sybil Attack also known as spoofing attack which creates multiple fake identities called Sybil nodes. It behave as normal nodes.

Deniel of service In this attack malicious node prevents other authorized node to access network data or service and resources like bandwidth will be wasted. It completely disrupts the network.

WormHole Attack In this attack packets in one location are recorded and tunnelled to another location in the network by the attacker. Other than these attacks, there are many possible attacks in MANET that is major threat to the networking system. Those attacks may either be internal or external. Internal attacks caused from nodes that are part of the network where external attack is carried by the nodes that do not belong to the domain of the network.

IV. DESIGN OBJECTIVE

Mobile Ad-hoc is one of the increasing popular in a wide range of use cases. Due to is dynamic nature it is open to a large number of security issues. To resolve these issues this paper proposes a security protocol called, Security Using Pre-Existing Routing for Mobile Ad hoc Networks (SUPERMAN). SUPERMAN is a framework that operates at the network layer (layer 3) of the OSI model. Key Management and cryptography has to be applied in very secure manner. As mentioned before, due to lack of infrastructure, it is vulnerable to various attacks and threats. To overcome the problems of MANET, Ad hoc On-demand Distance Vector(AODV) and Optimised Link State Routing(OLSR) protocols are proposed. AODV find the shortest path from the source node and destination node. OLSR takes a proactive approach, periodically flooding the network to generate and maintain the routing table entries which persist until the next update. These basic versions of AODV and OLSR allows malicious nodes to interfere with the network in several ways. So secure approach of AODV, SAODV(Secure Ad hoc OnDemand Distance Vector) and secure approach OLSR, SOLSR(Secure Optimised Link State Routing) is used. SAODV secures the routing mechanism which provides random numbers in Route Request packets. SAODV requires that at least two secure Route Request Packets arrive at the destination node by different routes. SOLSR allows detection of wormhole attacks. The objective of SOLSR and SAODV is to protect the network from blackhole ,wormhole ,grayhole and Sybil attacks. The secure routing is also established. These protocols do not protect data sent over the secured routes. The main design objective of the proposed system is to maintain secure route and secure communication throughout the networking nodes in MANET(Mobile AdHoc Networks).The nodes are dynamic and has limited energy constraint.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

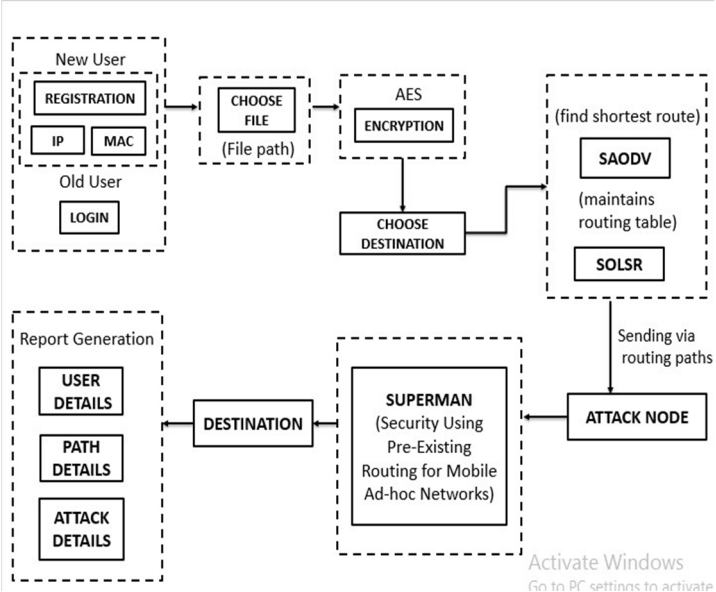


Figure 2: Architecture of proposed system

The above figure represents the architecture of the proposed framework. The simulation model represents the source sends data packet to the selected destination node via intermediate nodes. The transmitting nodes are selected or chosen by the aforementioned routing algorithms SAODV and SOLSR. If attack has to be happened, then the secure framework activates the SUPERMAN node and the data is securely transmitted to the destination node without any attack and packet loss as represented in the proposed system architecture. Fig.2 shows the overall design of the proposed framework where the data protection is done by encrypting the data by using AES (Advanced Encryption Standard) encryption scheme. SUPERMAN framework provides dynamic generation of keys to provide secure communication. The Diffie-Hellman key exchange algorithm provides generating of symmetric keys dynamically and to generate the SK keys.

