**International Journal of Advanced Research and Development**
**ISSN: 2455-4030**
**Impact Factor: RJIF 5.24**
**www.advancedjournal.com**
**Volume 2; Issue 5; September 2017; Page No. 640-645**

# A survey: Different type of protocols and their security issues in ad-hoc network for secure data transmission

**[1] Bhawna Sharma, [2] Sudesh Kumar**
[1] Assistant Professor, GNG College, Yamunanagar, Haryana, India
[2] Associate Professor, GNK College, Yamunanagar, Haryana, India

**Abstract**
Wireless mobile ad-hoc networks are normal as networks except there is no static topology due to the mobility of interference, direction loss, multipath propagation and nodes, Hence a Routing protocol is needed for these networks to feature properly. The feature of protocols is to enable the exchange of information between computers or network devices using rules. Several routing protocols have been proposed for Ad-hoc networks however sometimes these protocols are susceptible to routing attacks like packet shedding and delayed packet forwarding, this is the major trouble in Ad-hoc network. This paper gives an overview of the protocols that are used in Ad-hoc network device and determined security features of all the protocols for secure data transmission.

**Keywords:** protocol, MANET, routing protocol, secure data transmission, security

## 1. Introduction

A mobile Ad-hoc network is a self-governing collection of mobile users that join over relatively “slow” wireless connections. Since the nodes are mobile, the system topology can change firstly and unusually over time. The network is decentralized, where all network program, including finding the topology and conveying communications must be performed by the nodes themselves. Therefore routing activities will have to be incorporated into the mobile nodes. Since the nodes communicate over wireless connections, they need to contend with the effects of radio communication, for example interference, fading and noise. In addition, the connections typically have less data transfer capacity than a wired network. Every node in a wireless ad hoc network functions as both a host and a router, and handle of the system is disseminated between the nodes. The topology of the ad-hoc system is in general dynamic, because the connectivity between the nodes may vary with time due to node departures, new node comes, and the probability of taking mobile nodes.

Routing is the process of selecting paths in a network [1] to transmit data packets from one node to another node in the network. A MANET routing protocol is a convention or we can say that it is a standard that controls flow of data packets in the network and also decide that which path should be followed by the packets to the reach the particular destination. In a MANET, topology of the network is not fixed due to its dynamic nature. Because of it, we do not have a fixed path from one node to another node in the network, they have to discover by the announcement of its presence. Every node in the network and should also listen to announcements broadcasted by its neighbors [2]. There are some challenges that make the design of Mobile Ad-hoc Network routing protocols a tough task. Firstly, in MANET, node mobility causes frequent topology changes and network partitions. Secondly, because of the variable and unpredictable capacity of wireless links, packet losses may happen frequently. These are the security issues in mobile Ad-hoc network [3].

Types of protocol for MANETs is described in Section 2, security issues of protocol for MANETs is described in Section 3, Section 4 shows types of attacks for ad hoc network that are very dangerous for MANET, The secure ad-hoc routing for MANET is described in Section 5 shows and Section 6 shows conclusion.

## 2. Routing Protocols

Design of efficient routing protocols in such a network is a challenging problem due to its unique characteristics, such as dynamic topology and scare wireless bandwidth [4]. Routing is the process of finding a path from a source to some arbitrary destination on the network. A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks [5]. These protocols find a route for packet delivery and deliver the packet to the correct destination. The studies on various aspects of routing protocols have been an active area of research for many years. Many protocols have been suggested keeping applications and type in view [6]. MANET routing protocols fall into two general categories,

1. Proactive routing protocols
2. Reactive routing protocols
3. Hybrid routing protocol

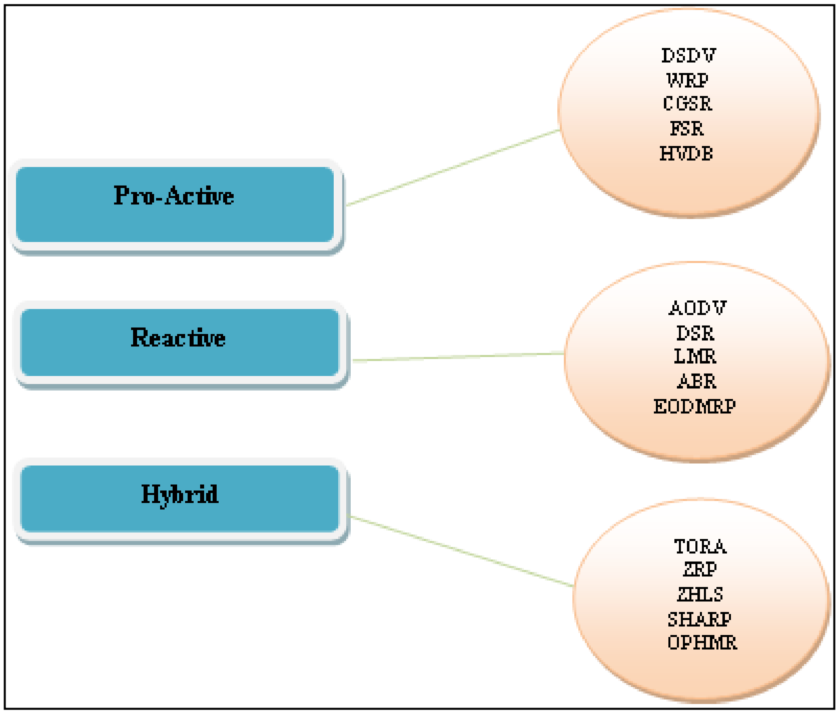

**Fig 1:** Different types of protocol

### 2.1 Pro-active / table driven routing protocols

Proactive protocols is table driven protocol of MANET and will actively define the structure of the system. Through a steady interchange of network topology packets between the nodes of the network, a complete characterization of the network is kept up at every individual node [7]. There is hence minimal delay in deciding the path to be held.

Some of the existing proactive/table driven routing protocols are.

- Destination Sequenced Distance Vector routing (DSDV)
- Wireless Routing Protocol (WRP)
- Cluster Gateway Switch Routing protocol (CGSR)
- Fisheye State Routing (FSR)
- The logical Hypercube-based Virtual Dynamic Backbone protocol (HVDB)

### DSDV

This is a distance vector routing protocol so ensures a loop-free routing by means of tagging every route table penetration together with an adjunct number and is based totally upon the Bellman-Ford algorithm in conformity with count the shortest variety of nodes to the end point. Each node of DSDV protocol keeps a routing table as store send point, next node addresses or number over nodes as well as much adjunct numbers routing table updates are forward periodically as incremental dumps constrained after a volume on 1 packet containing only current information [8].

### WRP

Distance vector routing protocol that intends to diminish the possibility of forming transitory routing loops in MANET. It is a proactive, goal based protocol. WRP has a place with the class of way discovering algorithms. The typical feature for these algorithms is that they use data about separation and second-to-last node along the way to every destination.

In WRP there is a very muddled table structure. Every node keeps up 4 distinct tables as in many other table-driven protocols just two tables are required. These 4 tables are,

- Distance table
- Routing table
- Link- cost table
- MRL- Message Retransmission List table.

### CGSR

This is a typical cluster based hierarchical routing. A stable clustering algorithm Least Cluster head Change (LCC) is utilized to partition the entire system into clusters and a Cluster head is chosen in each cluster. A mobile node that has a place with at least two or more clusters is a gateway connecting the clusters. Information packets are routed across the routes having a layout of Cluster head Gateway among any source and destination groups.

### FSR

The Fisheye State Routing is a proactive unicast routing protocol in view of Link State routing algorithm with viably reduced overhead to keep up arrange topology data. As showed in its name, FSR utilizes a function like a fish eye. The eyes of fishes get the pixels close to the central with high detail, and the detail diminishes as the distance from the central point increases. Like fish eyes, FSR keeps up the exact distance and way quality data about the quick neighboring hubs, and dynamically reduce detail as the separation increments. State routing algorithm utilized for wired networks, link state updates are created and flooded through the network whenever a node identifies a topology change.

