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.2019.1078

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

Secured System for Social Network Based an Access Control & Prevention Application

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

Abstract: ***Mobile ad hoc networks pose new kinds of security problems, caused by their nature of collaborative and open systems and by limited availability of resources. Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks in military government, commercial applications etc. Privacy-preserving routing is crucial for such ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks.***

This paper proposes a system to develop social Network Based Access Control and detection of the defected node and lost packet during the transition of file from source to destination. In propose of system, file is successfully transferred without any packet loss.

Keywords: Ad-hoc Network, Routing, Security, Attacks, MANET, Diffie-Hellman key generation algorithm, Dijkstra's Algorithm, MD5 Algorithm.

I. INTRODUCTION

Routing is a basic functionality for mobile ad hoc networks (MANETs) [1]. These networks are decentralized, with nodes acting both as hosts and as routers, forwarding packets for nodes that are not in transmission range of each other [2]. Next generation of wireless communication systems, there is a tremendous need for the rapid deployment of independent mobile users. Significant examples include emergency search/rescue missions, disaster relief efforts, mine site operations, battlefield military operations, electronic classrooms, conferences, convention centers, etc. Routing in ad hoc networks has been an active research area and in recent years numerous routing protocols have been introduced for MANETs. The deployment of such networks still faces challenges, such as limited physical security, node mobility, and limited resources (i.e., processor, power, bandwidth, storage). The major issues that affect the design, deployment, and performance of a MANET include: medium access scheme, routing, multicasting, transport layer protocol, pricing scheme, quality of service provisioning, self-organization, security, energy management, addressing and service discovery, scalability and deployment consideration. The protocol design issues are inherently related to the underlying ad hoc applications [3]. A great number of current applications require a reliable multicast scheme, meaning that one sender must ensure data delivery to multiple receivers; this may sometimes be hard to do, especially in a wireless environment [4]. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect users' mobility behavior or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments [5]. In this paper propose system to Develop Social Network Based Access Control and detection the defected node and lost packet during the transition of file from source to destination. In propose a system a file is successfully transferred without any packet loss.

II. BACKGROUND

Routing is a basic network functionality that supports Communication. In MANETs, each node acts as a router forwarding data to other nodes. We distinguish three basic phases in routing: 1) route discovery in which one or more routes (of adjacent nodes) that link a source S to a target T are sought, 2) route maintenance in which broken links of established routes are fixed, and 3) packet forwarding in which communication is achieved via established routes [1]. In general, encryption is used to combat such attacks. Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network [2]. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the ad hoc network are involved, the attacks are referred to as internal attacks [3]. Major challenges that a routing protocol designed for Ad Hoc wireless networks faces include: mobility of nodes, resource constraints, error-prone channel state, and hidden and exposed terminal problems [4]. A number of anonymous routing schemes have been proposed for ad hoc networks in recent years, and they provide different level of privacy protection at different cost. Most of them rely on public key cryptosystems (PKC) to achieve anonymity and unlink ability in routing. Although asymmetry of PKC can provide better support for privacy protection, expensive PKC operations also bring significant computation Overhead [5].

This paper is organized as follows.

Section I contains Introduction of this paper. In Section II discussed Background. Section III introduced previous work done. Section IV explains existing methodologies. In Section V discussed existing framework and analyzed it. Section VI presents the proposed work. Its outcome possible results are analyzed in Section VII. Section VIII concludes this paper. Finally Section IX presents future scope.

III. PREVIOUS WORK DONE

Mobile ad hoc networks pose new kinds of security problems, caused by their nature of collaborative and open systems and by limited availability of resources. In this article DavideCerri and Alessandro Ghioni(2008) [1], consider a Wi-Fi connectivity data link layer as a basis and focus on routing security. Here discuss the implementation of the secure AODV protocol extension, which includes tuning strategies aimed at improving its performance. Namely, propose an adaptive mechanism that tunes SAODV behavior. Moreover, we analyze our adaptive strategy and another technique that delays the verification of digital signatures.

In research Mike Burmesterand and Breno de Medeiros(2009) [2], show that the security proof for the route discovery algorithm endairA is flawed, and moreover, this algorithm is vulnerable to a hidden channel attack. It also analyzes the security framework that was used for route discovery and argues that compos ability is an essential feature for ubiquitous applications. And conclude by discussing some of the major security challenges for route discovery in MANETs.

In article Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani(2008) [3], discuss a DSR model is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. There is no beacon (does not require a periodic update hello packet, which are used by a node to inform its neighbors of its presence). Bander H. AlQarni and Ahmad S. AlMogren (2014) propose a technique REEDDRE, routes are established based on on-demand techniques. Route discovery in proposed protocol and other reactive protocols is based on the request route (RREQ) packet and route reply(RREP) packet has been used for traditional AODV protocol. In proposed protocol, a modification to this request reply packet procedures is proposed. In research Zhiguo Wan, KuiRen, and Ming Gu(2012) [5], propose a protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature. The setup of USOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme like.

IV. EXISTING METHODOLOGY

A. The A-SAODV Secure Routing Prototype

A-SAODV is a multithreaded application: cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other messages [1]. Therefore, in A-SAODV, there are two execution threads: one dedicated to cryptographic operations and the other to all other functions (routing message processing, SAODV routing table management, timeout management, SAODV message generation, and data packet forwarding). The two threads communicate via a first input first output (FIFO) queue containing all the messages that must be signed or verified. In AODV, allowing intermediate nodes to generate RREPs on behalf of the destination node has a positive impact on performance, because it does not require heavyweight operations by intermediate nodes themselves. The situation is different in SAODV, because generating such a reply requires the intermediate node to generate a cryptographic signature: nodes may spend much time in computing these signatures and become overloaded.

B. The Protocol End Air

The protocol endairA is claimed to be proven secure in the ABV security framework. This implies that the route can be uniquely partitioned as follows: each partition consists of a single non compromised identifier (label) or a sequence of consecutive compromised identifiers. A plausible route is one whose partitions correspond to that of a real route that physically exists in the network. The security statement of endairA is that it only accepts plausible routes. The ABV model prohibits direct communication (either via wireless links or through any out-of-band channels) between two adversarial nodes [2].

C. Destination Sequenced Distance Vector protocols (DSDV)

Destination Sequenced Distance Vector protocols (DSDV) is based on Bellman-Ford shortest path algorithm. Each node has a table, which contains the shortest path to every other node in the network. These tables are constantly updated and forwarded to other nodes in the network whenever a change is detected. When a node receives an update it can either update the tables or hold it for a while in order to select shortest route. Fig:1 shows an example where node 1 is the source and node 15 is the destination [3].

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

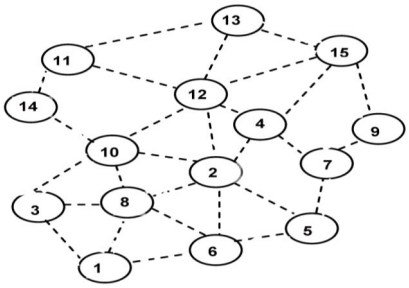


Fig 1. Route establishment in DSDV

D. The Unobservable Routing Scheme

The unobservable routing scheme comprises of two phases: anonymous key establishment as the first phase and the route discovery process as the second phase. In the first phase of the scheme, each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node [5]. Fig:2 shows the mathematical model for Anonymous key establishment Anonymous key establishment. S broadcast the first message to its direct neighbors. Each of S's neighbors does the same things as X does to learn S's local broadcast key. kSX = H2(rSrXP) as shown.

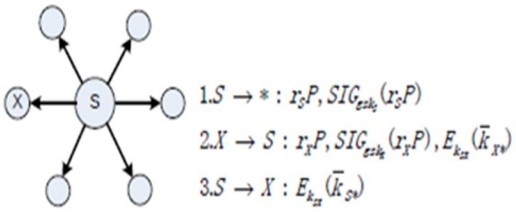


Fig:2 Anonymous key establishments

E. Route Discovery in REEDDRE Protocol

In REEDDRE, routes are established based on on-demand techniques. Route discovery in proposed protocol and other reactive protocols is based on the request route (RREQ) packet and route reply(RREP) packet has been used for traditional AODV protocol. In proposed protocol, a modification to this request reply packet procedures is proposed. In proposed model, apply tones to these requests and reply packets that will be sent before the RREQ and RREP packets to make model more efficient in terms of saving the network resources. Since proposed model is supporting using tones of short pluses, adding predefined tones for the request and reply mechanism [4].

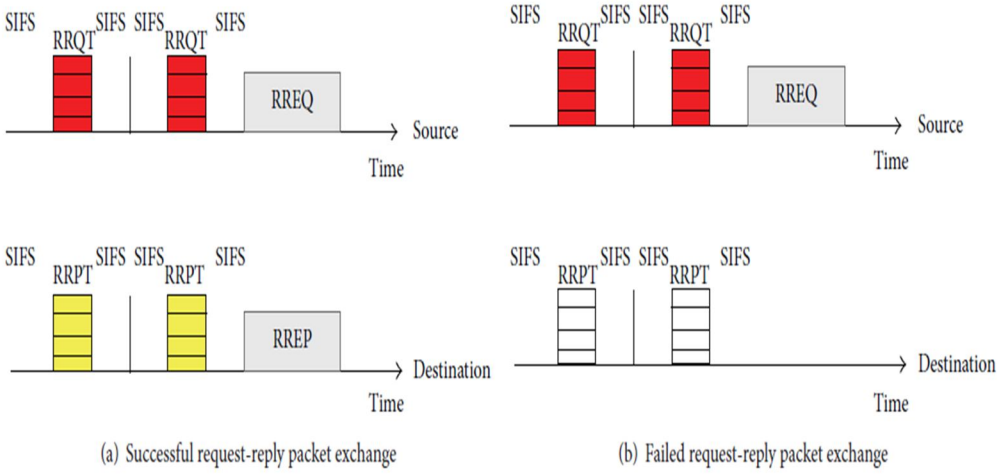


Fig 3: Route discovery in REEDDRE

V. ANALYSIS AND DISCUSSION

In order to combat passive and active attacks, a secure ad hoc network is expected to meet the following different security requirements

1) *Confidentiality*: Only the intended receivers should be able to interpret the transmitted data.
2) *Integrity*: Data should not change during the transmission process, i.e., data integrity must be ensured.
3) *Availability*: Network services should be available all the time and it should be possible to correct failures to keep the connection stable.
4) *Authentication*: Every transmitting or receiving node has its own signature. Nodes must be able to authenticate that the data has been sent by the legitimate node.
5) Non-Repudiation: Sender of a message shall not be able to later deny sending the message and that the recipients shall not be able to deny the receipt after receiving the message.

Table:1 outlines different active attacks that have been used in the literature to study the performance of routing protocols corresponding to above described security requirements. We use these attacks along with the security requirements as a guide to review the salient passive, active, and hybrid routing protocols for MANETs [3].

Protocols	Advantages	Disadvantages
AODV	In AODV, route discovery process is in on demand, which is more efficient in dynamic nature of mobile as-hoc network.	Due to on demand manner, it won't check route in periodic interval so transmission of data after discover the route is taking some more delay.
DSR	The route is created only when it is required and the nodes utilize the route cache information efficiently to reduce the overhead and collision.	The route maintenance mechanism does not locally repair a broken link. The delay is higher than in table-driven protocols.
DSDV	DSDV was one of the early algorithms available. It is quite suitable for creating as hoc networks with small number of nodes.	DSDV requires a regular update of it routing tables, which uses up battery power and a small amount of bandwidth.

Table 1. Active Ad Hoc Network Protocols.

VI. PROPOSED METHODOLOGY

A. Social Network Based Access Control & Prevention Application

This paper proposes a System to Develop Social Network Based Access Control & Prevention Application. Fig:4 shows the flow chart of proposed system. And Fig:5 shows the architecture of proposed system. Architecture is describing the user and admin flow. User can send the file from source to destination, view router on which file is transfer and attackers list also. User can block the router on which attacker is found. In admin section, admin mange the users, file and attackers.

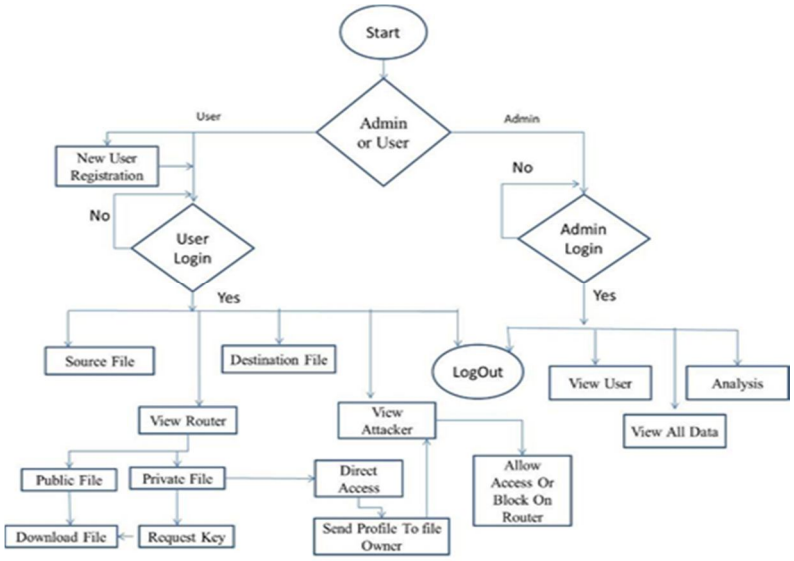


Fig: 4 Flow chart

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

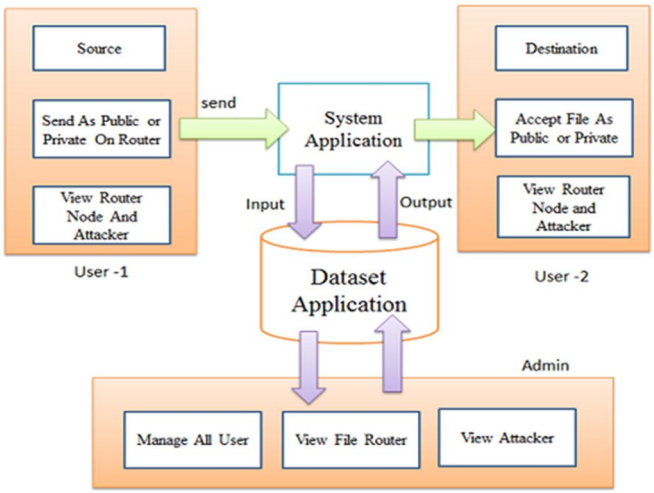


Fig: 5 Secure Routing Architecture

In this paper, for a proposed system two algorithms are designed. Considering the first algorithm as a base.

1) *Diffie-Hellman key Generation Algorithm:* The Diffie-Hellman key generation algorithm is an example of a means of generating symmetric keys without the need to explicitly communicate any sensitive key information. Nodes exchange locally generated data using globally known primes and local secret data. The resulting variable (referred to as a key-share) is then communicated by both nodes, facilitating the calculation of a symmetric key that is identical at both ends, without the need to communicate sensitive data at any point. This allows the discreet and secure establishment of node-to-node confidentiality between specific node pairs.

2) *Dijkstra's Algorithm - Shortest Path*

a) *Step 1*: Temporarily assign C(A) = 0 and C(x) = infinity for all other x. C(A) means the Cost of A C(x) means node x getting current cost.

b) *Step 2*: Find the node x such that it have the smallest temporary value of c(x). If there are no such temporary nodes or if c(x) = infinity, then stop. Now node X is as permanent node and labeled as the current node. C(x) and parent of x will not change again.

c) *Step 3*: For each temporary node labeled vertex y adjacent to x, make the following comparison: if c(x) + Wxy < c(y), then c(y) is changed to c(x) + Wxy assign y to have parent x

d) *Step 4*: Return to step 1. For continue the all remaining nodes.

3) *MD5 Algorithm (Message-digest algorithm)*

a) The file authentication will be check by MD5 algorithm

b) Input file

i) convert file in 512 blocks

ii) compress all data in 128 bit

iii) Divides the data in 4 blocks of 32bit

iv) apply binary shifting to each block

v) Convert each block in hex value

vi) combine all blocks and create a hash value of 128 bit

c) 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 RESULTS

The proposed an architecture for security routing of mobile network. In this architecture detect the damage packet and node on which it damages packets. Here 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

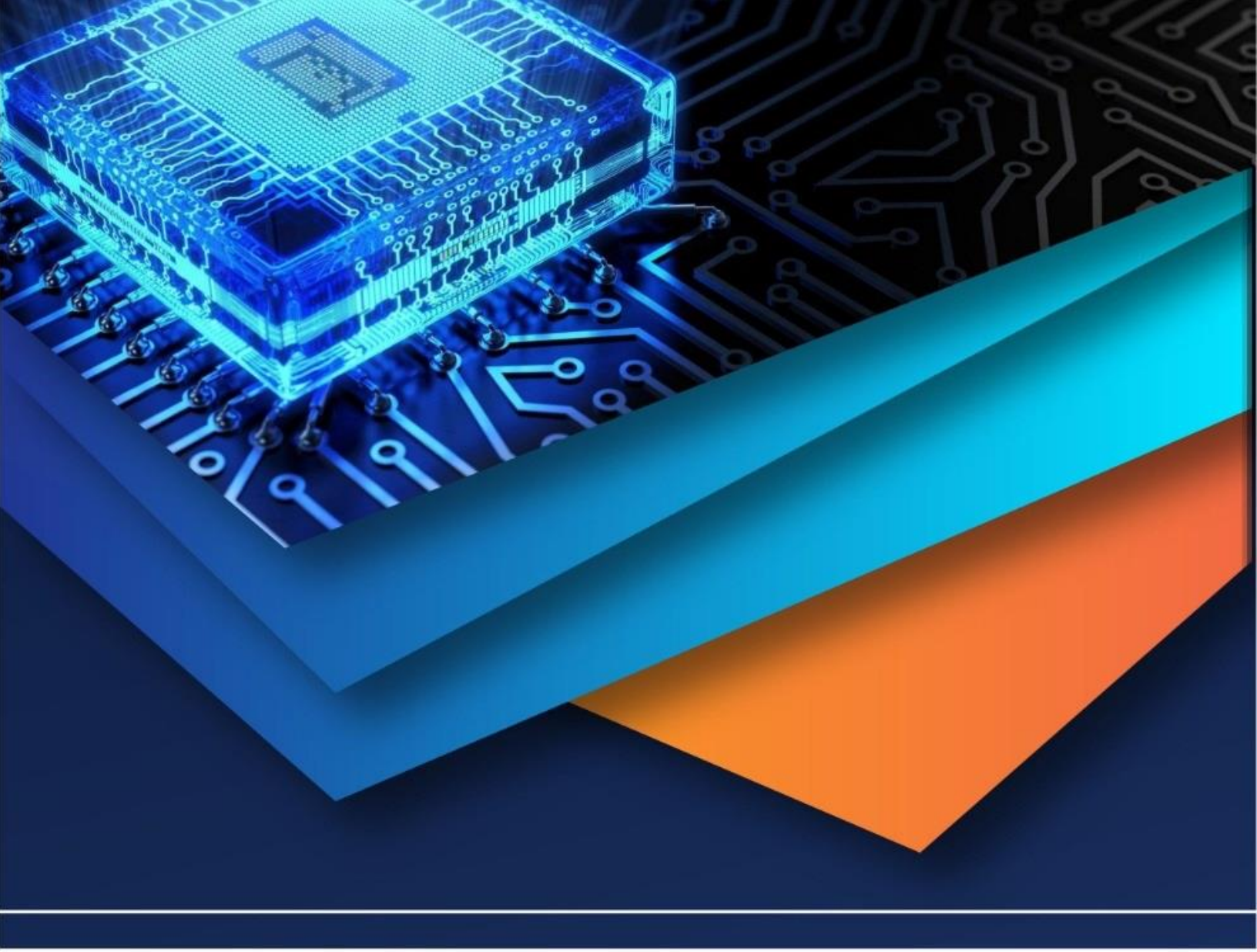
Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks. In this paper propose system to Develop Social Network Based Access Control and detection the defected node and lost packet during the transition of file from source to destination. In propose a system a file is successfully transfer without any packet loss.

IX. FUTURE SCOPE

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 attack. Means to prevent the transaction of file transformation from same attack in future.

REFERENCE

[1] DavideCerri and Alessandro Ghioni," Securing AODV: The A-SAODV Secure Routing Prototype", SECURITY IN MOBILE AD HOC ANDSENSOR NETWORKS (IEEE Communications Magazine), February 2008.
[2] Mike Burmesterand and Breno de Medeiros," On the Security of Route Discovery in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 8, September 2009
[3] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani," A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 10, Fourth Quarter 2008
[4] Bander H. AlQarni and Ahmad S. AlMogren," Reliable and Energy Efficient Protocol for MANET Multicasting," JOURNAL OF COMPUTER NETWORKS AND COMMUNICATIONS (Hindawi Publishing Corporation), Vol2016, May 2016
[5] Zhiguo Wan, KuiRen, and Ming Gu," USOR: An Unobservable Secure On-DemandRouting Protocol for Mobile Ad Hoc Networks," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, vol. 11, May 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY