iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Hybrid Routing Protocol In Mobile Adhoc Network: A Review

Mubashir Moin[1], Aarti Malik[2]
[1]*Department of ECE, SVIET, Banur, Punjab, INDIA*

Abstract: ***Ad hoc network is a collection of nodes that are mobile in nature interlinked by using a wireless medium and thus creates a dynamic network. The ad hoc network did not follow any network topology and hence the ad hoc network suffers from unpredictable variations in network structure. Since the nodes are mobile therefore the ad hoc network is more prone to security attacks by malicious nodes. In ad hoc network like MANETs, the sensor's transmission range is limited therefore, it requires multi hop communication. The multi hop communication is done by using different routing protocols to elect the next hop for data transmission. This study provides an overview to the various routing protocols that provides a secure and effective routing and data transmission in ad hoc networks.***

Keywords: Ad hoc Networks, Routing, Secure Routing, Proactive Routing, Reactive Routing, Hybrid Routing, HARARAN.

I. INTRODUCTION

Ad Hoc Networks are the wireless networks which poses the property of self-organizing or did not follow any physical infra to settle down in the environment. Nodes or hubs in specially appointed systems (Ad Hoc Networks) act as both client and router. A few uses of specially appointed systems could incorporate mechanical and business applications including helpful versatile information exchange [1], such as military.

As of late, developing advances, for example, remote sensor systems (WSNs), wearable computing, pervasive processing, Internet of Things, have a great extent added to a further push toward application possibilities of specially appointed systems [2]. Ad hoc Networks present the characterized attributes of open connect, dynamic topology, and dispersed operation.

Ad hoc Networks are considered as totally self-ruling remote brief systems built up utilizing the gathered mobile devices principally for military, crisis and emergency cases where accessibility is restricted[3]. It is a gathering of versatile hubs which don't require a physical infrastructure or existence of the network for security and convenient purpose [4]. Dissimilar to hardwired systems with physical guard at firewalls and entryways, assaults on systems can originate from all headings and may focus on any node.

Independent nodes have deficient physical assurance and can be caught, traded off, and captured effortlessly [6]. Interruptions from a compromised hub are more hazardous and significantly harder to recognize [7]. Harm incorporates releasing confidential data, intrusive message and imitating nodes or hubs, in this way violates the essential security necessities. All these imply that each hub must be set up to experience with a foe either directly or indirectly [8].

II. ROUTING PROTOCOL

Routing protocols in ad hoc networks are categorized in three types as follows:

A. Proactive Routing Protocol

Nodes in MANETs continuously verify and estimate routes from source to destination node so that the information stored in the table is up to date and consistent in nature. This process helps in providing the routing path immediately to the source node in case of requirement. Proactive routing is also referred as "table driven" routing protocol as it updates the table continuously. In case of change in network topology, updates must be known throughout the network for application of change in the table.

1) *Destination Sequenced Distance Vector routing(DSDV):* Destination Sequence Distance Vector is based on Bellman-Ford algorithm. Whereas, the mechanism followed to get better routing performance is little bit different. In routing table, the entry stored in routing table is regarding the next hop towards a destination, the cost metrics for destination path and a list of destination sequence generated by destination. [5] And then this list of sequence number is used to detect the stale routes and to handle the formation of route loops.

B. Wireless Routing Protocol (WRP)

The objective of this protocol is to decrease the chances of temporary route loop creation in MANETs. It is related to the concept of path detection algorithms. The characteristic of this technique is that it makes proper use of the information related to the predecessor node and how far the node located form the destination node. WRP follows a table structure for path finding. In this each and every node have to maintain multiple tables whereas in other table driven protocols the nodes are required to maintain only two tables. Hence the drawback of this protocol is that it requires a lot of memory for storing these tables.

C. Cluster Gateway Switch Routing Protocol (CGSR)

CGSR stands for Cluster gateway switching routing protocol. It is mainly a cluster based hierarchical routing protocol. It divides the whole network into sub sections that are known as clusters and then a node is elected from each sub section which represent that particular section while communication process. A mobile node which relates to more than one sub sections or clusters act as a gateway node which connects the cluster to each other. The communication initialized by routing the data packets through the route that have proper format of cluster heads within source and sink node [6]. The only leverage of this protocol is that it consist the routing tables which are small in size and require less memory for storing as compare to other protocols. The table consist only a single entry corresponding to all nodes corresponding to a cluster. Hence the size of table is reduced.

D. Reactive Routing Protocols

These protocols are also referred as “on-demand” routing protocol because the routing paths are defined or obtained at the time of requirement to a particular node [7]. In this process, route determination procedure has been followed in which this procedure terminates when a route has been found or when there is no route available for the communication. The process examines whole the network and then terminates after applying all route permutations in case of no route. Some of the examples of this routing are:

E. Ad-Hoc On-Demand Distance Vector Routing (Aodv)

The Ad Hoc On-demand Distance Vector is the AODV routing protocol abbreviation which is used in MANETs as reactive unicast routing protocol. The active paths regarding information is also need to be maintain using AODV. The routing information of each node is stored using routing table. The current routed destination information of each node is maintained by routing table. Before the expiration of lifetime as there is expiry time for each routing table entry. The DSDV like destination sequence number is also been used in AODV. The operation of route discovery is runs by AODV when there is availability of no existing route. The DSR similarly generated RREQ packet is broadcasted by source. The destination and source address along with unique broadcast id and last source and destination sequence number contain in RREQ. The up to date and loop free routes are guaranteed using sequence number [8]. The RREQ packets node dispose is used for route discovery operation and decrease the overhead traffic that extends ring search algorithm before seen it. The Time to Live (TTL) value is initiated by RREQ and TTL is incremented in the below given RREQs if destination is not detection.

F. Dynamic Source Routing (DSR)

The Dynamic Source Routing (DSR) is a reactive uncast routing protocol type. The source routing algorithm is used by it and in order to reach its destination complete routing information is exist in data packets. The route information is maintained using caching technology. The Route maintenance and Discovery phase are two phases of DSR. At the sender side a packets transmission is performed using Route cache. When route is available then routing information is appended with the packets of data. In another case a route request packets are broadcasted by route discovery operation that help in detecting the source node [9]. The source and destination address and packet are identified using unique request id given by route request packet. The route cache is checked when a route request packet is received by a node. The own address of node is added in the field of route record when requested destination information is not present in node itself. The requested packet is transmitted to its neighboring node. The route request packets are processed by node that helps in controlling route request packet communication. The address of those nodes is not present in route record field and they are not seen before using it. When destination routing information is contain by intermediate node and each packets of route request reach to destination then a route reply is generated. When destinations generate a packet route reply is included along with traversed nodes addresses.

G. Hybrid Routing Protocols

The reactive and proactive routing protocols merits are combined in hybrid routing protocols and their demerits is not added in it

[10]. The hierarchical architectures property is exploited in this approach. The different hierarchical level is the criteria to divide first two approaches. The Zone-based Hierarchical link state (ZHLS), Zone routing protocol and hybrid ad hoc routing protocol is the example of Hybrid routing. There are different existing hybrid routing protocols and some of them are given below:

1) Temporally Ordered Routing Algorithm (TORA)
2) Zone Routing Protocol (ZRP)
3) Zone-based Hierarchical Link State (ZHLS)
4) Sharp Hybrid Adaptive Routing Protocol(SHARP)
5) Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR)

H. HRARAN

HRARAN is a highly reputed authenticated routing protocol that is used in MANETs. It is a routing protocol which ensures the route safety by implementing the cryptographic techniques to overcome all attacks. Its main objective is to protect a route from unauthorized access. In this protocol it is mandatory for each and every node to validate its identity before taking part into communication process . The identification validation is done by linking to the certification authority to send a certification request corresponding to its address and public key from a server T. The certification consist of following notations-

$$T \rightarrow A : Cert_A = [IP_A, K_{A+}, t, e\,]KT \qquad (1.1)$$

Here in equation (1.1) the notation

$Cert_A$ represents certification corresponding to node A.

Generalized algorithm for HARARAN protocol-

1) *Collect data from T, RDP,IP, N*
2) *Each node receives a certificate from Trusted Server*

$$T \rightarrow A : Cert_A = [IP_A, K_{A+}, t, e\,]KT \ldots\ldots\ldots\ldots\ldots\ldots (1.2).$$

3) *The Source broadcasts the route request to next hop (REQ).The same step repeats until the desired destination is reached.*

$$S \rightarrow broadcast : [RDP, IP_X, N_Q]KS, Cert_S \ldots\ldots\ldots\ldots\ldots\ldots (1.3)$$

4) *The Receiver routes the response (REP) back to the originator.*

$$X \rightarrow R : [REP, IP_S, N_S]K_X, Cert_X \ldots\ldots\ldots\ldots\ldots\ldots (1.4)$$

5) *The Route causes node to generate an error ERR) message. Error is identified.*

$$P \rightarrow Q : [ERR, IP_S, IP_X, N_Q]K_P, Cert_P \ldots\ldots\ldots\ldots\ldots\ldots (1.5)$$

6) *The trusted server T sends a broadcast message to the ad hoc group that announces that revocation.*

$$T \rightarrow Broadcast : [revoke, cert]KT \ldots\ldots\ldots\ldots\ldots\ldots (1.6)$$

Table 1: Comparison of Routing Protocol

Protocol	Advantages	Disadvantages
Proactive	High Availability of Information. Low Latency.	High Overhead, Routing Information is flooded.
Reactive	Low Overhead, loop free.	High Latency.
Hybrid	Suitable for large scale networks.	High Complexity.

III. RELATED WORK

Houda Moudni et al [4], Mobile ad-hoc network does not have any specific infrastructure and nodes are linked with one another and no centralized control is required. This characteristic of the network is susceptible to different attacks. Therefore it is difficult job for various researchers to determine the suitable solution pacify the attacks encountered in routing protocols. Different threats to Ad-hoc on demand distance vector routing protocol had been simulated and the number of threats were as follow: black hole, flooding and rushing. The simulation had been done to determine its effects on this protocol. The simulator used was NS-2 network simulator. Old researches just consider one attacker or the size of network in order to analyse the efficiency of protocols in network. Various parameters like packet delivery ratio, average latency and rate of output generation to evaluate the performance. After simulation the results had shown that network efficiency is highly affected by black hole attack as compare to flooding and rushing attacks and degradation in network performance in case of black hole attack.

Vinay Rishiwal et al,[8],. The AODV had been investigated for various numbers of times and had been described in different literature but the concept of uniformity was not discussed yet. The term heterogeneity can be described as diversity in various nodes. The network is generally heterogeneous in nature while there is restricted fluid dynamic surrounding in mobile ad-hoc networks. In this paper, the experiments had been conducted to analyze the efficiency of routing protocol and also the performance of AODV routing protocol had been analyzed. The performance had been analyzed by measuring various features and that were: ratio of distributed packets, rate of output, average latency, and average value calculated for energy consumption, etc. For simulation of routing protocols had been done by using the NS-2 simulator.

Zhenqiang We [10], In general, it is necessary to present redundancy while presenting multi node-disjoint routes from transmission end to receiving end. Firstly in this paper a changed version of AODV routing protocol had been presented that had permitted to determine the multi node-disjoint routes from transmission end to receiving. It was observed that only few routes can be determined. Moreover, with the increment in length among transmission node and receiving node, Blockage cannot be avoided and therefore, the probability of determining the various routes had been minimized significantly. It had been concluded that it was very important to locate the reliable nodes in the network for optimum performance. Various location and route to reliable nodes determining techniques had been also proposed in this paper so that the framework can be obtained to get the efficient routing data. Different ideas to determine the reliable path containing different segments and all the segments consist of either complete reliable nodes or predefined multiple routes among different end points of segments. In this it was defined that notion of a reliable path which is made up of multiple segments. It had been shown that possibility of forming the reliable route between random source and target pairs had been increased significantly even with limited number of reliable node

Vanita Rani [11], In this paper, the main focus was on study of different Ad Hoc network and various protocols used in it, because this is newly rising field in networking. As the nodes were not static and varying from one position to another therefore the topic of dynamic mobility had been added in Ad Hoc networks. By adding this concept any node can enter into the network and can exit the network at any moment. The term node here means devices working in the network for example mobile unit, laptop, MP3 player and PC etc. these devices were part of network and can vary their location and simultaneously these nodes can work as both host and router. The priority in these networks was security and fast communication.

Table 2 Related Works

Authors	Techniques	Brief	Outcomes
Renisha P Salim et al(2016)[1]	Distributed Hash Table (DHT)	Enhanced DHT by using Bloom Filters	---
Houda Moudni et al(2016) [4]	Ad hoc On Demand Distant Vector (AODV)	Simulate black hole, flooding and rushing attacks	Advantages: Analyzes the impact of attacks on the mobile network. Disadvantage: Did not consider or evaluate for wormhole attack in the network.
Mamta Rath et al (2016)[7]	Ad hoc On Demand Distant Vector (AODV)	Analysis of power efficient routing protocols in Mobile Ad hoc Network(MANET)	Advantages: Considers power management, delay, quality of service and resource reservation as major factor. Disadvantages: Low Throughput and

			maximized delay.
Vinay Rishiwal et al(2016)[8]	Ad hoc On Demand Distant Vector (AODV)	Analyzing behavior of AODV in homogeneous and heterogeneous MANETs	Advantages The loyal byzantine army general are suppose to coordinate in a battlefield to conclude a common plan in the presence of traitor generals which can disrupt such coordination. Disadvantages: Less Reliable
Divya Bandral et al(2016)[16]	Ad hoc On Demand Distant Vector (AODV)	To improve the quality of performance of MANETs.	Advantages: Generates highly reliable and efficient outcomes. Disadvantages: less improvement in path establishment and QoS parameters for communication.
C. Atheeq et al(2016) [17]	Trust Based Mechanism	Securing both mobile or fixed nodes in the network	Advantages: Protection of data from un-trusted nodes in MANETs Disadvantage: Less reliable due to the lack of encryption mechanism.
S Sasila jabmani et al(2016) [18]	Encryption	Degrade packet dropping rate in MANETs.	Advantages: Reduced energy utilization, High packet delivery, throughput, and reduced delay in transmission. Disadvantage: Used ID based encryption strategy which is less effective to secure the data.
Y. Kanizo et al (2015) [19]	Hash Tables	The tradeoff problem discussed and solved by analysis of expected maximum matching size with fixed left side vertex degree.	Advantages: Deduction of asymptotic results and High efficient by improvement in memory access. Disadvantages: Avoidance of DRAM access is not suitable for high efficient schemes.
Qian et al [47] (2015)	Hash Tables	High efficient index structure for event matching presented. Realization of overlapping regions provided the more efficient space consumption.	Advantages: Improved matching efficiency and fast matching speed. Disadvantage: The performance improvement is required only if the size of subscriptions and constraints are large.
Anchugam Vangilli et al [21] (2015)	AODV	Analyzed the effects of black hole attack in the light of network load, throughput and end-to-end delay in MANETs and simulating the black hole attack using reactive routing protocols (e.g. AODV).	Advantages: Improved PDR, end-to-end delay and throughput. Disadvantages: Able to detect only black hole attack.

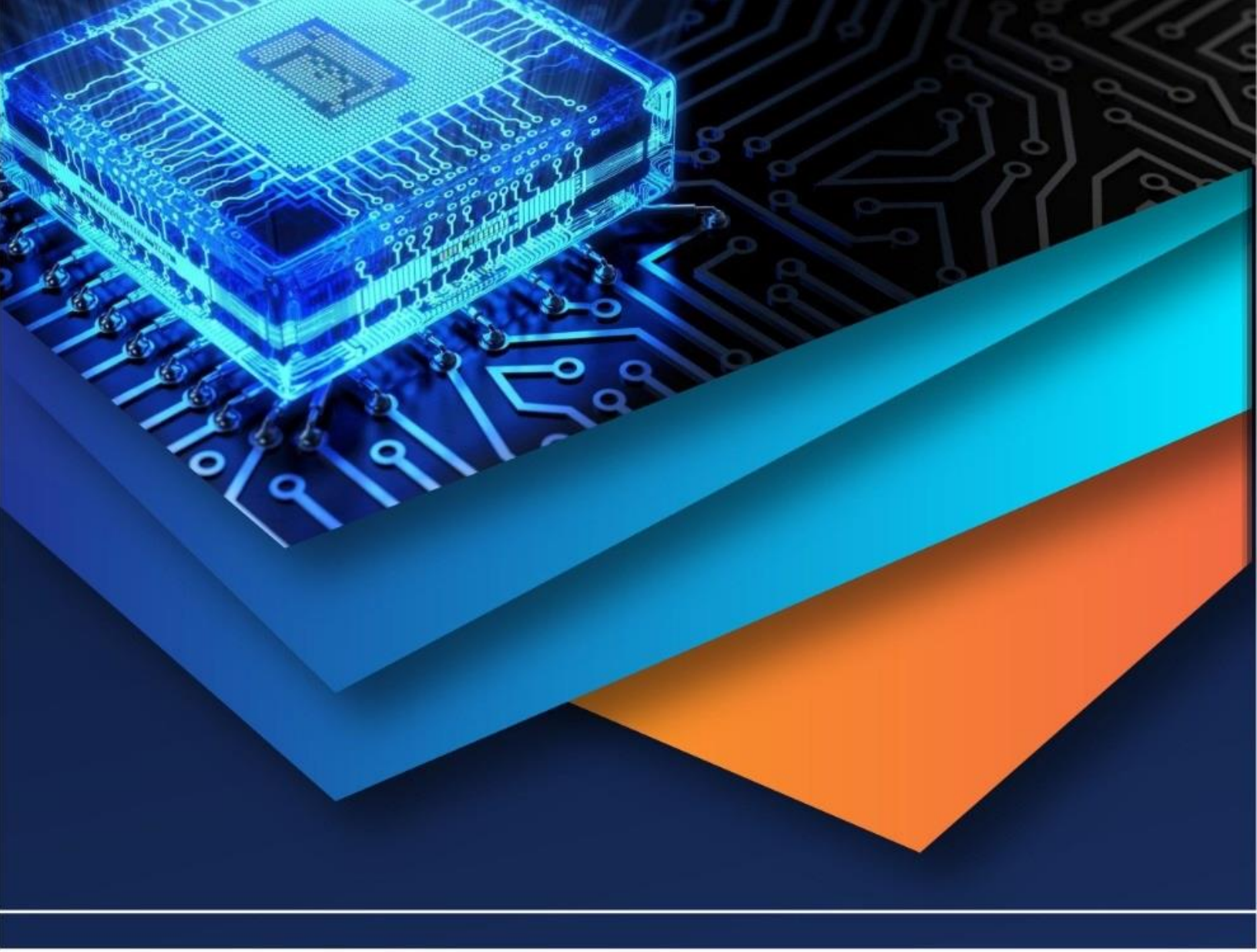
IV. CONCLUSION

The routing is the major concern as the advancements takes place in wireless network technology. The ad hoc network is also a kind of wireless network in which the nodes are mobile in nature and do not have a fixed structure and topology. Thus to achieve

effective routing and data transmission in ad hoc network is quite difficult as it suffers from various issues like security etc. This study concludes various routing protocols that are developed to achieve successful data transmission without losing its confidentiality and quality. This work can provide guidance to the researchers who are interested to do development under this field.

REFERENCES

[1] Renisha P Salim , Rajesh R."A Survey: Optimal node routing strategies in MANET", IEEE, Pp 1-8, 2016
[2] Burak Yanar,Weilian Su, "Dynamic Extension of network for collecting data from multiple ground nodes", IEEE, Pp 1-6, 2016
[3] Vinay Rishiwal , "Analysis of ad hoc routing protocols: A retrospective view", IEEE, Pp 1-6, 2016
[4] Houda Moudni,Mohamed Er-rouidi , Hicham Mouncif, Benachir El Hadadi, "Performance Analysis of AODV routing protocol in MANET under the influence of routing attacks", IEEE, Pp 1-7, 2016
[5] Houda Moudni , "Secure Routing Protocols for Mobile Ad hoc Networks", IEEE, Pp 1-7, 2016
[6] Ziau Rahman, Fazirulhisyam Hashim, Mohamed Othman , Mohd Fadlee A. Rasid, "Reliable and Energy Efficient Routing Protocol for Under water Wireless Sensor Network", IEEE, Pp 24-30, 2015
[7] Mamta Rath , "Group based analysis of AODV related protocols in MANET", IEEE, Pp 548-553, 2016
[8] Vinay Rishiwal, Sandeep Kumar Agarwal , Mano Yadav, "Performance of AODV protocol for H-MANETs", IEEE, Pp 1-4, 2016,
[9] Dan-Yang Qin, Libn Mah, "An Effective Survivable Routing Strategy for MANET", 2011
[10] Zhenqiang. Wei, Helen Tang , F. Richard Yu , Maoyu Wang , Peter Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning", IEEE Trans. Veh. Technol., vol. 63, no. 9, Pp. 4647–4658, 2014
[11] Vanita Rani,Dr. Renu Dhir "A Study of Ad-Hoc Network: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, vol 3, Issue 3, Pp 135-138, 2013
[12] Muhammad Imran,Farrukh, Aslam KhanbTauseef, Jamala Muhammad, Hanif Durada, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science, Pp: 384-390, 2015.
[13] Sayan Banerjee, Roshni Nandi , Rohan Dey , Himadri Nath Saha, "A Review on Different Intrusion Detection Systems for MANET and its Vulnerabilities", IEEE, 2015
[14] Ana Maria Popescu,Ion Gabriel, Tudor ache, Bo Peng, A.H. Kemp,"Surveying Position Based Routing Protocols for Wireless Sensor and Ad-hoc Networks", IJCNIS, Vol 4, 2012
[15] Mahesh K. Marina, "Routing in Mobile Ad Hoc Networks", Springer, Pp. 63-90
[16] Divya Bandral, Reena Aggarwal, "Simulation Analysis of AODV and DSDV Routing Protocols for Improving Quality of Service in MANET", International Journal of Information and Education Technology, Vol 9(32), Pp. 1-5 ,2016
[17] C. Atheeq, , "Secure Data Transmission in Integrated Internet MANETs Based on Effective Trusted Knowledge Algorithm", International Journal of Science and Technology, Vol 9(47), Pp. 1-7, 2016
[18] S. Sasila Jabamani, E. Rajinikanth, "Integrity Key based Mechanism to Debase Packet Dropping in Manets", International Journal of Information and Education Technology, Vol 9(14), Pp. 1-4, 2016
[19] Y. Kanizo, D. Hay, and I. Keslassy, "Maximizing the Throughput of Hash Tables in Network Devices with Combined SRAM/DRAM Memory," IEEE Transactions on Parallel and Distributed Systems, vol. 26, pp. 796-809, 2015
[20] S. Qian, J. Cao, Y. Zhu, M. Li, and J. Wang, "H-tree: An efficient index structure for event matching in content-based publish/subscribe systems," 2013.
[21] Anchugam Vangili , K. Thangadurai, "Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis", International Journal of Science and Technology, Vol 8(13), Pp. 1-10, 2015



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY