A Review on Security Issues and Gaps in the Literature in Mobile Adhoc Networks

[1] B. Aruna kumari, [2] K. Rohini
[1, 2] Assistant Professor
[1, 2] Department of CSE
[1, 2] AITS-Rajampet, A.P, India

Abstract: Mobile Ad Hoc Network (MANET) is an infrastructure independent network with wireless mobile nodes. These networks have several advantages compared to traditional wireless networks includes ease of deployment, speed of deployment and decreased dependency on a fixed infrastructure. MANET is a kind of Ad Hoc networks with special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications. These characteristics of MANET made it popular, especially in military and disaster management applications. As communication media is wireless, each node will receive packets in its wireless range, either it has been packets destination or not. Due to these characteristics, each node can easily gain access to other nodes packets or inject fault packets to the network. There have been many studies done in this area to improve the quality and efficiency of the routing protocols and security measures in MANETs. Therefore, securing MANET against malicious behaviors and nodes, became one of the most important challenge in MANET. The main contribution of this paper is that to give an overview of MANET and the routing protocols, major challenges along with the gaps in the literature. Based upon the characteristics we defined 3 important security issues. Furthermore we presented various attacks occurred in MANET along with defeating approaches and the objective measures that are used for the qualitative analysis.

Index Terms **– Wireless Networks, MANET, Security Issues, Performance parameters.**

I. INTRODUCTION

In the modern era, the greater expansion of mobile computing gadgets such as laptops, Personnel Digital Assistants (PDA's), handheld digital devices and so on are taken into consideration and has incited a revolutionary amendment to the computing world. In the past few years, wireless technology is enhancing in its progress and popularity of wireless devices and networks as well. MANET is an independent network constitutes of wireless mobile nodes. It is said as one of the Ad Hoc networks kinds and has special features such as open network boundary, dynamic topology, distributed network, speed and immediate implementation and hop-by-hop communications. Those MANET features made it popular, particularly in military and disaster management. Due to special features, expansion of MANET faced many challenges. Peer to Peer applications, internet integration, network topology and energy maintaining are some of the key challenges in MANET is our past work. There are many merits with MANET's over traditional wireless networks. These include deployment easy and speed, and decreased dependency on a constant infrastructure. Many studies on this domain is to enhance the quality and efficiency of MANET's routing protocols. However unique features of MANET topology like peer-to-peer architecture, dynamic network topology, shared wireless medium and restricted resources (battery, memory and computation power) pose more non-trivial challenges to security design. Based on these challenges and features need MANET's to provide huge protection and required network performance [1].

All nodes in MANET can freely join and leave the network and it is called as open network boundary. All intermediate nodes between a source and destination take part in routing, also called as hop by hop communication. Since it is a wireless communication media, every node will receive packets inside its range, either it has been packets destination or not. MANET's with no established infrastructure setup available for routing packets from node to node in a network and they dependent on intermediate nodes. MANET nodes have a problem of different attacks like eavesdropping attack, battery draining attack etc. The common target of such attacks is data bandwidth, power of battery, routing protocols. This paper depicts an overview of secure routing protocols by presenting their key functions, security against multiple attacks, merits and demerits.
The structure of Simple MANET is shown in Figure 1.

By these features, every node will get ease of access to other nodes packets or give false packets to network. Hence, securing MANET against malicious attacks and nodes become one of the vital MANET's challenges. The rise in MANET's security challenges due to its self-configuration and self-maintenance capabilities [2]. In this paper, we proposed a view of issues in MANET security elaborately. On the basis of MANET's special features, we define three security parameters for MANET. Besides we divided MANET security into two different aspects. A comprehensive analysis in such MANET aspects and defeating approaches are presented and these defeating approaches against the attacks have evaluated in some key metrics. Thereafter, the future scope of our work also been presented. In this paper, we also test some of the routing protocols and the features of these over MANET [3].

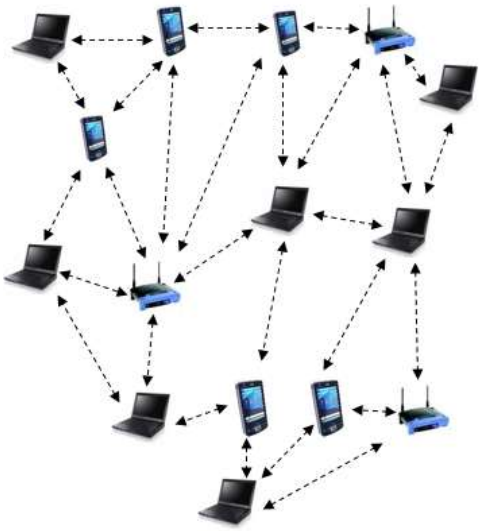

Figure 1: Mobile Adhoc Network

The rest of the paper is organized as follows. Section 2 discuss about the related theory about wireless networks and its applications along with routing mechanisms that are available in MANET. Section 3 covers the challenges in security and various attacks that occurred in MANET. Section 4 discuss about the objective parameters and Section 5 concludes the paper.

II. RELATED THEORY

2.1 Wireless Networks

Apart from connection flexibility among various users at heterogeneous areas they also help in the network expansion to any building or area with the absence of physical-wired connection. Those connections exist in two types; Infrastructure networks and Ad-Hoc networks as shown in below Figure 2. Access Point (AP), in infrastructure wireless networks, represents a central controller for every device. With the access point the network can be combined by any node. To make the route ready when there is a need, this access point allows linking among the Basic Set Services (BSS's). Also there is a limitation in using a network organization is that there is a big overhead of preserving the routing tables [4]. Structure less or Ad-hoc networks has deficiency of firm topology or a central controlling point, so transfer and receive of data packets is very complex over structured networks. Wireless networks are classified into single hop and multi hop along with infrastructure and ad hoc based. In single hop networks base station(BS) and wireless devices communicates directly with BS by exchanging data between device to device and to other and so on.

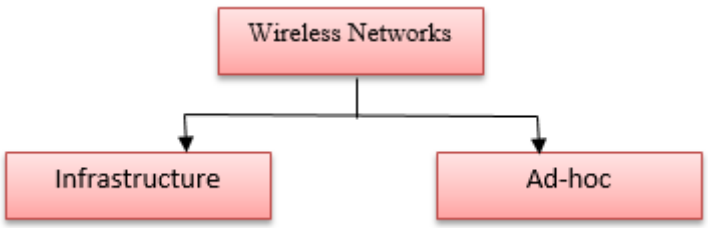

Figure 2: Types of Wireless Networks

2.2 Applications

MANETs are widely used in the following fields such as Military, Education, Business, and Sensor Networks etc. We have briefly discussed few of these applications [5].

Military: Ad-Hoc networking allows army to get advantage of conventional network expertise to preserve any info network among vehicles, armed forces, and headquarters of information.

PAN and Bluetooth: A PAN is local and small range network in which the devices are specifically belongs to particular individual. Bluetooth, a restricted-range MANET made transfer simpler among many portable devices such as laptop and mobile phone.

Business Sector: Ad-hoc network can be used for rescuing and emergency processes for adversity assistance struggles, for example during the time of floods or earthquakes. Immediate saving procedures must be taken where damaged and non-existing transmissions structure and immediate making of a transmission network is required.

Sensor Networks: Home appliances can be managed with MANET's for both nearly and distantly. Objects like creatures are tracked. Activities regarding Weather sensing

Backup Services: liberation operations, tragedy recovery, diagnosis or status or record handing in hospitals, stationary infrastructure replacement.

Educational sector: providing communications facilities for computer-generated conference rooms or classrooms or laboratories.

A MANET network has self-configuration with wireless links connections. More Ad Hoc networks are independent on fixed underlying infrastructure like base stations or access points. Every device in MANET has no restrictions and can move in any way independently and will so that its links changes frequently to other devices [8]. Every node must forward traffic for making consistent network. Hence, every node of MANET is considered as a router. It is broadly used as wireless network for upcoming generation, which is a type of peer-to-peer network and is comprises of wireless nodes group that supports with each other to exchange information with no infrastructure or central control node. The MANET routing protocol design faces many challenges, since the MANET network has features like restricted bandwidth and node energy, fast change in network topology, asymmetric and unstable link and distributed and autonomous network's architecture. Most of classical MANET routing protocols have been introduced, such as Optimized Link State Routing (OLSR) protocol, Ad-hoc On-demand Distance vector (AODV) routing protocol [2], Dynamic Source Routing (DSR) protocol, Ad-hoc On-demand Multipath Distance Vector routing(AOMDV) [9].

Some MANET's are restricted to small or local areas of wireless devices (cluster of laptop computers), whereas the rest might be internet connected. For instance, a VANET (Vehicular Ad Hoc network) is a kind of MANET which permits vehicles to interact with roadside equipment. In such cases the vehicles may not have internet connection directly. The wireless roadside equipment connects to internet and allows data from the vehicles could be spent through the internet. These vehicles data can be used in evaluating traffic rules otherwise keep track of trucking fleets. Due to MANET's dynamic nature, they are insecure, so it is vital to be alert what data is sent over the MANET.

2.3.1 Routing Protocols

The Routing Protocols in MANET are majorly classified into three categories such as Proactive, Reactive and Hybrid Protocols.

1. **Proactive Protocols**

Proactive Protocols or Table-Driven Protocols roots are always maintained between the nodes in the network also when the routes are not in use. Every node upgrades to other node inside the network so that all the network nodes eventually understands the network's state. The plus of this method is that there is less or zero time delay when the node-to-new node communication begins. The problem with this method is that in huge networks, within the network the maintenance of route's message overhead will gradually reduce the capacity of that network. Pro-active protocols are the Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) and so on [8].

2. **Reactive Protocols**

Reactive Protocols otherwise On-Demand Protocols performs search on routes among nodes for communication purpose. Whenever the node wants to communicate with other node for which it do not have any information in its route table a process of route discovery is called. Once the discovery of route is done it requires route maintenance process. Whichever the roots are inactive are removed at continuous intervals. The proficiency of reactive protocol over proactive routing protocols is its more scalability. The drawback with such methods is that, in the way to detect a new root it requires additional time delay. Ad-Hoc on Demand Distance Vector (AODV) is reactive protocol [6].

3. **Hybrid Routing Protocols**

These protocols work with the integration of reactive and proactive methods. Based on the reactive method, Proactive methods can make a routing between members of a zone and between different zones. Zone Routing Protocol (ZRP) is Hybrid Routing Protocols.

2.3.2 Secure routing protocols

There exist various routing protocols. Among them we discussed only three protocols that are widely used:

ARAN

The ARAN is an on demand secure routing protocol that finds against the hazardous activities by the third parties in an ad-hoc network. APAN provides security services like authentication, non-repudiation and message integrity as a minimum security policy. ARAN needs the use of trusted certificate server (T) before connecting with ad-hoc network. In ARAN, every node must request a certificate from the trusted certificate server T. The certificate gives the node's IP address, time stamp when T was made, its public key, the certificate's expire time. Here all the nodes will have new certificates of trusted certificate server and public key of certificate server T must be known**.**

SEAD

SEAD is a proactive secure routing protocol which is Destination Sequenced Distance Vector protocol (DSDV) based. In this routing protocol every node exchanges routing information with the rest of other nodes and constitute a route between each and every nodes in the network. With the use of hash chain technique SEAD performs authentication on ordered number field and metric field of a routing table. In this protocol, the sender will be authenticated by destination node and makes sure that the received information is from exact node. In order to prevent the attacks from third parties every routing message from the source should be authenticated.

SRP

The Secure Routing Protocol (SRP) was compatible protocol with many of reactive routing protocols. SRP was not vulnerable to attacks that disrupt the route discovery process. SRP permits the route discovery's source to ignore unwanted replies. SRP is dependent on Security Association (SA) between Source(S) and Destination (D). SA can be made with the use of hybrid key distribution on the basis of S and D's public keys. S and D may use a secret symmetric key along with the use of public keys of one another.

III. BROAD CHALLENGES

The general issues in MANET environment will be covered in this section. The issues related to the security point of view for example security parameters and various attacks that occurred in MANET are covered in the subsequent section.

(1). There is a confined remote transmission range; as a penalty it can give substantially slighter than what a bound network can give. This includes routing mechanisms of wireless networks must be utilize data transmission in a perfect way. Especially in MANETs on account of customary varieties in topology, saving the topological information for each hub incorporates more controller overhead which brings about extra data transfer capacity exhaustion [10]

(2) Time-varying wireless link characteristics: Wireless channel is liable to a range of broadcast disorders such as path harm, declining, intervention and obstruction. These features resist the series, data rate, and consistency of these cordless transmissions. The range of which these features disturb the transmission that rest on atmospheric situations and flexibility of receiver and transmitter. Even two dissimilar key restraints, Nyquist's and Shannon's theorems that rule over capability to communicate the information at diverse data degrees can be measured [11].

(3)Broadcast nature of the wireless medium: The broadcast nature of the radio channel, such as transmissions prepared by a device is established by all devices that are in its straight transmission covering area. When a device receives data, no other device in its neighborhood, apart from the sender, must transfer. A device can acquire access to the mutual medium when its communications cannot disturb any constant session. Meanwhile several devices may resist for medium contemporarily, chance of data-packet crashes is very tall in wireless networks. [12].

(4) Mobility-induced route changes: The system topography in ad hoc wireless network is extremely active because of node movement; as a result, a constant meeting undergoes numerous pathway breakages. Such position often results in regular path alterations. So flexibility administration is massive investigation theme in ad hoc networks. [13].

3.1 Security Parameters

Because of MANET's special characteristics, there are some important metrics in MANET security that are important in all security approaches; we call them "Security Parameters". Being unaware of these parameters may cause a security approach useless in MANET. Figure 3 shows the relation between security parameters and security challenges. Each security approach must be aware of security parameters as shown in Figure 3. All mechanisms proposed for security aspects, must be aware of these parameters and don't disregard them, otherwise they may be useless in MANET. Security parameters in MANET are as follows:

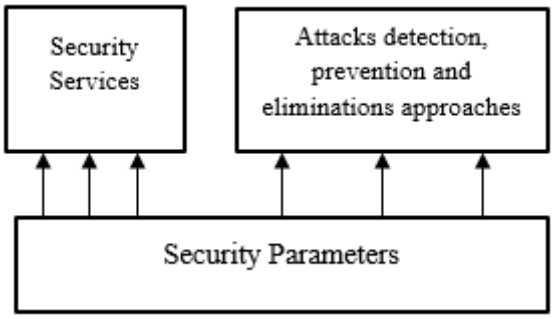

Figure 3: Security Parameters

Node mobility causes frequent changes in network topology. The wireless nature of communication and lack of any security infrastructure increases several security problems discussed in further sections. There are mainly five MANET security parameters that are Confidentiality, Availability, Authentication, Non repudiation and Integrity and will be discussed in section 3.2.1.

3.2 Challenges over these parameters

There are several security challenges in MANET and most of them were inherited from ad hoc networks [15, 16]. Two main important aspects in security are Security services and Attacks.

3.2.1 Security Services

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network.

Availability: Availability denotes that every user who is authorized should access all the data and services exists in the network. This challenge arises since MANET's dynamic topology and open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time. Authors in [17] provided a solution to this

problem by using trust based clustered approach. In their method it is ABTMC (Availability Based Trust Model of Clusters), by using availability based trust model, hostile nodes are identified quickly and should be isolated from the network in a period of time, therefore availability of MANET will be guaranteed.

Authentication: The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever in absence of central control unit, key distribution and key management are challengeable. In [18] the authors presented a new way based on trust model and clustering to public the certificate keys. In this case, the network is divided into some clusters and in this clusters public key distribution will be safe by mechanisms provided in the paper..

Data confidentially: According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible. Authors in [19] proposed a new scheme for reliable data delivery to enhance the data confidentially. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination.

Integrity: According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them. Authors in [20] presented a mechanism to modify the DSR routing protocol and gain to data integrity by securing the discovering phase of routing protocol.

Non-Repudiation: By using this service, no source or destination can repudiate their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent. Authors in [21] presented a new approach that is based on grouping and limiting hops in broadcast packets. All group members have a private key to ensure that another node couldn't create packets with its properties. But creating groups in MANET is challengeable.

3.2.2 Other Important Parameters

Along with few of the other parameters also considered. **Network Overhead** is parameter refers to number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily lead to congestion or collision in MANET. Packet lost is one the results of congestion and collision. **Processing Time** is another parameter which is a time to detect misbehaviors and eliminate malicious nodes. Due to MANET's dynamic topology it's strongly possible that routes between two different nodes break because of mobility. Therefore, security approaches must have as low as possible processing time in order to increase MANET flexibility and avoid rerouting process. The last important parameter is **Energy Consumption**, the nodes in MANET are limited in the view of Energy. Therefore, optimizing energy consumption is highly challengeable in MANET. High energy consumption reduces nodes and network's lifetime. All the security protocols must be aware of these three important parameters. In some situations a trade-off between these parameters is provided in order to perform a satisfaction level in all of them. Security protocols that are not giving the best result in these parameters they are not considered as efficient and considered as useless.

3.2.3 Attacks

MANETs are not secure in some kinds of attacks. Attacks can cause drop of network traffic and modification of control message fields or forwarding routing message. Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows:

Worm Hole Attack: In this kind of attack, the node records the packets at one location of the networks and tunnels them in to another location [22].Fault routing information could disorder routes in network [23]. The authors in the paper [24] presented a secure way against to this attack by encrypting and using location of the node. But as mentioned before, key distribution is a challenge in MANET. In Figure 4, Source node A wants to communicate with node M. Node A will send RREQ packet to immediate neighbors B and I and Malicious node C. C will tunnel the packet directly to other malicious node F, thereby, shortening the path. Thus, M will accept the shortest path through F and ignore other paths.

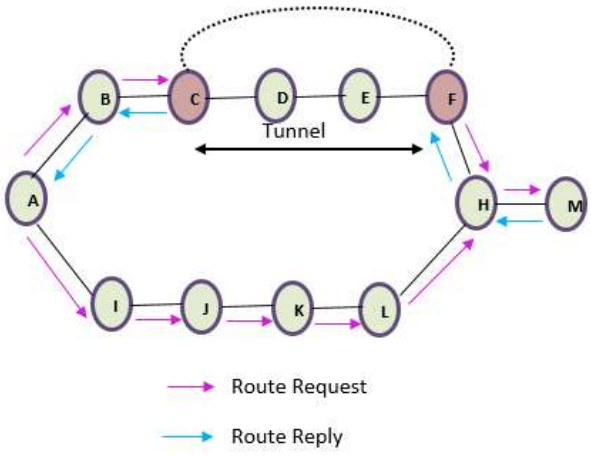

Figure 4: Warm-Hole Attack

Black Hole Attack: Attacker first sends fake route related information to the source node and state that it has the shortest route to the destination and after establishment of the route, attacker receives the data packet from the source node then drops or misuses these packets and it is shown in Figure 5.

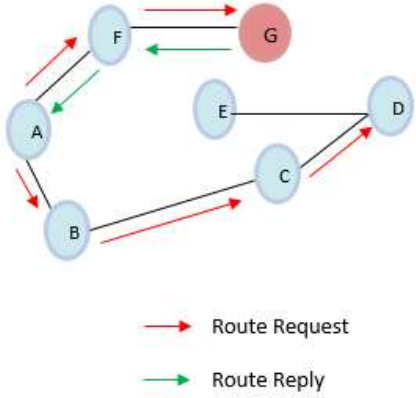

Figure 5: Black Hole Attack

Gray-hole attack: It is also called as routing misbehavior attack, in this attack the messages ignored in two phases in the first phase a legitimate route to destination is advertise by node itself. In second phase, with a certain probability nodes drops intercepted packets and it is shown in Figure 6.

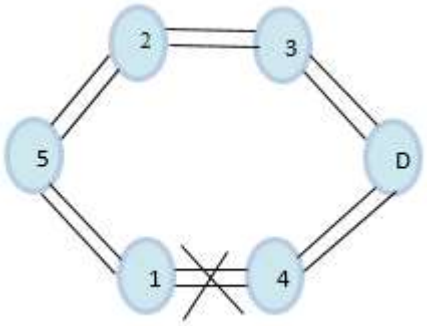

Figure 6: Gray-Hole Attack

Byzantine attack: In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop [25, 26]. One way to protect network against this attack is using authentication. Authors in [27] presented a mechanism to defeat against this attack using RSA authentication.

Denial of service: In this attack, malicious node prevents other authorized nodes to access network data or services [28]. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. In addition, packet delay and congestion increases.

Man-in-the-middle attack: In this attack, malicious node puts itself between source and destination. Then, captures all packets and drops or modifies them [29]. Hop by hop communications are made MANET vulnerable against this attack. Authentication and cryptography are the most effective ways to defeat this attack.

Jamming attack: Jamming attack is a kind of DOS attack. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets [30].

IV. PERFORMANCE METRICS

There are several parameters for estimating the performance for example Throughput, PDR, delay from both ends called end to end delay and normalized routing load. For evaluating the quality or goodness the given measures are computed as:

1. **Throughput** is the ration of total number of packets delivered and total simulation time. It denoted as shown below. Assume 'N' is the total number of packets.

$$\text{Throughput}=\frac{N}{100} \qquad (1)$$

2. **Packet delivery ratio** is computed by dividing the total number of packets received by the sender through the number of packets received at the receiver.

$$\text{PDR} = \frac{\Sigma CBRrecv}{\Sigma CBRsour} \qquad (2)$$

3. **End to End delay** is the mean time by the packets to pass through the computer network.

$$\text{E\_to\_E} = \frac{\Sigma(CBRstime - CBRrtime)}{\Sigma CBRrec} \qquad (3)$$

4. **Normalized Routing Load** is the amount of routing packets transmitted per the overall data packet.

$$NRL=\frac{Number\ of\ packet\ received}{Number\ of\ packet\ transmitted} \quad (4)$$

V. CONCLUSION

In the recent years, wireless technology is progressing and increasing its popularity of wireless devices, made wireless networks so popular. MANET is a kind of Ad hoc network with mobile, wireless nodes. Due to its special characteristics like open network boundary, dynamic topology and hop-by-hop communications. MANETs are facing numerous challenges. In this paper we have covered the comprehensive review of MANET along with issues related to the security point of view for example security parameters and various attacks that occurred in MANET along with the additional parameters such as Network Overhead, Processing Time and Energy Consumption. The security is the main challenges in the networks and especially in the wireless technologies such as MANET. We can get better results from MANET by using its applications. The security can be enhanced with the implementation of better security mechanisms. The performance metrics like PDR, throughput, routing overhead, PSNR and frame/packet loss have been discussed. From the above discussion, it is urge to develop new algorithms for providing the better security and will continue our future work in this domain.

REFERENCES

[1] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyam, and et al., "Optimized Link State Routing Protocol for Ad Hoc Networks," Proc. IEEE Multi Topic Conference (INMIC 2001), IEEE Press, 2001, pp. 6268.
[2] C. E. Perkins and E. M. Royer, "Ad-hoc On-demand Distance Vector Routing," Proc. IEEE Workshop. Mobile Computing Systems and Applications (WMCSA 99), IEEE Press, Feb. 1999, pp. 90-100, doi:10.1109/MCSA.1999.749281.
[3] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in Mobile Computing of the Kluwer International Series in Engineering and Computer Science, vol. 353, T. Imielinski and H. F. Korth, Eds. Springer US, 1996, pp. 153-181, doi:10.1007/978-0-58529603-6_5.
[4] A. H. Mohsin, K. A. Bakar, A. Adekiigbe, K. Z. Ghafoor, "A survey of energy-aware routing and mac layer protocols in MANETs: trends and challenges", Network Protocols and Algorithms, vol. 4, pp. 82-107, June 2012.
[5] Macker, J.P., Scott Corson, M. Mobile ad-hoc networking and the IETF in Mob. Compute. Common. Rev. Vol.2. ACM Press, New York, NY (1998) 9-15.
[6]. Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir R. Das. "Ad Hoc on Demand Distance Vector (AODV) Routing. "Internet draft, draft-ietf-manet-aodv-13.txt, Feb 2003.
[7]. Charles E. Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90–100.
[8]. D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, ed. T.Imielinski and H. Korth, Kluwer Academic Publishers, pp.153-181, 1996.
[9]. V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proceedings of INFOCOM '97, April 1997.
[10] Mamatha, G. and Sharma, D.S. (2010) Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues. International Journal of Computer Science & Engineering Survey, 1, 14-21. http://dx.doi.org/10.5121/ijcses.2010.1102
[11] Goyal, P., Parmar, V. and Rishi, R. (2011) Manet: Vulnerabilities, Challenges, Attacks, Application. International Journal of Computational Engineering & Management, 11, 32-37.
[12] Aftab, M.U., Nisar, A., Asif, D., Ashraf, A. and Gill, B. (2013) RBAC Architecture Design Issues in Institutions Collaborative Environment. International Journal of Computer Science Issues, 10, 216-221.
[13] Aftab, M.U., Habib, M.A., Mehmood, N., Aslam, M. and Irfan, M. (2015) Attributed Role Based Access Control Model. Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, 18 December 2015, 83-89. http://dx.doi.org/10.1109/CIACS.2015.7395571
[14] Chitkara, M. and Ahmad, M.W. (2014) Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols. International Journal of Computer Science and Mobile Computing, 3, 432-437.
[15] H.Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks,," Communications Magazine,IEEE, 2002.
[16] Y.Z.a and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," presented at the 6th Int'l. Conf. Mobile Comp. Net., MobiCom, 2000.
[17] F.S.a and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks," 7th Int'l. Wksp on Security Protocols. Proc., LNC, 1999.
[18] X.Zhao, Z. You, Z. Zhao, D. Chen, and F. Peng, "Availability Based Trust Model of Clusters for MANET," presented at the 7th International Conference on Service Systems and Service Management (ICSSSM), 2011.
[19] E.C.H.Ngai and L. M. R, "Trust and clustering-based Authentication Services in Mobile ad hoc networks," presented at the proceeding of the 24th international conference on Distributed Computing systems Workshops 2004.
[20] W.Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," presented at the Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, 2004.
[21] S.Rana and A. Kapil, "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies, Communications in Computer and Information Science, vol. 101, pp. 186-194, 2010.
[22] M.A. Gorlatova, P. C. Mason, M. Wang, and L. Lamont, " Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, IEEE, MILCOM, 2006.

[23] S.Keer and A. Suryavanshi, "To prevent wormhole attacks using wireless protocol in MANET," presented at the nternational Conference on Computer and Communication Technology (ICCCT), 2010.
[24] Z.A.Khan and M. H. Islam, "Wormhole attack: A new detection technique," presented at the international conference on Emerging Technologies (ICET), 2012.
[25] M.Yu, M. C. Zhou, and W. Su, "A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments," IEEE Transactions on Vehicular Technology, vol. 58
[26] G.Singla, M. S. Sathisha, A. Ranjan, S. D., and P. Kumara, "Implementation of protected routing to defend byzantine attacks for MANET's," International Journal of Advanced Research in Computer Science, vol. 3, p. 109, 2012.
[27] G.Singla and P. Kaliyar, "A Secure Routing Protocol for MANETs Against Byzantine Attacks," Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, vol. 131, pp. 571-578, and 2013.
[28] R.H.Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012
[29] P.T. Tharani, K. Muthupriya, and C. Timotta, "Secured consistent network for coping up with gabrication attack in MANET," international journal of Emerging Technology and Advanced Engineering, vol. 3, 2013.
[30] J.Ben-othman and A. Hamieh, "Defending method against jamming attack in wireless ad hoc networks," presented at the 34th Conference on Local Computer Networks, LCN, IEEE, 2009.

Author's Profile:

Ms. B. Aruna Kumari, currently working as Assistant Professor at AITS, Rajampeta. She received her master's degree in Computer Science and Engineering from JNTUA pulivendula in the year 2015. She received her Bachelor's degree in computer science and engineering from CBIT, Proddutur affiliated to JNTUA University in 2012. Her areas of interest include Internet of Things and wireless networks

Ms. K.ROHINI, currently working as Assistant Professor at AITS, Rajampeta. She received her master's degree in Computer Science and Engineering from JNTUA University in the year 2015. She received her Bachelor's degree in Information Technology from RGMCET, Nandyal affiliated to JNTUA University in 2013. Her areas of interest include Internet of Things and wireless networks.