Multifarious Secured Path for Stable Routing in Mobile Ad Hoc Networks

Gaurav Sharma, Surbhi Dhiman

Abstract: A Mobile Adhoc Network (MANET) is characterized by mobile nodes, multi hop wireless connectivity, infrastructure less environment and dynamic topology. A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Stable and secure routing and power efficiency are the major concerns in this field. This paper is an effort to study security problems associated with MANETS and solutions to achieve more reliable routing. The ad hoc environment is accessible to both legitimate network users and illegitimate attackers. The study will help in making protocol more robust against attacks to achieve stable routing in routing protocols.

Keywords: Ad hoc Networks, AODV, security, wireless network, packet delivery

I. INTRODUCTION

Since their emergence in the 1970s, wireless networks [1, 11] have become increasingly as popular in the computing industry. This is particularly true within the past decade, which has seen wireless networks being adapted to enable mobility. Wireless networks allow users to access information and services via electronic medium, without taking geographic positions in account. Mobile hosts and wireless networking hardware are becoming widely available, and extensive work has been done recently in integrating these elements into traditional networks such as the Internet. Wireless networks have taken the world by storm. Enterprises and homeowners are avoiding the expenses and delays associated with installing wired networks. High-speed Internet facility is enjoyed by travelers all over the places worldwide. With increases in throughput, wireless networks remain unlicensed and affordable. This has further helped their exponential growth in businesses, homes, communities and open spaces. There are currently two variations of mobile wireless networks: Infra-structured or Infrastructure less [10, 12, 13, 18, 19, 20]. In Infra-structured wireless networks, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station that is within its communication radius. Figure 1, given below depicts the Infra-structured wireless network. Typical applications of this type of network include office wireless local area networks (WLANs). In Infrastructure less wireless network commonly known as an ad hoc network; the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers.

Revised Version Manuscript Received on June 06, 2017.

Gaurav Sharma, Associate Professor, Department of Computer Science and Engineering, JMIT Radaur, Yamunanagar (Haryana), India. E-mail: gauravsharma@jmit.ac.in

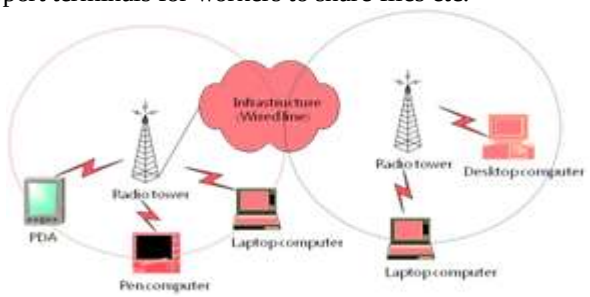
Surbhi Dhiman, M. Tech Scholar, Department of Computer Science and Engineering, JMIT Radaur, Yamunanagar (Haryana), India. E-mail: surabhi2308@hotmail.com

The mobile nodes in the Ad Hoc network dynamically establish routes among themselves to create their own network architecture on the fly. This type of network can be shown as in figure 1. Due to the self-configuration and self-maintenance capabilities, mobile ad hoc networks (MANETs) become more vulnerable. So, Security challenges have become a primary concern to provide secure communication between mobile nodes.

II. AD HOC NETWORK

An Ad hoc network [1, 11] is a self-configuring network of wireless connections connecting mobile nodes. These nodes may be routers and/or hosts. Each node or mobile device is equipped with a transmitter and receiver. They are said to be autonomous, dynamic and purpose-specific. Ad hoc networking is a concept in computer technology, which means that users wanting to communicate with each other form a temporary network, without any kind of central administration. Term Ad hoc means a network which can take different forms in terms of topologies and in term of devices used. Ad hoc devices can be mobile, standalone or networked. MANETs [16] are best suited for emergency situations as they facilitate fully distributed, self maintainable dynamic topology networks that operate without the use of external infrastructure.

MANET [4, 5] is an autonomous system of mobile hosts which are free to move around randomly and organize themselves arbitrarily. Mobile ad-hoc networks are infrastructure-less networks consisting of wireless, possibly mobile nodes which are organized in peer-to-peer and autonomous fashion [17]. In a distributed Mobile Ad Hoc Network (MANET), collaboration and cooperation is critical concern to managing trust. The networks work well only if the mobile nodes are trustworthy and behave cooperatively. MANET is a suitable system which can support some specific applications as virtual classrooms, military communications, emergency hostile environments, search and rescue operations, data acquisition in communications set up in exhibitions, conferences and meetings, in battle field among soldiers to coordinate defense or attack, at airport terminals for workers to share files etc.



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

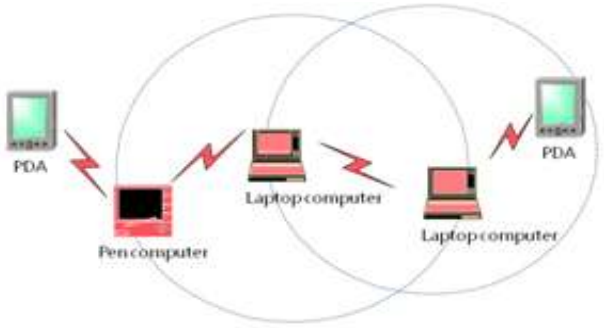


Fig. 1: Infra-structured and Infra-structure less Network

In Ad hoc networks nodes can change their positions quite frequently. The nodes in an ad hoc network can be laptops, PDA (personal digital assistant), cell phones or palm tops, etc. They have limited resources such as CPU capacity, storage capacity, battery power and bandwidth. Each node participating in the route establishment acts both as a router and as a host and must therefore be transferring packets to other nodes. For this purpose a routing protocol is needed and the new protocol should try to minimize control traffic. The most important characteristic of ad hoc network is dynamic topology, which is a result of node mobility. It should be reactive i.e. calculates routes only upon receiving a specific request.

MANET is working on routing specifications for Ad hoc networks. This research work will evaluate some of the existing protocols and suggests a new protocol. To accomplish this task, several routing protocols for Ad hoc networks have been studied such as Dynamic Source Routing (DSR)[6], Dynamic Distributed Routing (DDR)[7], Temporarily Ordered Routing Algorithm (TORA)[2], Ad Hoc On Demand Distance Vector Routing (AODV)[4,5]. In all the protocols major emphasis has been on stable and shortest routes ignoring the major issue of delay in response whenever break occurs. Most of the protocols proposed require knowledge of the network topology for routing. These protocols involve communication overheads of route discovery, route establishment and maintenance. Later, position based protocols were proposed to eliminate these overheads. Most of the protocols in this category, however, use single route and do not utilize multiple alternate paths. Those routing protocols should also minimize the usage of valuable resources such as bandwidth, power and processor.

III. MANET CHALLENGES

The special features of mobile ad hoc networks bring great technological opportunities together with different challenges [9, 10]. Some of the key challenges in the area of mobile ad hoc networks include:

1. Unicast routing
2. Multicast routing
3. Dynamic network topology
4. Speed
5. Frequency of updates or Network overhead
6. Scalability
7. Mobile agent based routing
8. Secure routing
9. Quality of Service
10. Energy efficient/Power aware routing

IV. SECURITY ISSUES OVER AD HOC NETWORKS

Many organizations including retail stores, hospitals, airports and business enterprises plan to capitalize on the benefits of going wireless. But if we think about the security of the modern wireless network, this wouldn't looks so positive. There have been numerous published reports and papers describing attacks on wireless networks that expose organizations to security risks such as attacks on confidentiality, integrity, non repudiation and network availability [8, 9]. There are various proposals to solve these issues but they target the specific threats separately. Therefore, there is a requirement to have an efficient security system which takes care of all aspects of security.

Security Threats: Network security attacks are typically divided into passive & active attacks as explained below:

Passive Attack: An attack in which an unauthorized party gains access to an asset and does not modify its content. Passive attacks are eavesdropping and traffic analysis (sometimes called traffic flow analysis). The two passive attacks are described below:

a) Eavesdropping
b) Traffic analysis

a) **Eavesdropping:** The attacker monitors transmissions for message content. An example of this attack is an intruder listening to the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.

b) **Traffic analysis:** The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties which an intruder can analyse.

Active Attack: An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it is not preventable. Active attacks may be one of the four types i.e. masquerading, replay, message modification, and Denial-of-Service (DoS). These attacks are summarized as:

a) Masquerading / Spoofing
b) Replaying
c) DoS

a) Masquerading: The attacker impersonates a legitimate user and gains certain unauthorized privileges. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

b) Replay: A replay is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the sender or by an adversary who intercepts the data and re-transmits it [22].

c) Denial-of-Service: The intruder seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the network.

The consequences of these attacks include loss of proprietary information,

legal and recovery costs, tarnished image, and loss of network service. Due to the dynamically changing topology and infrastructure less, decentralized characteristics, security is difficult to achieve in mobile ad hoc networks. Hence, security mechanisms have to be a built-in feature for all sorts of ad hoc network based applications.

V. EXISTING SECURITY MEASURES

Some of the measures that can be incorporated are:

1. Virtual Private Networks (VPN): This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Softwares are available to implement VPNs on every platform. Authentication depends upon three factors such as password, fingerprints and a security token.

2. Encryption: Encryption is a technique used for many years for passing information from one place to other in a secured manner. A message in its original shape is referred to as a plain text (or Text) and a message used to conceal original message is called Cipher text (or Cipher). The process of changing plain text into cipher text is called Encryption and the reversal is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA). These algorithms are key based algorithms.

3. One Way Hash Function: There is another algorithm called one way hash Function. It is like checksum of a block of text and is secure. It is impossible to generate the same hash function value without knowing the correct algorithm and key. It accepts a variable size message and produces an affixed size tag as output.

4. Digital Signature: A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A digital signature [21] makes a receiver think that the message was created by a known sender (authentication), and the sender cannot deny having sent this message (non-repudiation), and the message integrity was not lost in transit. Digital signatures are easily transferrable, cannot be imitated by other person, and can be automatically time-stamped. External attacks can be detected using confidential routing information and authentication and integrity assurance features. Encryption can be solution to this by applying digital signature.

VI. PROPOSED MODEL

The effort is to propose a solution for routing in Ad hoc networks by tackling the core issue of stability and security. A protocol will be developed which improves existing on-demand routing protocols by adding security parameter. An effort will also be made to develop a cryptographic algorithm or to implement new strategy to existing algorithm.

The scheme will establish multi paths without transmitting any extra control message. It will offer quick adaptation to distributed processing, dynamic linking, memory overhead and loop freedom. The proposed scheme will respond to link breakages and changes in network topology in a timely manner. The distinguishing feature will be security factor for Ad hoc routing protocol.

The work will present a new scheme based on stable and secured nodes and the goal is to be able to address the following features:

- The proposed scheme performs better for finding a good route, such that better packet delivery is assured.
- The scheme performs well in denser mediums.
- Scheme should be successful in minimum hop count as metrics for optimality.
- The Scheme should offer Secured Routing
- It should be able to provide stable route selection.
- The Proposed scheme should perform with both bi-directional and unidirectional traffic patterns.

The Metrics [1, 3, 12, 15] that will be used for Performance evaluation and comparison are:

- **Packet Delivery Ratio**: The fraction of successfully received packets, which survive in finding their way to destination is called packet delivery ratio. This performance metric determines the correctness and completeness of the routing protocol.

PROPOSED ALGORITHM (CAODV)

In proposed algorithm there are three parts as

A. Route Request,

B. Route Reply &

C. Data Transmission.

A. Route request phase is started using Source and Destination nodes. At the time of route request it uses malicious and non-malicious nodes. Nodes are verified one by one as:

If node status is True then this node enters into the Non_Malicious array &

if node status is False then this node enters into the Malicious_array.

A.1: Initialize/ activate the following variables for:

Count Number of hackers
Identification number for nodes
Total Nodes
Source node ID
Destination node ID
Arrays for malicious/ non malicious nodes

A.2: Set each node Status (True/False) from source to destination

A.3: Detect attacking nodes by checking status

```
if nNodeStatus== "FALSE"
   nhackers++;
   nhack_NodehackerNode[i]=Node;
   else if nNodeStatus== "TRUE";
   nNon_MaliciousNode[i]=Node;
```

B. Route reply starts from destination node checking each node.

If status of node = TRUE, All the possible routes will be searched by RREP. Then available route will be selected by the RREP broadcasting. It repeats procedure until it reaches source node. Source node will select the path for data transmission.

B.1: Destination Node rebroadcast the RREP like the RREQ

B.2: All the possible routes will be searched by RREP. Then available route will be selected by the RREP broadcasting.

B.3: Source node will select the path for data transmission.

C. Data Transmission starts from initial to final node.

If node id is between Source Node & Destination Node, then it set status of this node = TRUE otherwise it set status of this node = FALSE.

C.1: Start transmitting of packet from Source to Destination.

C.2: Initialize loop for detecting malicious nodes from array.

C.3: After detecting malicious node CAODV will send an error message to the source node. Source node will declare it as a malicious node by making its Status = "FALSE" in the routing table and the present route will be deactivated and new route is searched.

This process repeats until CAODV establishes a stable and secure path for data transmission.

- **End-to-End Delay**: Average end-to-end delay is the delay experienced by packets which successfully delivers to their destinations. This denotes the efficiency of the underlying routing algorithm, because delay primarily depends on optimality of path chosen.
- **Throughput:** This declares overall throughput in terms of packets received and helps in performance evaluation of the proposed scheme.

VII. PERFORMANCE EVALUATION

The evaluation is carried out using the Network simulator (NS-2) by performing several experiments that describes the performance of the system. The simulation parameters like number of nodes, speed, etc. are given in table 2 along with their respective values and are used to examine the performance of the network. For all the simulations, the comparison is performed on the basis of pause time & speed.

Table 2: Simulation Parameters

Parameter	Value	Description
Simulation Time	600 ms	Maximum execution time
Terrain Dimensions	1Km × 1Km	Physical area in which the nodes are placed in meters
Number of Nodes	50	Nodes participating in the network
Performance Parameter	Through put, End to End delay, Packet delivery ratio	Parameter considered in evaluating
Routing Protocol	AODV, MAODV, CAODV	Routing protocol Used

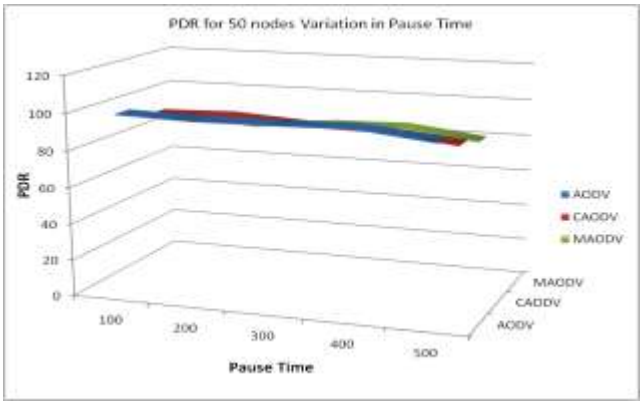


Fig 2: Packet Delivery Ratio for 50 Nodes vs. Pause Time

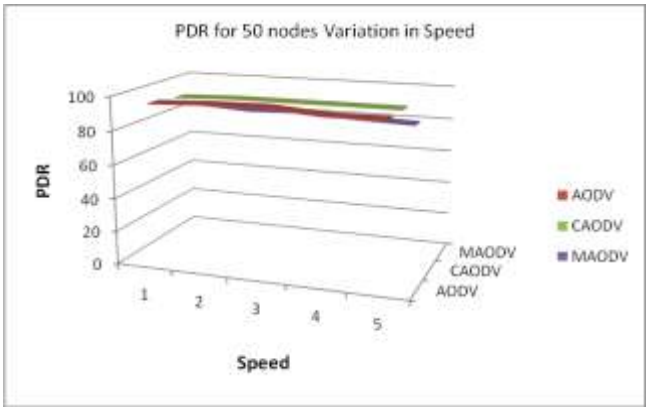


Fig 3: Packet Delivery Ratio for 50 Nodes vs. Speed

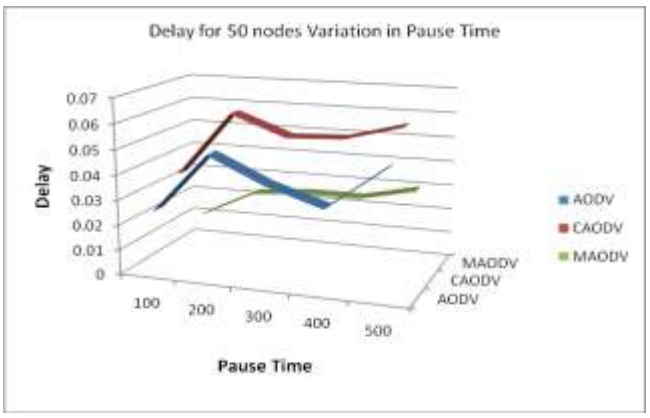


Fig 4: End-To-End Delay for 50 Nodes vs. Pause Time

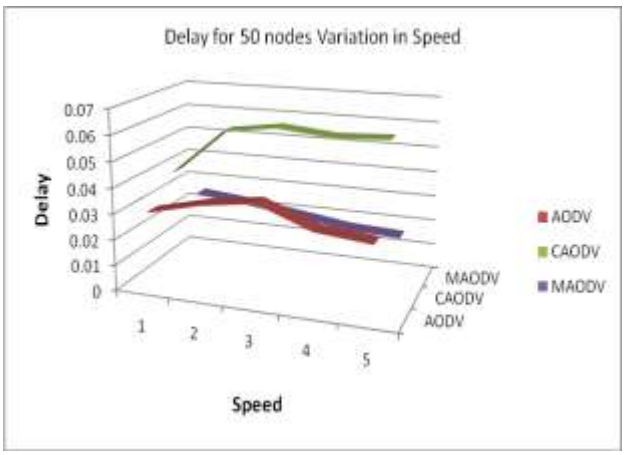


Fig 5: End-To-End Delay for 50 Nodes vs. Speed

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

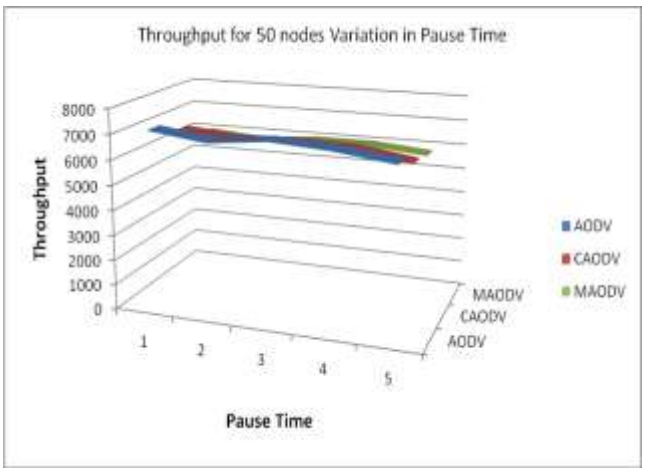


Fig 6: Throughput for 50 Nodes vs. Pause Time

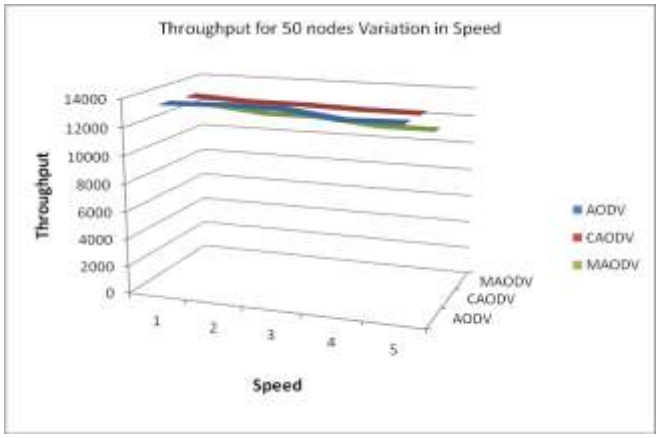


Fig 7: Throughput for 50 Nodes vs. Speed

VIII. CONCLUSION AND RESULTS

The existing routing protocols are typically attack-oriented. They first identify the security threats and then enhance the existing protocol to conquer such attacks. The ultimate goal for ad hoc network security is to develop a multifarious security solution that results in in-depth protection that offers multiple lines of defense against both known and unknown security threats. When MANET routing is discussed then its working is called better only according to the actual packets transferred between source and destination successfully without packets loss. In this study a multifarious security solution is obtained by developing a new on-demand stable and secure routing protocol. This protocol is designed to provide secure multiple paths having better PDR and high throughput.

REFERENCES

1. Kush, P. Gupta, R. Kumar, "Performance Comparison of Wireless Routing Protocols", Journal of CSI, Vol. 35 No.2, 2005.
2. Kush, P. Gupta, C J Hwang, **"**Stable and Energy Efficient Routing for Mobile Adhoc Networks", Information Technology: New Generations, ITNG, Fifth International Conference, LAS VEGAS USA ,2008, Page(s):1028 – 1033.
3. Bayya Arun et. al., "Security in Ad hoc Networks", Computer Science Department, University of Kentucky, 2013.
4. Parkins and E. Royer , "Ad Hoc on demand distance vector routing", 2nd IEEE workshop on mobile computing , pages 90-100, 1999.
5. Charles Perkins et. al., "Performance of two on-demand Routing Protocols for Ad-hoc Networks", IEEE Personal Communications, February 2001, pages 16-28.
6. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc networks", Kluwer academic publishers, 1996.
7. Y.C. Hu et. al., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF Draft, April 2003,
8. B. J. et. al., "Ariadne: A secure on-demand routing protocol for ad-hoc networks", Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.
9. Hao Yang et. al., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", UCLA Computer Science Department, 2004.
10. Md. Golam Kaosar et. al., "Simulation-Based Comparative Study of On Demand Routing Protocols for MANET", January 2005.
11. NIST, Fed. Inf. Proc. Standards, "Secure Hash Standard", Pub. 180, May 1993.
12. A.Kush and Sunil Taneja, " Simulation of MANET schemes", International Journal of Computing and Business Research, Vol 1, Issue 2, Nov 2010.
13. Kush and Sunil Taneja, "End to End Delay Analysis of Prominent On-demand Routing Protocols" IJCST, International Journal of Computer Science and Technology, Vol 2 Issue 1 March 2011, pp 42-46.
14. Kush et. al., "Encryption Scheme for Secure Routing in Ad Hoc Networks", International Journal of Advancements in Technology, Vol 2, No 1, January 2011, pp22-29.
15. Nitin Goyal and Alka Gaba, "A review over MANET- Issues and Challenges", International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, Vol. 2, Issue 4, April-2013.
16. Sanjay K. Dhurandher et. al., "GAODV: A Modified AODV Against Single and Collaborative Black Hole Attacks in MANETs", 27th IEEE International Conference on Advanced Information Networking and Applications Workshops, Pages 357-362, March 25 - 28, 2013, USA.
17. H Shokrani and S Jabbehdari, "A survey of ant-based routing algorithms for mobile ad-hoc networks", IEEE International Conference on Signal Processing, 2009.
18. Nitin Goyal, Alka Gaba, "A New Approach of Location Aided Routing Protocol Using Minimum Bandwidth in Mobile Ad-Hoc Network", International Journal of Computer Technology & Applications, Volume 4, Issue 4, pp 653-659, July 2013.
19. Nitin Goyal, Alka Gaba, "Review over Diverse Location Aided Routing", Global Journal for Current Engineering Research, Volume 2, Issue 2, pp 141-144, August 2013.
20. Nitin Goyal, Pratibha Kamboj, "Survey of Various Keys Management Techniques in MANET", International Journal of Emerging Research in Management & Technology, Volume 4, Issue 6, pp 176-178, June 2015.
21. https://en.wikipedia.org/wiki/Digital_signature.
22. https://en.wikipedia.org/wiki/Replay_attack.