### HVDB

The logical Hypercube primarily based digital Dynamic backbone is a proactive, QoS-conscious and hybrid multicast routing protocol for big scale MANET. It includes proactive logical route preservation, summary based totally club update and logical location-primarily based multicast routing. Because of the regularity and symmetry homes of hypercube, no leader is needed in a logical hypercube, and every node performs nearly the equal role besides for the slightly exclusive roles of border cluster heads and inner cluster heads. For this reason, no single node is greater loaded than another nodes, and no problem of bottlenecks exists, which is possibly to arise in tree-based totally architectures.

## 2.2 Reactive / On Demand Routing Protocols

On-demand for routing is a famous routing set for wi-fi Ad-hoc routing. It's far a particularly new routing philosophy that provides a scalable way to fantastically big network typologies. The layout follows the concept that every node attempts to reduce routing overhead with the aid of only sending routing packets whilst verbal exchange is requested. Commonplace for maximum on-demand for routing protocols are the route discovery segment wherein packets are flooded into the community in search of an ideal direction to end point in the network [9, 10].

A Number of the prevailing proactive routing protocols are,

- Ad-hoc On-demand Distance Vector routing(AODV)
- Dynamic Source Routing (DSR)
- Light-weight Mobile Routing (LMR)
- Associativity Based Routing (ABR)
- The Enhanced On Demand Multicast Routing Protocol (EODMRP)

### AODV

The ad-hoc On-demand Distance Vector routing is an development on DSDV as it commonly minimizes the quantity of necessary broadcasts through growing routes on a demand for foundation, instead of preserving a whole record of routes as inside the algorithm of DSDV. The researcher of AODV categorize it as a natural on-demand for route acquisition device, seeing that hops that is not on a selected way do not hold routing facts or contribute in exchange the routing table.

### DSR

DSR lets in hops in the mobile Ad-hoc network to dynamically found a source route throughout various network nodes to any endpoint. On this protocol, the requirement of the cell nodes to control route caches or the identified routes. The route cache is updated while any new path is known for a particular entry within the course cache. DSR Routing is done using 2 stages router find out and route protection. Whilst a source node like to send a packet to an endpoint, it primary consults its direction cache to find out whether it already is aware of about any route to the destination or no longer. If already there's an access for that end point, the source uses that to ship the packet.

### LMR

This protocol is based on the concept of hyperlink reversal set of rules. LMR addresses the problem of partitioned network by means of offering a link erasure mechanism. LMR requires 2 passes to re-set up and converge to an alternate path, if one exists. LMR can erase invalid routes and discover partition in a single pass. It is considered to lessen the manipulate message propagation in surprisingly dynamic cell networking environment. Due to this shortest hop paths are given simplest secondary significance and this protocol fits under the steadiness criteria. The advantage of this protocol is that routes will be found rather quickly and damaged links we have only local affect. It has good performance if the network connectivity is excessive, i.e., in the case of dense community.

### ABR

This protocol defines a new form of routing metric, degree of affiliation balance for MANET. In this routing protocol, a path is selected based totally at the degree of association stability of cellular nodes. Each node periodically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity desk. For each beacon acquired, the associativity tick of the receiving node with the beaconing node is increased. A high importance of associativity tick for any particular beaconing node means that the node is highly static. Associativity tick is reset when any neighboring node turn out of the neighborhood of any other node.

### EODMRP

The Enhanced on Demand Multicast Routing Protocol is an enhancement of ODMRP, which is a reactive mesh-based multicast routing protocol. It is an enhanced version of ODMRP with adaptive refresh. Adaptation is driven by receivers' reports. The second enhancement is the "unified" local recovery and receiver joining scheme. As the time between refresh episodes can be quite long, a new node or a momentarily detached node Might lose some data while waiting for the routing to it to be refreshed and reconstructed.

## 2.3 Hybrid routing protocols

Hybrid routing protocols are a new generation of protocols, where both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. This is mostly achieved by proactively maintaining routes to nearby nodes and determining the route to faraway nodes using a route discovery strategy [11].

Some of the existing hybrid routing protocols are.

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

### TORA

This is a distributed highly adaptive routing protocol designed to operate in a dynamic multihop network. TORA uses an arbitrary height parameter to determine the direction of link between any two nodes for a given destination. Consequently, multiple routes often exist for a given destination but none of them are necessarily the shortest route. To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination [12].

### ZRP

ZRP utilizes both proactive and reactive routing strategies in order to gain benefits from the advantages of both types. It is a hybrid routing protocol which combines the advantages of both proactive and reactive approaches. It takes advantage of proactive protocol to find node's local neighborhood as well as reactive protocol for routing between these neighborhoods [13].

### ZHLS

In this protocol, the network is divided into no overlapping zones as in cellular networks. Each node knows the node connectivity within its own zone and the zone connectivity information of the entire network. The link state routing is performed by employing two levels: node level and global zone level. ZHLS does not have any cluster head in the network like other hierarchical routing protocols. The zone level topological information is distributed to all nodes. Since only zone ID and node ID of a destination are needed for routing, the route from a source to a destination is adaptable to changing topology. The zone ID of the destination is found by sending one location request to every zone [14].

### SHARP

SHARP adapts between reactive and proactive routing by dynamically varying the amount of routing information shared proactively. This protocol defines the proactive zones around some nodes. The number of nodes in a particular proactive zone is determined by the node-specific zone radius. All nodes within the zone radius of a particular node become the member of that particular proactive zone for that node. If for a given destination a node is not present within a particular proactive zone, reactive routing mechanism (query-reply) is used to establish the route to that node [15].

### OPHMR

The Optimized Polymorphic Hybrid Multicast Routing protocol is a proactive, polymorphic energy efficient and hybrid multicast routing protocol. It attempts to benefit from the high efficiency of proactive behavior and the limited network traffic overhead of the reactive behavior, while being power, mobility, and vicinity-density aware. The protocol is based on the principle of adaptability and multi-behavioral modes of operations. It is able to change behavior in different situations in order to improve certain metrics like maximizing battery life, reducing communication delays, improving deliverability, etc. [16].

## 3. Security Issues in Ad-hoc Network

Protection is a totally challenging difficulty for designing an efficient and cozy routing protocol for MANETs. The infrastructure much less and the dynamic nature of MANET needs new set of networking techniques to be implemented so as to offer efficient and at ease quit to stop verbal exchange [13]. Because of the shortage of a predefined centralized management for path discovery system which leaving MANETs vulnerable to assaults, that effects in degradation within the overall performance of the community. Protection attacks disturb routing operations which create many problems like jamming the network, Denial of provider, or other sorts of severe assaults within the network.

### 3.1 Routing Security Issues

A MANET's routing protocol unearths routes between nodes, then permits information packets to be forwarded through different network's nodes in the direction of the very last destination. In evaluation to standard network routing protocols, Ad-hoc community routing protocols must adapt extra fast to cope with MANETs factors provided formerly, mainly the frequent alternate of the community topology [17] This hassle of routing in ad-hoc networks is an essential one and has been considerably studied, especially in the MANET running group of the net Engineering task pressure (IETF). Considering the fact that MANET surroundings is untrusted, a secure routing protocol is needed.

### 3.2 Data forwarding security issues

Protecting the network layer in an Ad-hoc system is a main research topic of wi-fi protection. The core functionalities provided in the network layer are pathing and packet forwarding, malicious attacks on either of them will interrupt the normal network processes. Although several current proposals have addressed the problem of protection MANET routing, as shown formerly, protection of information forwarding facility has received exceedingly much less attention except the works of. Now we discuss approximately the difficulty of shielding packet forwarding [18].

### 3.3 Data forwarding attacks

#### 3.3.1 Eavesdrop

The wi-fi channels are using in mobile Ad-hoc network are freely and easily accessible. Furthermore, promiscuous mode, which means shooting packets by using a node that is not the precise destination, is employed via protocols to function or to ensure greater efficiency, a routing protocol may additionally use this mode to analyze routes. These features may be hired through malicious to eavesdrop records in transit. The apparent proactive answer towards that is to use cryptography, this answer simply guarantees confidentiality, however does no longer prevent eavesdropping, and to the nice of our know-how, no detecting solution is available. When you consider that breaking keys is constantly feasible and using a strong key revocation inside MANET is tricky, eavesdropping is a serious attack in opposition to records forwarding.

#### 3.3.2 Dropping data packets

Due to the fact that packets comply with multi-hop routes, a malicious can take part in routing and drop all packets it receives to ahead. To do this, it first assaults the routing protocol to benefit participation in routing, using one or more of the attacks provided previously.

#### 3.3.3 Inject forged data packet

A malicious may additionally data records to inject and disperse them without a different interest than overloading the community, this may bring about disruption of forwarding prison packets.

- **Secure routing protocol requirements**

A good protect routing protocol purpose is to save each of the exploits. For this reason, it should fulfill the following requirements:

1. Routing loops cannot be formed through malicious actions.
2. Unauthorized nodes should be excluded from route computation and discovery.
3. Routing messages cannot be altered in transit.
4. Fabricated routing messages cannot be injected into the network.
5. Routes cannot be redirected from the shortest path by malicious actions.
6. Routing packets cannot be spoofed.

## 4. Types of attacks in Ad-hoc Network

Due to their specific structure, MANET are more without difficulty attacked than wired community. We can distinguish two varieties of attack: the passive assaults and the active assaults. A passive assault does now not disrupt the operation of the protocol, however attempts to find out valuable records by paying attention to visitors as an alternative, an active assault injects arbitrary packets and attempts to disrupt the operation of the protocol in order to restriction availability, benefit authentication, or entice packets destined to different nodes [19]. The routing protocols in MANET are quite insecure due to the fact attackers can without difficulty gain records approximately community topology.

### 4.1 Passive Attacks

In Passive assaults, attacker don't damage any records within the network as opposed to it he examine network traffic like perceive communicating nodes, observe records which is exchanged between them and steal treasured records. A passive assault tries to research or employ facts from the network. In passive attacks, attackers don't disrupt the operation of routing protocol, but best attempt to discover treasured data by way of being attentive to the routing site visitors [20]. The attacker handiest looks and watches the transmission and does not try and modify or alternate the records packets. Detection of those assaults is difficult since the operation of network itself does now not get affected. Passive assaults are done the eavesdropping, traffic evaluation and monitoring operations.

### 4.2 Active Attacks

The active assaults actively adjust the statistics consisting of message adjustments, message replays and message fabrications. It disrupts normal capability of the community. Active assaults consist in perturbing the algorithm procedure to obtain a strange behavior and/or an erroneous computation result that may be exploited to get better completely or partly the secrets [21].

### 4.3 External Attacks

This type of attacks Contains attacks launched by a node that do not belong to the logical network, or is not allowed to get to it. This type of node penetrates the network area to release its assault.

### 4.4 Internal Attacks

This category includes attacks launched by an internal compromised node, it's far a more several kind of risk to the community because the proposed defense toward external attacks is useless against compromised and inner malicious nodes.

A MANET presents network connectivity between mobile nodes over doubtlessly multihop wireless channels especially thru hyperlink-layer protocols that ensure one node connectivity, and community layer protocols that expand the connectivity to a several of nodes. Those allotted protocols typically assume that each one nodes are cooperative in the coordination operation. This assumption is regrettably no longer genuine in an antagonistic environment [22]. Due to the fact cooperation is believed but now not enforced in MANETs, malicious attackers can without difficulty disrupt network operations by violating protocol specs.

## 5. Secure Ad-hoc Routing

The secure ad hoc routing protocols take the proactive approach and enhance the existing ad hoc routing protocols, such as DSR and AODV, with security extensions. In these protocols, each mobile node proactively signs its routing messages using the cryptographic authentication primitives described above. This way, collaborative nodes can efficiently authenticate the legitimate traffic and differentiate the unauthenticated packets from outsider attackers [23]. However, an authenticated node may have been compromised and controlled by the attacker. Therefore, we have to further ensure proper compliance with the routing protocols even for an authenticated node. In the following, we describe how different types of routing protocol are secured.

The protected MANET protocols take the proactive technique and enhance the current MANET protocols, which consist AODV and DSR with protection extensions. In these protocols, every cellular node proactively symbols its routing information, by using the cryptographic authentication primitives. This way, collaborative nodes can efficaciously authenticate the legitimate site visitors and differentiate the unauthenticated packets from outsider attackers. But, an authenticated node may also were compromised and managed by the attacker [24]. Consequently, we ought to in addition make certain right compliance with the routing protocols even for an authenticated node.

## 6. Conclusion

A MANET carries self-configuring, self-organizing and self-running nodes, every of them communicates with other nodes at once, without any assist of centralized management or fixed infrastructure, inside transmission variety of nodes. Protect and effective conversation within a MANET, an efficient protocol is required to find out routes between cellular nodes. The ordinary goal of these protocol is to provide higher efficient strength aware and cozy routing schemes to MANET. On this paper, we try to explain for the MANET routing protocol and security threats inside the wireless network. Because of movability of nodes in MANET the safety desires are much better than as contrast to traditional wired network. For the duration of the survey, we mentioned how the attack has been took place inside the MANET network. To conclude, the safety is mobile ad hoc community is a complex and puzzling topic.

## 7. References

1. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan, A Local Intrusion Detection Routing Security over MANET Network, IEEE International Conference on Electrical Engineering and Informatics (ICEEI), 2011.
2. Fan Bai, Sadagopan N, Krishnamachari B, Helmy A. Modeling Path Duration Distributions in MANETs and Their Impact on Reactive Routing Protocols, IEEE journal on selected areas in communications. 2004; 22(7).
3. Alex Hinds, Michael Ngulube, Shaoying Zhu, Hussain Al-Aqrabi. A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology. 2013; 3(1).
4. Luo Junhai, Ye Danxia, Xue Liu, Fan Mingyu. A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks, IEEE Communications Surveys & Tutorials. 2009; 11(1).
5. Xiaoyan Hong, Kaixin Xu, Mario Gerla. Scalable Routing Protocols for Mobile Ad Hoc Networks, IEEE Network. 2002; 16(4).
6. Chethan Chandra S Basavaraddi and Geetha N.B., Current Project Work on Routing Protocols for MANET: A Literature Survey, International Journal of Scientific & Engineering Research. 2012; 3(5).
7. Muralishankar VG, Dr. George E, Dharma Prakash Raj, "Routing Protocols for MANET: A Literature Survey", International Journal of Computer Science and Mobile Applications. 2014; 2(3).
8. Sunil Taneja, Ashwani Kush. A Survey of Routing Protocols in Mobile Ad Hoc Networks, International Journal of Innovation, Management and Technology. 2010; 1(3).
9. Dinesh Singh, Ashish K. Maurya Anil K. Sarje, Comparative Performance Analysis of LANMAR, LAR1, DYMO and ZRP Routing Protocols in MANET using Random Waypoint Mobility Model, 3rd International Conference on Electronics Computer Technology (ICECT). 2011; 6.
10. Vijaya Kumar G, Vasudeva Reddyr Y, Dr. Nagendra M. Current Research Work on Routing Protocols for MANET: A Literature Survey, International Journal on Computer Science and Engineering (IJCSE). 2010; 2(3).
11. Ashwani Garg, Vikas Beniwal, A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering", Vol. 2, Issue 9, September 2012.
12. Tarek Sheltami & Hussein Mouftah, "A Comparative study of On-Demand & Cluster –Based Routing Protocols in MANETs, in IEEE, 2003.
13. Misra R. Manda CR. Performance Comparison of AODV/DSR On-Demand Routing Protocols for Ad Hoc Networks in Constrained Situation, IEEE ICPWC, 2005.
14. Azni AH, Rabiah Ahmad, Zul Azri Mohamad Noh, Farida Hazwani and Najwa Hayaati, Systematic Review for Network Survivability Analysis in MANETS", Procedia - Social and Behavioral Sciences. 2015; 195.
15. Gupta V, Krishnamurthy S, Faloutsos M. Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, IEEE MILCOM, 2002.
16. Hu YC, Perrig A, Johnson DB. Wormhole Attacks in Wireless Networks. IEEE J Sel. Area Comm. 2006; 24:370-380.
17. Ghosekar P, Katkar G, