International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Background Study of MANET

Umer Bashir[1], Ranjan Kumar Singh[2]
[1]M.Tech. Student, Department of Electronics and Communication Engineering, Pulwama, India
[2]Professor & HoD, Department of Electronics and Communication Engineering, Shri Ram College of Engineering & Management, Palwal, India

***Abstract*: Mobile ad-hoc network (MANET) is a collection of autonomous nodes, which have the properties like mobility, wireless. MANETs have dynamic network topology and self-configuring so that nodes in network can move independently in any direction and change their links to other nodes in network frequently. Mobile ad-hoc networks are more vulnerable to security attacks due to their unique characteristics such as dynamic topology, no fixed infrastructure, resource limitations and multi-hop scenario. In MANETs one the dangerous attack is packet dropping attack. This packet dropping attack is two types: 1. Black hole and 2. Gray hole. In both the attacks, an attacker sends the false reply to source node that it is having the shortest route to the destination. In black hole attack, attackers drops all the packets received from source node and in packet dropping attack, attacker drops packets selectively or forwards packets selectively or forwarding packets but not data packets. In this paper, we have proposed mechanism to detect and isolate these attacks in network. To evaluate the performance of our proposed method we used the same scenarios and simulation parameters that are used for simulating the attack. In the proposed solution, the sender sends the packets until the attack is detected and after the attack is detected, it blocks the route and chooses another route for data transmission.**

***Keywords*: MANET**

1. Introduction

A. Ad-hoc networks

Ad-Hoc networks have no organization where the nodes are free to join and left the network. The nodes are interconnected with each other via a wireless link. A node can serve as a router to forward the data to the neighbours' nodes. Therefore, this type of network is also recognised as infrastructure less networks. These networks have no centralized consolidate administration. Ad-Hoc networks have the abilities to handle any malfunctioning in the nodes or any variations that its know-how due to topology changes. Whenever a node in the network is down or leaves the network that causes the link among other nodes is broken. The affected nodes in the network simply request for new routes and new links are established Ad-Hoc network can be considered in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET).

B. Static ad-hoc networks

In static Ad-Hoc networks the geographic location of the nodes or the stations are fixed. There is no flexibility in the nodes of the networks, that's why they are known as static Ad-Hoc networks.

2. Mobile ad-hoc networks

Mobile Ad-Hoc network is an independent system, where nodes/stations are connected with each other through wireless links. There are no limitations on the nodes to join or leave the network, therefore the nodes join or leave spontaneously.

Mobile Ad-Hoc network topology is dynamic that can change swiftly because the nodes move freely and can organize themselves arbitrarily. This property of the nodes makes the mobile Ad-Hoc networks random from the point of view of scalability and topology. Mobile Ad-Hoc network topology is active that can change rapidly because the nodes move freely and can organize themselves randomly. This possessions of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology.

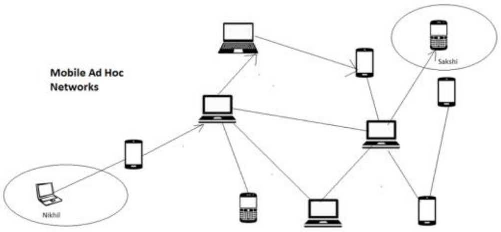

Fig. 1. Flow of Data Packets in MANET

Characteristics of MANET

When a node wants to communicate with another node, the destination node must lies within the radio zone of the source node that wants to initiate the communication. The intermediate nodes within the network supports in routing the packets for the source node to the destination node. These networks are fully self-structured, having the ability to work anywhere without any infrastructure. Nodes are autonomous and play the character of router and host at the same time. MANET is self-governing, where there is no centralized control and the communication is carried out with blind mutual belief between the nodes on each other. The network can be set up anywhere without any geographical limitations. One of the limitations of the MANET is the limited energy resources of the nodes.

Types of Mobile Ad-Hoc Network

- Vehicular Ad-Hoc Networks (VANET's)
- Intelligent Vehicular Ad-Hoc Networks (In VANET's)
- Internet Based Mobile Ad-Hoc Networks (iMANET's)
- Vehicular Ad-Hoc Networks (VANET's)

It is a type of Mobile Ad-Hoc network where vehicles are fortified with wireless and form a network without help of any infrastructure. The equipment is located inside vehicles as well as on the road for providing access to other vehicles in order to establish a network and interconnect to communicate.

- *Intelligent Vehicular Ad-Hoc Networks (In-VANET's):* Vehicles that form Mobile Ad-Hoc Network for communication via WiMAX IEEE 802.16 and WiFi 802.11. The main objective of designing In-VANET's is to ignore vehicle collision so as to retain passengers as safe as possible. This also help drivers to retain protected distance among the vehicles as well as contribution them at how much speed other vehicles are approaching. In-VANET's applications are also active for military purposes to communicate with each other.
- *Internet Based Mobile Ad-Hoc Networks (i-MANET's):* These are used for connecting up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms does not apply [2].

Applications of MANET

The properties of MANET make it so much positive that would bring so many aids. There are so many research areas in MANET which is under studies now. The most significant area is vehicle to vehicle communication where the vehicle would communicate with each other, keeping a secure distance between them as well as collision notices to the drivers. MANET can be used for automated battlefield and war games. One of the most important area where MANETs are applied is emergency services such as disaster recovery and relief activities, where out-dated wired network is already destroyed. There are so many other application areas for instance entertainment, education and commercial where MANETs are playing their vital character for connecting people.

Short comings of Mobile Ad-Hoc Networks

Certain drawbacks of MANETs are as follows.

- Limited Resources.
- Scalability issues.
- No dominant check on the network.
- Dynamic topology, where it is hard to find out malevolent nodes.

MANET's Routing Protocols

Mobile Ad-Hoc Network is the swiftly rising technology from the past 20 years. The advancement in their reputation is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs fashioned a new set of demands to be implemented and to provide effective improved end-to-end communication. MANETs mechanism on TCP/IP structure to provide the means of communication between communicating work stations. Work stations are portable and they have limited resources, therefore the traditional TCP/IP model needs to be overhauled or modified, in order to recompense the MANETs mobility to provide efficient functionality. Therefore, the crucial research area for the researchers is routing in any network. Routing protocols in MANETs are a challenging and striking tasks, researchers are giving marvelous amount of attention to this key area.

Classification of MANETs Routing Protocols

Routing protocols in MANETs are categorized into three different categories according to their functionality

A. Reactive protocols
B. Proactive protocols
C. Hybrid protocols

The order of these protocols is shown below in the figure.

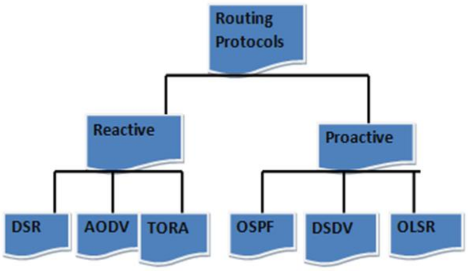

Fig. 2. Manet routing protocols

A. *Reactive protocols*

Reactive protocols also recognized as on demand driven reactive protocols. The fact they are identified as reactive protocols is, they do not pledge route discovery by themselves, till they are wished, when a source node request to discover a route. These protocols setup routes when required [3], [4]. When a node desires to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Typically, reactive protocols.

- Don't find route until needed
- When tries to discover the destination "on demand", it uses flooding technique to broadcast the request.
- Do not consume bandwidth for sending information.
- As soon as the node start transmitting the data to the destination node, they consume bandwidth only.

Ad-Hoc On Demand Distance Vector Protocol (AODV): AODV is defined in RFC 3561 [5]. It's reactive protocol, when a node needs to start transmission with another node in the network to which it has no route; AODV will deliver topology information for the node. AODV use control messages to find a route to the destination node in the network. Since there are three types of control messages in AODV which are conversed bellow.

- *Route Request Message (RREQ)* Source node that desires to communicate with another node in the network conveys RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to aware (TTL) value in every RREQ message, the value of TTL describes the number of hops the RREQ should be communicated.
- *Route Reply Message (RREP)* A node having a demanded uniqueness or any intermediate node that has a route to the demanded node generates a route reply RREP message back to the instigator node.
- *Route Error Message (RERR)* Each node in the network keeps monitoring the link status to its neighbour's nodes during active routes. As soon as the node notices a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

- *Route Discovery Mechanism in AODV*: When a node “A” wants to pledge broadcast with another node “G” as shown in the Fig. 2.4, it will produce a route request message (RREQ). This message is broadcasted through a limited flooding to other nodes. This control message is promoted to the neighbours, and those node advancing the control message to their neighbours' nodes. This procedure of finding destination node goes on until it finds a node that has a new enough route to the destination or destination node is situated itself. As soon as the destination node is located or an intermediate node with enough fresh routes is located, they start generating control message route reply message (RREP) towards the source node. When RREP ranges the source node, a route is established between the source node “A” and destination node “G”. Once the route is recognized among “A” and “G”, node “A” and “G” can communicate with each other. Fig3. signifies the exchange of control messages between source node and destination node.

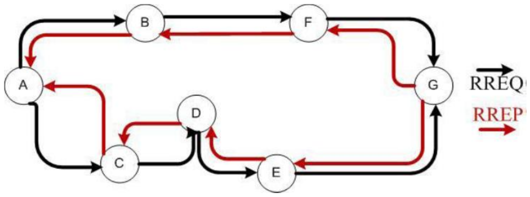

Fig. 3. AODV route discovery

Once there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or from the neighbours nodes, the RERR message is directed towards the source node. When RREQ message is broadcasted for finding the destination node i.e. from the node “A” to the neighbours nodes, at node “E” the link is broken between “E” and “G”, so a route error RERR message is generated at node “E” and transmitted to the source node informing the source node a route fault, where “A” is source node and “G” is the destination node. The structure is shown in the Fig. below.

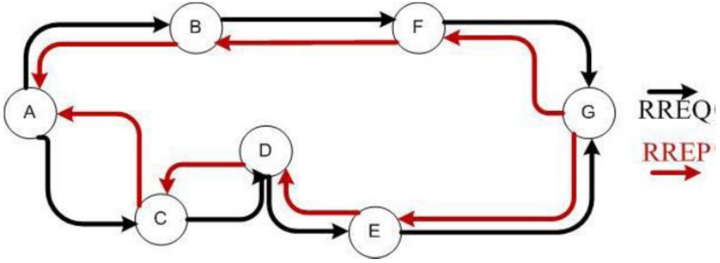

Fig. 4. Route error message in AODV

B. *Dynamic Source Routing Protocol*

Dynamic source routing protocol abbreviated by means of DSR is also a reactive protocol. DSR use to update its route caches by finding new routes. It keep informed its cache with new route discovered or when there exist a direct route between source and destination node. When a node wants to transmit data, it describes a route for the transmission and then starts transmitting data through the defined route. There are two procedures for route discovery and maintenance which are described below.

C. *Route discovery process*

Once a source node wants to start data transmission with another node in the network, it checks its routing cache. Once there is no route available to the destination in its cache or a route is expired, it broadcast RREQ. When the destination is located or any middle node that has fresh enough route to the destination node, RREP is generated [15]. Once the source node accepts the RREP it updates its caches and the traffic is routed through the route.

D. *Route maintenance process*

When the transmission of data started, it is the duty of the node that is transmitting data to confirm the next hop acknowledged the data along with source route. The node generates a route error message, if it does not receive any authorization to the originator node. The originator node again performs new route discovery process.

E. *Proactive protocols*

Proactive routing protocols works as compared to reactive routing protocols. These protocols continuously preserve the updated topology of the network. Every node in the network recognizes about the other node in advance, in other words the whole network is acknowledged to all the nodes making that network. All the routing information is usually reserved in tables [6]. Each time there is a change in the network topology, these tables are updated according to the change. The nodes interchange topology information with each other; they can have route information any time when they required [6].

- *Optimized Link State Routing Protocol (OLSR):* The Optimized Link State Routing (OLSR) protocol is termed in RFC3626 [7]. OLSR is proactive routing protocol that is also called as table driven protocol by the detail that it updates its routing tables. OLSR has also three types of control messages which are detailed bellow.

- *Hello:* This control message is communicated for sensing the neighbour and for Multi Point Distribution Relays (MPR) calculations.
- *Topology Control (TC):* These are connection state signalling that is achieved by OLSR. MPRs are used to enhance theses messaging.
- *Multiple Interface Declaration (MID):* MID messages comprehends the list of all IP addresses used through any node in the network. All the nodes running OLSR spread these messages on more than one interface.
- *OLSR Working Multi Point Relaying (MPR):* OLSR disperses the network topology information by flooding the packets throughout the network. The flooding is done in such technique that each node that received the packets retransmits the received packets. These packets contain a sequence number so as to evade loops. The receiver nodes record this sequence number making sure that the packet is retransmitted after. The simple concept of MPR is to reduce the duplication or loops of retransmissions of the packets.

Individual MPR nodes broadcast route packets. The nodes inside the network keep a list of MPR nodes. MPR nodes are nominated with in the vicinity of the source node. The assortment of MPR is based on HELLO message sent between the neighbour nodes. The selection of MPR is such that, a path exist to each of its 2 hop neighbours via MPR node. Routes are established, once it is done the source node that wants to initiate communication can start sending data.

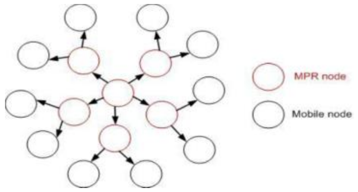

Fig. 5. Flooding packets using MPR

The whole process can be understand through looking into the Fig6. below. The nodes shown in the figure are neighbours. “A” transmits a HELLO message to the neighbour node “B”. As soon as node B receives this message, the link is distorted. The similar is the case when B send HELLO message to A. When there is two way communications between both of the nodes we call the link as symmetric link. HELLO message has all the information about the neighbours. MPR node transmits topology control (TC) message, along through link status information at a predetermined TC interval.

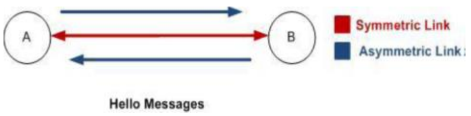

Fig. 6. Hello message exchange

F. *Hybrid protocols*

It exploits the strengths of both reactive and proactive protocols, and combine them together to get better results. The network is distributed into zones, and use different protocols in two different zones i.e. one protocol is used within zone, and the other protocol is used among them. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. ZRP practices proactive mechanism for route establishment within the nodes neighborhood, and for communication between the neighborhood it takes the benefit of reactive protocols. These local neighborhoods are known as zones, and the protocol is named for the same motive as zone routing protocol. Each zone can have different size and each node may be within numerous overlapping zones. The size of zone is given by radius of length P, where P is number of hops to the perimeter of the zone [8].

3. Basic security concepts

To understand security issues it is vital to know the attribute or basic concepts on which a network security is judged. These attribute associated to security are the desired objectives of Cryptographic mechanism. Cryptography can be defined in several ways, it is defined as Cryptography terminologies, key concepts, types are summarized. Following are the attributes or security services on which the security of the networks is evaluated.

Non-Repudiation

Non-repudiation ensures that an entity in a dispute cannot falsely deny its action or reject the validity of the contact. For example, during a transmission non repudiation service prevents the sender from denying sending a message which he sent earlier, or a receiver cannot claim to have received the message falsely.

A. *Availability*

Availability is another very important attribute, referring to ensuring that system resources and services are available for use by authorized users of the system. It is imperative to make sure all the network services remain available for its users given that an intruder can attempt to deny services in the network through denial of service attacks, and that a network without desired services is as bad as having no network. MANETs are especially vulnerable to different types of denial of service attacks due to their inherent characteristics. To achieve these security attributes or services in fixed networks several cryptographic mechanism are proposed using trusted third party (TIP). TIP is an entity in the network trusted by all users in the system for example Certificate Authority (CA) or Key Distribution Centers (KDC). They are mainly used to provide key management services such as creating, distributing, updating and revoking keying material for both symmetric (involve the use of single key) and asymmetric key (involve the use of two keys) systems. Security mechanisms developed using TIP are not directly implantable in MANETs because they lack a trusted infrastructure and absence of centralized control. However, some proposals based on modified approaches of key management for MANETs can be found in the literature for example approaches in [15] suggest use of identity-based public key management systems for MANETS. In [12] authors use identity based signcryption (combines the functionality of digital signature and symmetric key encryption) and threshold secret sharing (allows sharing of secret information among group of entities) to provide various security services in MANETs. Recently the concept of threshold cryptography i.e. protecting secret information by distributing it among a set of nodes or entities has proven to be an effective scheme for key management in MANETs.

MANETs are vulnerable in their functionality: intruders can compromise the network operations by either attacking at physical, MAC or network layer. MANETs are susceptible to eavesdropping, active interfering and frequency jamming attacks because of wireless links. Frequency jamming is a common physical layer attack on MANETs. Researchers have looked at MAC layer misbehavior in MANETs in a presence of compromised or selfish nodes. However, this thesis focuses on network layer vulnerabilities. Network layer especially routing protocols for MANETs are more vulnerable in their routing operations because of the following:

- Use of cooperative routing algorithm: Because each node in MANETs has to act as a router i.e. forward packets for other nodes, participate in route discovery and route maintenance procedures. Nodes with harmful intention can cause severe disruption exploiting this property of routing protocols.
- Rely on exhaustible batteries: most nodes in ad hoc network rely on exhaustible batteries; hence, their processing capabilities are limited. Intruder can exploit this property by forcing a node to process unnecessary packets in an attempt to exhaust their batteries within the rules of routing protocols. Any service offered by the victim nodes can be denied through this intrusive activity.
- Limited computational ability: nodes in such networks generally have limited computational capabilities having low processing frequencies and smaller memory size which also adds to the existing vulnerabilities.
- Easy theft of nodes: location of nodes in such networks is not permanent as they are allowed to move arbitrarily which makes them vulnerable to being physically captured. From a routing perspective, this means that a node can be compromised easily.
- Transient nature of services: because the topology of the network is dynamic as nodes move frequently, therefore any specific service provided by nodes is transient, this adds to the uncertainty in these networks. This makes it difficult to distinguish between acceptable or malicious behavior. cryptography key management scheme for MAENTs and their simulation results show the advantages and suitability of the idea in manets. vulnerability of manet routing protocols

Vulnerability, threat, and attacks are the terms used often in computer network security. We begin this subsection with defining these terms:

B. *Confidentiality*

Confidentiality is also known as secrecy or privacy. Confidentiality is the process of concealing information on the network, i.e. it ensures that information content cannot be revealed by unauthorized entities that are normally known as internal or external attacker or intruders. It can also be described as a security service that ensures only intended receivers could interpret the information transmitted on the network. Confidentiality is very important security service in MANETs considering wireless links in such networks are easily susceptible to eavesdropping. A security protocol for reliable data delivery is proposed to improve the confidentiality service in MANETs. They propose to split the encrypted message into separate shares and these shares should be transmitted through independent multiple paths so making it difficult for the attacker because now he has to eavesdrop all pieces of message and has to decrypt all of them successfully to understand the message. Seng et.al propose secure routing mechanism which provide data confidentiality using shared secret key.

C. *Integrity*

Integrity ensures that data packets are unaltered during transition from source to destination i.e. unauthorized user could not manipulate data through insertion, substitution, deletion or forging data. To maintain integrity, data is usually signed by the source and the receiver verifies the digital signature to be assured of integrity of the data. Such mechanism will incur extra overhead for nodes in MANETs with limited processing abilities and also because nodes relay data for other nodes, so integrity cheeks needs to carried out at every hop. Gavidia et. al. realize the cost of guaranteeing data integrity mechanism for MANETs and proposed a solution based on probabilistic integrity checks and traffic analysis. They prove that probabilistic verification is an effective method to restrict the amount of corrupted content and their spread i.e. ensures data integrity in MANETs.

D. *Authentication*

Authentication is a process that allows node to verify the identity of the other nodes with it is communicating. Two types of authentication are entity and data authentication [36]. Entity authentication ensures that other communicating parties are who they claim to be and data authentication is focused on providing a guarantee as to the origin of the data.

4. Conclusion

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our research work we proposed a feasible solution for the AODV protocol. The main concern of this work to show the performance of AODV under normal surroundings, under Packet Dropping attack and performance after elimination of Packet Dropping attack in term of delay, throughput and traffic received. The network performance with Packet Dropping attack in term of throughput decreases around bits per second. By our proposed approach, we have recovered around in throughput. The network performance with Packet Dropping attack in term of end to end delay increases around % and with our proposed approach, we have recovered around % in delay. Concept has shown improved results after elimination of the gray-hole attack in the simulation. Elimination of malicious nodes takes place on Network layer by broadcasting the information of malicious nodes. Overall, elimination of Packet Dropping attack has been done so that ad-hoc communication can be normalized as normal communication. It will be very useful in saving a lot of resources for mobile ad-hoc communication as we have used unicasting process instead of broadcasting which saves resources as malicious nodes are only detected through partial multicasting process. In nutshell, elimination of Packet Dropping attack has been done so that ad-hoc communication can be normalized as normal communication.

References

[1] Abedi, O.; Berangi, R.; Azgomi, M.A., "Improving Route Stability and Overhead on AODV Routing Protocol and Make it Usable for MANET," in Proceedings of 29th IEEE International Conference on Mobile Ad Hoc Networks, June 2009, pp.464,467.

[2] Robert E. Chandler, Robert Herman, Elliott W. Montroll, “Traffic Dynamics.”

[3] Balon N., and J. Guo, “Increasing Broadcast Reliability in Mobile Ad Hoc Networks(MANET),” in Proceeding of the 3rd ACM International Workshop on Mobile Ad Hoc Networks MANET, NY, USA, 2006, pp. 104-105.

[4] Bernsen, J. Manivannan, “Routing Protocols for Mobile Ad Hoc Networks That Ensure Quality of Service” In Proceedings of the fourth international conference on Wireless and Mobile Communications, Aug. 2008, pp.1-6.

[5] Blum J., Eskandarian A., and HoffmanL. "Performance Characteristics of Inter- Vehicle Ad Hoc Networks". In Proceedings of IEEE 6th International Conference on Intelligent Transportation Systems, Shanghai, China,2004, Pp. 115-119.

[6] Brian D. Noble, Jungkeun Yoon, Mingyan Liu, Minkyong Kim, “Building realistic mobility models in MANET”, in Proceeding of the ACM International Conference On Mobile Systems, Applications and Services, pp. 177-190, 2006.

[7] David B. Johnson, David A. Maltz, and Josh Broch, “The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, in Ad Hoc Networking, Editor: Charles E. Perkins, Addison-Wesley, Chapter 5, 2001, pp. 139-172.

[8] Deepali A. Lokare, A. M Kanthe, Dina Simunic, “Cooperative Packet Dropping Attack Discovery and Elimination using Credit based Technique in Manet,” in Proceeding of International Journal of Computer Applications, Vol. 88, February,2014, pp. 13-22.

[9] Dirk Reichardt, Maurizio Miglietta, and Wolfgang Schulz “CARTALK 2000 Safe and Comfortable Driving Based Inter-Vehicle-Communication in MANET”, in proceedings of IEEE Intelligent Vehicle Symposium, June 2002, pp. 145-147.

[10] Dharmendra Mishra, Deepak, Sukheja,Sunil, Patel,” A Review on Packet DroppingAttack in Wireless Sensor Network”, International Journal of Computer Applications, Volume 122, No. 2, July 2015, pp. 0975 – 8887.

[11] Fan Li and Yu Wang; “Survey of Routing in Mobile Ad Hoc Networks”, in Proceedings of IEEE Mobile Technology Magazine, Volume 2, Issue 2, June 2007; pp. 12-22.

[12] Garima Neekhra, Sharda Patel, “Effect of Packet Dropping Attack with IDS Techniques for AODV Routing Protocol using Network Simulator”, in Proceeding of International Journal of Advanced Research in Computer Engineering & Technology, Vol. 3, December 2014, pp. 4184-4190.

[13] Goel A., Ramakrishnan K. G., D. Kataria, and D. Logothetis, “Efficient computation of delay-sensitive routes from one source to all destinations,” in Proceedings of IEEE Conference on Computer Communications, 2001, pp. 854-858.

[14] Heissenbüttel M., T. Braun, M. Wälchli, and T. Bernoulli, “Optimized stateless broadcasting in wireless multi-hop networks,” in proceeding of 4th IEEE international conference on Infocom Barcelona, 2006, pp. 234-250.

[15] H.P. Glathe, L. Karlsson, G.P. Brusaglino, L. Calandrino, “The PROMETHEUS Programme– Objectives, Concepts and Technology for Future Road Traffic”, in Proceedings of 12th conference of networking, May 1990, pp. 477-484.

[16] H. Safa, H. Artail, and R. Shibli, “An interoperability model for supporting reliability and power-efficient routing in mobile ad hoc network,” International Journal of Ad Hoc and Ubiquitous Computing, Vol. 4, 2009, pp. 74-83.