V. PROPOSED SYSTEM

MANET is a rapidly growing technology which is self-organized,self configuring and has dynamic wireless links. Several traditional schemes proposes Security Routing Protocol along with Public Key Infrastructure(PKI) and Firewall but nodes can have different privileges based on their trust level [10].

To improve the security level in ad hoc networks, SUPERMAN framework combines routing and communication security at the network layer which provide routing and communication security along with data encryption using AES encryption scheme to protect the network. SUPERMAN also provides node authentication. The proposed system has several advantages like improve privacy of the network, increase data integrity, checks authenticity and integrity at each hop ,data encryption and report generation. It is designed to provide a fully secured communication framework for MANETs. Every legitimate node in the network is provided with a certificate by the associated Trusted Authority (TA). Each node is provided with a certificate from a TA(Trusted Authority), to join SUPERMAN networks[1].

The joining node (A) joins a network by periodically broadcasting Discovery Request (DReq) packets containing its DKSp (Diffie Hellman KeyShare).

This continues until it receives a Certificate Request (CReq) from other node (B) in the network. This can be demonstrated by the following scenario. If A needs to communicate with B and A is adjacent to B. A lacks B s DKSp(DiffieHellmanKeysharepublic).A DKSpReq (Diffie Hellman KeyShare Request) is sent to B by A. B responds with a DSKpRep (Diffie HellmanKeyShareRequest) containing its DKSp. A adds B's DKSp to its security table. If A wants to communicate with C and it requires an intermediate node B for further communication. A and B does not know C, but know each other. A sends a DSKpReq to C via B but C is not known to B. B forwards the DSKpReq to C. C replies to B with a DSKpRep.B adds C s DKSp to its security table the forwards it to the node A. A receives B s forwarded DSKpRep, then adds C s security details to its security table.

The experimental scenario is described as follows,

Consider, If A needs to communicate with C it requires a route through D and B to reach the node C.A knows D but do not know the nodes B or C.If nodes D or B hold the DKSp for C, they may respond on C s behalf and pass C s details to A.[1]The optional communication other than this will not occur for the mentioned nodes. SUPERMAN framework stores keys in each node's security table. The security table contains the security credentials of each node.The security table has n entries, where n is the number of nodes. The security table for the communicated nodes are updated for each node that has participated in the network.The shared symmetric broadcast key (SKb) has two derived forms, the SKbe and SKbp. SKe and SKp for end-to-end and point to point secure communication. These keys are stored in the security table which possess a separate broadcast address, denoted by I(*).These keys represents every security credentials held by the whole network. A node's ID would be the address of that node. SKe keys are used to secure end-to-end communication with other nodes that are participated in the network. SKp keys are used for point-to-point security[1].Various security threats , issues ,routing attacks in MANET and their preventive measures are considered by proactive and reactive protocols[11].

The SUPERMAN framework with data encryption and report generation is represented diagrammatically as flow diagram in fig 3. Which represents the SUPERMAN framework which has SUPERMAN node that is activated if any attack is happened in the MANET. In the flow diagram the source chooses the data that is to be sent to the destination through possible intermediate nodes. The data packet is encrypted and is further transmitted between the shortest chosen intermediate nodes to reach the destination faster and also secure .If any attack is identified or found in the intermediate nodes the SUPERMAN node activates and securely transmits the data packet to the destination.

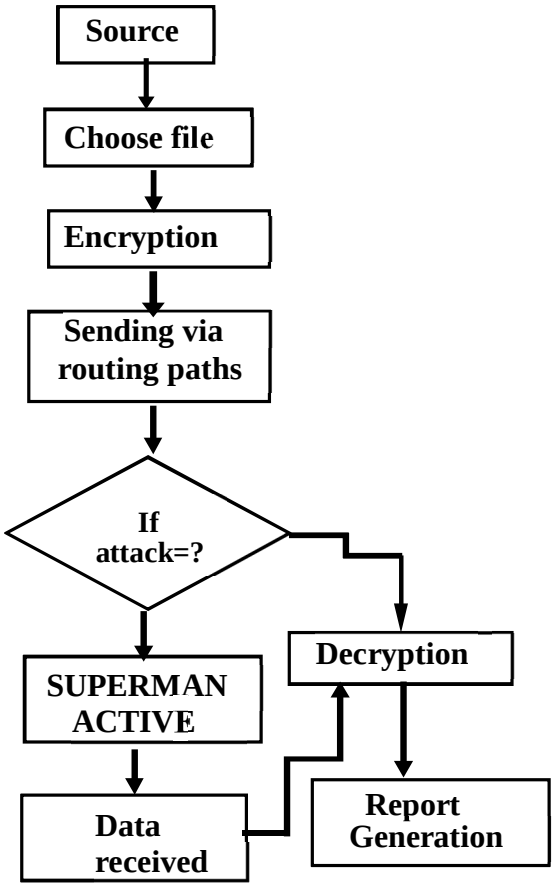


Figure 3: Flowchart of proposed system

The flowchart clearly shows the overall representation of flow of the proposed scheme. The attack in the MANET may be active attacks or passive attacks or it may be internal or external. If the data transmission is get delayed between the intermediate nodes it may also considered as a attack and the data loss is prevented by activating the SUPERMAN node[1]. The data loss may happen by aforementioned possible attacks or it may be any disaster that interrupts the data transmission between the nodes that are participated in the network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

VI. PERFORMANCE ANALYSIS

The performance of SUPERMAN framework is compared with Secret Common Randomness Establishment Algorithm in order to compare the security overhead between these mechanisms in MANET. To determine the security overhead two terms are considered, number of tasks and number of megabytes for security overhead. These two terms are taken for both SUPERMAN framework and SREA algorithm to represent graphically. Number of Mega Bytes for Security Overhead in MANET is defined as the number of Mega bytes required for routing process in the network with minimal security overhead. It is measured in terms of numbers as follows,

$$SO = \frac{(f(c)*(n\ (n-1)))*(h + t)}{P} \quad (1)$$

In Equation (1), f(c) denotes the number of rounds needed by given consensus based distributed task allocation algorithm[1]. The number of nodes is denoted by n. The header and tag size are denoted as h and t respectively. When the number of mega bytes for security overhead is lesser, the method is to be more efficient. The graphical representation of number of mega bytes for Security Overhead for SUPERMAN framework and SREA(Secret Common Randomness Establishment Algorithm) [5] is shown in fig 4.The measure of number of mega bytes for security overhead for the SUPERMAN framework and SRE Algorithm is compared to evaluate the performance of these two mechanisms. The comparison graph fig.4 clearly shows that the number of mega bytes required for security overhead is lesser than Secret Common Randomness Establishment Algorithm (SREA).

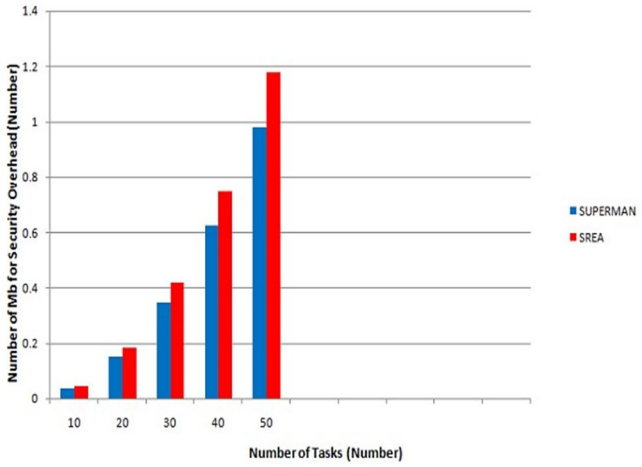


Figure 4: Measure of number of Mb for Security Overhead

The above graph describes the comparison of number of kilo bytes for security overhead for number of tasks using two techniques, namely Secret-Common Randomness Establishment Algorithm (SREA), Secure framework (SUPERMAN) . When number of tasks gets increased, the number of kilo bytes for security overhead gets increased correspondingly. The graphical representation of number of kilo bytes for security overhead for different techniques is explained in the above figure.

The number of kilo bytes for security overhead of SUPERMAN is lesser than SREA. SUPERMAN allows network and routing protocols to present their functions for node authentication, access control and communication security mechanisms. SUPERMAN joins routing and communication security at network layer. This in turn helps to reduce the number of kilo bytes for security overhead. The number of kilo bytes for security overhead of SUPERMAN is lesser than Secret Common-Randomness Establishment Algorithm[5].

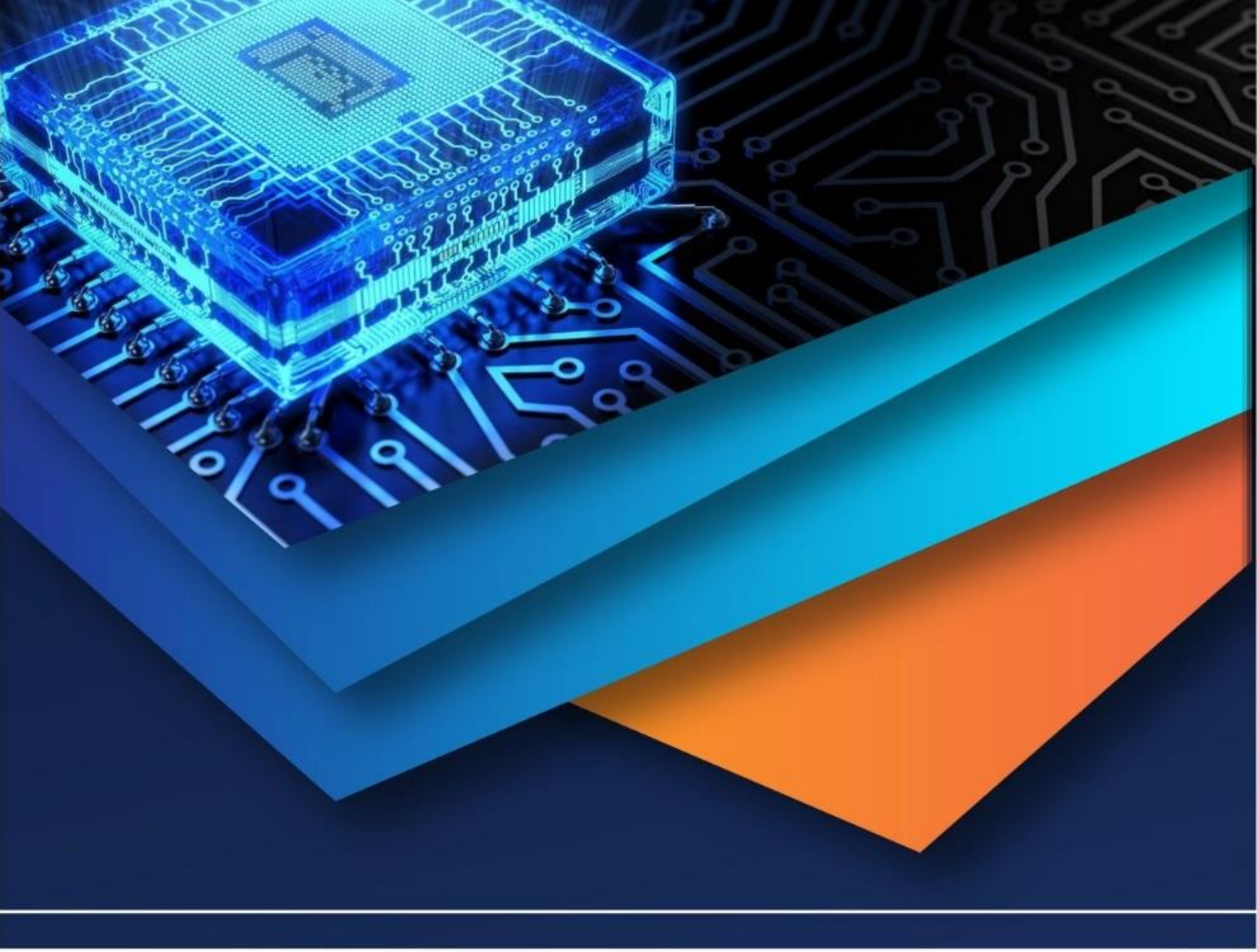
VII. CONCLUSION AND FUTURE WORK

Since MANET has dynamic infrastructure and no centralized management, it is susceptible to various types of attacks. Therefore security need are higher in mobile ad hoc network as compared to traditional networks. The research regarding security issues in MANET is still open as the solutions are designed to only a limited kind of attacks and vulnerabilities. Existing system protects only routes or communication but not both. The communication is commonly wireless also called mobile mesh network[9]. Wireless communication can be trivially intercepted by any node in range of the transmitter. This may cause attacks like the Sybil attack and route manipulation attacks that can compromise the integrity of the network.

As there is no universal algorithm to protect against those attacks , secure routing protocol is still a question among researches. Routing protocols are designed on the basis of changing topology of the MANET while the security issues are ignored. When malicious node work together they cause huge damage. Various literature survey has been undertaken to detect malicious nodes and their attacks in MANET. In existing system there is no cent percent assurance of data confidentiality and data integrity but in proposed system this implementing AES encryption algorithm. In existing system security protocols have been developed to protect routes or communication, but not both. So there is a need to protect both routes and communication. To resolve this, a framework called SUPERMAN is proposed that protects both routing and communication in MANET. The future work involves the SUPERMAN framework is to be used in large scale of ad hoc networks without need of high bandwidth and capacity in the nodes and the experimental results are taken and analysed.

REFERENCES

[1] Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", IEEE Transactions on Mobile Computing, Vol.16, Issue.10, Oct 1, 2017
[2] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, Vol.10, Issue.4, April 2010
[3] Priyanka Goyal, Vinti Parmar, Rahul Rishi,"MANET: Vulnerabilities, Challenges, Attacks, Applications", International Journal of Computational Engineering and Management, Vol.11, Issue.3, Jan 2011
[4] Zaiba Ishrat, " Security issues, challenges & solutions in MANET", International Journal of Computer Science and Technology, Vol.2, Issue.4, Dec 2011.
[5] C. Daniel Nesa Kumar, Dr. V. Saravanan "A Survival Study on Energy Efficient And Secured Routing In Mobile Adhoc Network "International Organization of Scientific Research Journal of Computer Engineering,, Vol.2, Issue.1,Feb 2018.
[6] Kirti Gupta, Dr. Pardeep Kumar Mittal, " An Overview of Security in MANET", International Journals of Advanced Research in Computer Science and Software Engineering , Vol.7, Issue.6, June 2017.
[7] Dr. Gurjeet Singh Dhillon, "Vulnerabilities & Attacks in Mobile ad-hoc Networks (MANET)", International Journal of Advanced Research in Computer Science, Vol.8,Issue.4,May 2017.
[8] E. Edwin Lawrence, Dr.R. Latha, "A Comparative Study of Routing Protocols for Mobile Ad-Hoc Networks",International Journal of Computer Science and Mobile Computing,Vol.3, Issue.11,Nov2014.
[9] Anshul Jain, Sumeet Dhillion , Yogendra Kumar Jain,"Secure Mobile Adhoc Network using AES and RSA"International Journal of Computer Science and Information Technologies,Vol.7, Issue.4,Sep 2016.
[10] Jozef Filipek, Ladislav Hudec, "Security Architecture for Mobile Ad-Hoc Network" , Journal of Electrical Engineering, Vol.69, Issue.3, July 2018.
[11] Shikha Jain, "Security Threats in MANET: A Review" ,International Journey on Information Theory, Vol.3, No.2, April 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY