A COMPARATIVE ANALYSIS OF ROUTING ISSUES IN MOBILE ADHOC NETWORKS (MANET)

[1] L Raghavendar Raju, [2] P Vijayapal Reddy, [3] M. Praveen Kumar
[1]Assistant Professor, Dept of CSE, Matrusri Engineering College, Hyderabad, India,
[2]Professor, Dept of CSE, Matrusri Engineering College, Hyderabad, India, [3]
Assistant Professor, Dept of CSE, Matrusri Engineering College, Hyderabad, India,

Abstract- A Mobile Adhoc Network (MANET) is featured by multi-hop wireless connectivity with topology change due to highly mobile stations with autonomous configuration ability. Therefore, it is very challenging to develop vibrant and resourceful routing Protocol for MANET which also performs excellent routing with security feasibility. This paper presents a detailed study and analysis of various routing issues faced by protocols, and it also discusses the improved methods proposed by many researchers to solve these problems during routing up to some extent considering multiple parameters. This survey also offers a brief comparative analysis of prominent protocols which are proposed by eminent researchers considering the average delay and packet delivery ratio as network performance parameters.

***Index Terms*: MANET, Delay, QoS, Throughput.**

I. INTRODUCTION

Mobile Adhoc Network is an assemblage of self-governing mobile nodes which can correspond with each other in the wireless atmosphere. The mobile nodes which are not in the same range can converse with each other through multiple intermediate nodes. These nodes are flexible, self-configured, robust and are a part of a distributed network. Although routing in such a network is competent, but it is a challenging task due to the limited battery based power in the mobile nodes and to maintain routing we have to apply efficient routing strategies. In this paper different routing issues such as power management techniques and separate attacks during routing have been described and comparative analysis has been presented on different categories of procedures implemented in multiple routing protocols. Organization of this paper has been done as follows. Section 2 describes the related research on the said area; section 3 presents security mechanism in MANET routing, section 4 gives challenges and attacks, and section 5 presents comparative analysis and simulation with results, and at the end section, 6 concludes the paper.

II. RELATED WORK

In this section remarkable contributions of researchers in this area has been included. Paper [1] describes developed trust protocol based on congestion control, and this protocol guarantees the stability of the network and does the distribution of the load on the most highly trust nodes. Paper [2] defines the early detection congestion control routing protocol for the ad-hoc wireless network, and it detects congestion at node-level, and it finds congestion status by utilizing noncongested predecessor and successor nodes of a congested node. Paper [3] identifies the various security threats on the network layer. Paper [4] presents the security issues of data query processing and location monitoring. Paper [5] presents the rushing attack, i.e., a standard attack against routing protocol in MANET. Paper [6] offers about congestion control scheme in MANET, and it overcomes the disadvantage of existing multicast congestion control protocols. Paper [7] says about link-layer congestion control for ad-hoc wireless MANET, and here the bandwidth and delay is measured at each node along the path and based on the cumulated values the receiver calculates the window size and transmits the information to the sender as feedback.

III. SECURITY MECHANISM IN MANET

There are many essential features of MANET which makes it well known and very special. But susceptibility still emerges because of the inbuilt features of self-arrangement and frequent re-configuration. There are some reasons mentioned below that cause vulnerability in MANET.

(i). No Restriction
MANET has no limitation for nodes to combine, join, and leave in the network. The lack of security measures makes the MANET tending to the attacks. The MANET is open to attack because of absence of firewall and network gateway.

(ii).Topology change dynamically – Due to the high mobility of the nodes, the topology of MANET changes very frequently. Since nodes are changing & joining the mobile network; It is impractical to record the freed in a dynamic network. Some of these nodes can be a scoundrel and can be put in danger as these nodes do not have a place in the trusted zone.

(iii). No monitoring of Centralized Management – There is no central administrator in MANET that controls the working of activities in MANET. During the hop to hop data transmission, this issue sometimes brings about breakdown and failure in transmitted data. Thus, nodes don't contribute to any security operations. The inadequacy of this type cause can hamper the general operations of the nodes association and disjoints.

(iv).Restricted Power Supply **-** Source of energy in MANET - nodes is only their battery power, which is an embarrassed type of power supply because the power drains away with the use of it during packet forwarding.

(v). Inconsistent Scalability- Everything considered in wired network scale is predefined when outlined and not change such all through the usage. However, the size is improving each time in case of compliance with the ad-hoc network. There is no network to foresee the number of nodes in MANET. This infers that network needs scale all over at every one time in network.
Table 1. shows different work done by eminent researchers with their proposed protocols with security features executed by them.

Table 1. Details of studied security mechanisms.

Sl	Literature	Year	Basic Security mechanism used
1	Praveen Joshi[11]	2010	Security threats in Network layer
2	Jan Von Mulert et.al.[12]	2012	Focuses on networks that use AODV and SAODV protocols
3.	Rashid Sheik et.al.[13]	2010	Identification mechanism is needed between nodes using identification and credentials and this leads to privacy problems.
4.	Athuly MS	2012	Secure transmission of audio is not done
5.	Md. Qayyum et.al.[15]	2011	Security issues of data query processing and location monitoring.
6.	Edl Echchaachoui et.al.[16]	2014	Data security is a key issue in MANET
7.	V. Sheesha Bhargavi et.al.[17]	2016	Improvement of the security of files shared across MANET
8.	Vishnu Sharma et.al.[18]	2016	Attacks on the network layer of the protocol stack.
9.	Shilpi burman Sharma et.al.[19]	2015	Security issues in MANET
10.	Seyed- Mohsen Ghoreishi et.al.[20]	2014	Rushing attack is one of the comVmon attack against routing protocol in MANET

IV. CHALLENGES AND ATTACKS

It is a very challenging issue to prevent attacks in a MANET. General types of attacks and challenges found in MANET Routing Protocols are described in this section. Mobile ad-hoc networks are more challenging in comparison to other wire-based networks due to their dynamic nature of network reconfiguration. The challenged overpowering on MANET routing protocols are featured as a passive attack can not disturb the behavior of the protocol, but reveal the original data by tuning into movement of the nodes. In general concept, the passive attacks get essential routing knowledge by sniffing regarding the network. These type of network attacks are habitually tricky to set up and in this method, checking against such attacks is difficult. It is observed that it is not practical to compute the exact location of a station in a network. But one may be able to get the knowledge about the network topology using these type of attacks. Another class of active attack encompasses groups of nodes and makes an effort to halt the functioning of the protocol and tries to get confirmation. In this way, they try to hack the information from network stations. The target is done lavishly to draw in all groups of the attacker to modify the network. Such attacks could be set and may detect the nodes.

A) Different types of Attacks in MANETs

In ad-hoc networks, different kinds of attacks are there. Still some attacks are recognized as follows.

(i)Eavesdropping Attacks: These attacks usually are exposure attacks that are done by outside and interior stations who are not much involved in network activity. The basic purpose of the The attacker's target of Eavesdropping is to separate show messages and procure some helpful content close to the network that is essential all through the communication.

***(ii)Denial of Service (DoS*)**: In DoS attacks, attackers endeavor to attack at the availability of organizations of the entire Mobile Ad-hoc network. The attackers use the battery exhaustion routines and the radio is adhering to perform Dos attacks to the Mobile Ad-hoc network.

(iii)Dropping Attacks: In Mobile Ad-hoc network nodes those are malicious nodes intentional drops all the packets. This attacks, disturb the affiliation due to the malicious nodes. self-intent nodes thought to defend their performance. It decreases the network performance. By transferring data packets to be sent as yet again and find the new routes to the destination.

V. COMPARATIVE ANALYSIS AND SIMULATION RESULTS

A trust-based security protocol [8] has been designed with an improved security feature at the MAC layer. Another security protocol has been proposed named MAODV [9] based on the receive reply method specifically designed to prevent the black hole attack. In [10] a secured DSR algorithm has been proposed for better network security during routing. In the following section, three prominent security based protocols those discussed above have been simulated for their performance for the network parameters such as packet delivery ratio (PDR), transmission delay and power consumption. Glomosim simulation tool was used for simulation with the following network parameters.

Table 2, Simulation Parameters

Simulation parameters	Data/Value
Channel Type	Wireless Channel
MAC Protocol	802.11
Traffic Type	CBR
Packet Size	512 Bytes
No. of Mobile Nodes	50
Simulation Time	600 seconds
Simulation area	2000 x 2000 m
Protocols Name	MAODV,SDSR,TBS
Model for Node Movement	Random way point
Data rate	11 mbps
Application Type	Video Transmission
Bandwidth	2Mb/s for both
Simulator	Ns2.35

Table 2 shows the network simulation parameters considered during the simulation process for simulating the protocols considered for comparison of energy efficiency and security based protocols.

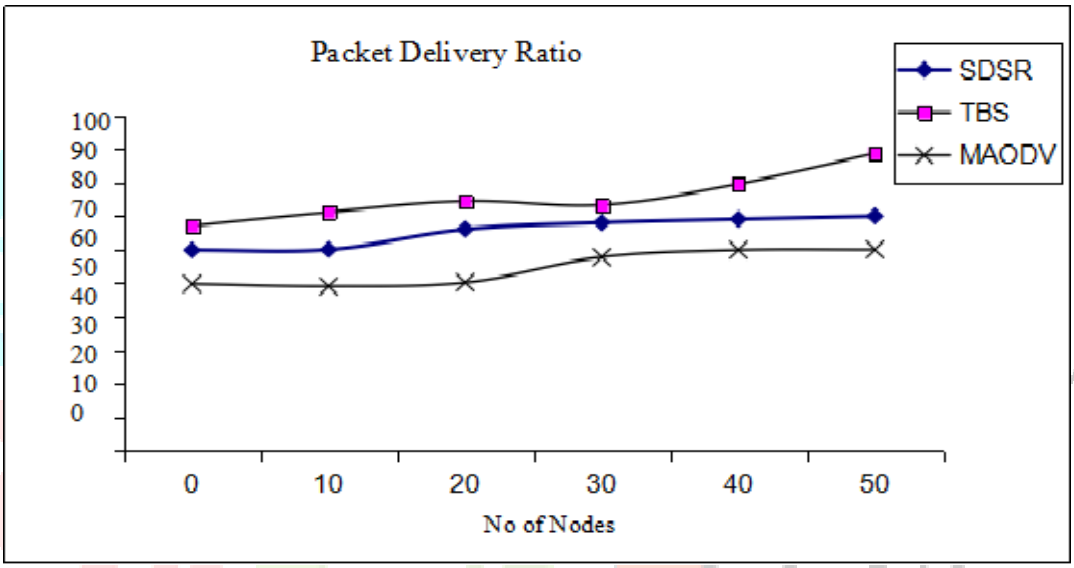

Fig.1 Comparison of Packet Delivery Ratio

Fig.1 displays the graphical result of comparison of packet delivery ratio (PDR). TBS Protocol with an improved MAC Layer technique shows better PDR when compared with MAODV and SDSR approach.

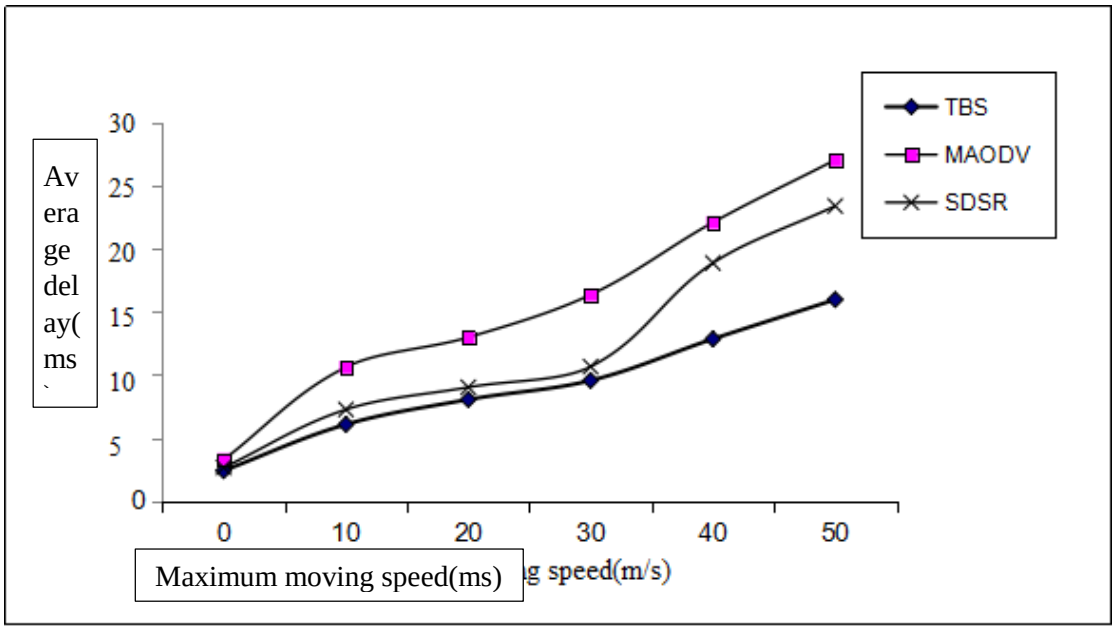

Fig.2 Comparison of Average Delay

Fig.2 shows the comparison of the average end to end delay between the discussed protocols. TBS exhibits minimum delay when compared with other approaches.

VI. CONCLUSIONS

In this paper, present an analysis and study on security issues in MANET and essential protocols proposed by researchers with their routing significance and security mechanism, another novel contribution and their performance results for security-based routing protocols in a very energetic Mobile Ad hoc network environment. First, the features of the secured protocols have been discussed and then we have enlightened the challenges that emerge due to different types of attacks in MANET. Taking the fundamental concept of Mobile routing, this paper highlights on the unfocused areas of routing with novel contributions which provide ample opportunity for new researchers to work further in the field of MANET routing.

REFERENCES

[1] R. Rashidi, M. A. J. Jamali, A. Salmasi and R. Tati, "Trust routing protocol based on congestion control in MANET," *2009 International Conference on Application of Information and Communication Technologies*, Baku, Page 1- 5., 2009.
[2] T. Senthil kumaran and V. Sankaranarayanan, "Early detection congestion and control routing in MANET," *Seventh International Conference on Wireless and Optical Communications Networks - (WOCN)*, Colombo, page 1-5,2010.
[3] Praveen Joshi,“ Security Issues in Routing protocols in MANETs at network layer”, *Procedia Computer Science*, Elsevier,Vol.3,pp. 954-960,2011.
[4]Mohammed Qayyum,P.Subhash and Mohammed Husamuddin, “ Security issues of Data Query Processing and Location Monitoring in MANETs”, *International Conference on Communication, Information and Computing Technology (ICCICT)*, IEEE, 2012.
[5] Syed Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari, “ Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Network”, *International Symposium on Biometrics and Security Technologies*, IEEE, 2014.
[6] P. Lv, X. Wang, X. Xue and M. Xu, "SWIMMING: Seamless and Efficient WiFi-Based Internet Access from Moving Vehicles," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 5, pp. 1085-1097, May 1 2015.
[7] Makoto Ikeda, Elis Kulla, Masahiro Hiyama, Leonard Barolli, Rozeta Miho and Makoto Takizawa, “ TCP Congestion-Control in MANETs for Multiple Traffic Considering Proactive and Reactive Routing Protocols”, 15th IEEE International Conference on Network-Based Information Systems, 2012.
[8] A. Rajaram and S. Palaniswami, "The Trust-Based MAC - Layer Security Protocol for Mobile Ad Hoc Networks," *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, Chengdu, 2010, pp. 1-4.
[9] Debarati Roy Choudhury, Dr. LeenaRagha, Prof. NileshMarathe,” Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack”, *International Conference on Advanced Computing Technologies and Applications (ICACTA-2015), Procedia Computer Science*, Vol.45, Pages 564 – 570,2015
[10] V. S. Bhargavi, M. Seetha and S. Viswanadharaju, "A hybrid secure routing scheme for MANETS," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*,Pudukkottai,pages1-5,2016.
[11] Praveen Joshi,“ Security Issues in Routing protocols in MANETs at network layer”, Procedia Computer Science, Elsevier,Vol.3,pp. 954-960,2011.
[12] Jan Von Mulert, Ian Weich and Winston K.G. Seah, “Security threats and solutions in MANETs: A case study using AODV and SAODV”, Journal of Network and Computer Applications, Elsevier,Vol. 35,pp.1249-1259,2012.
[13]Rashid Sheik, Mahakal Singh Chandel and Durgesh Kumar Mishra, “Security Issues in MANET: A Review”,IEEE,2010.
[14]Athulya MS and Sheeba VS, “ Security in Mobile Ad- Hoc Networks”, IEEE,2012.
[15]Mohammed Qayyum,P.Subhash and Mohammed Husamuddin, “ Security issues of Data Query Processing and Location Monitoring in MANETs”, International Conference on Communication, Information and Computing Technology (ICCICT), IEEE, 2012.
16]Adel Echachaachoui, Ali Choukri, Ahmed Habbani and Mohammed Elkoutbi, “ Asymetric and Dynamic Encryption for Routing Security in MANETs”, IEEE, 2014.
[17]V.Sesha Bhargavi, Dr. M. Seetha and S.Viswanadharaju, “ A Hybrid Security Routing Scheme for MANETS”, IEEE, 2014.
[18] Vishnu Sharma and Akansha Vij, “ Security Issues in Mobile Ad Hoc Network: A Survey Paper”, International Conference on Computing,Communication and Automation, IEEE, 2016.
[19]Shilpi Burman Sharma and Nidhi Chauhan, “ Security issues and their solutions in MANET”, International Conference on Futuristic trend in Computational Analysis and Knowledge Management”,IEEE, 2015
[20]Syed- Mohsen Ghoreishi, Shukor Abd Razak, Ismail Fauzi Isnin and Hassan Chizari, “ Rushing Attack Against Routing Protocols in Mobile Ad-Hoc Network”, International Symposium on Biometrics and Security Technologies, IEEE, 2014.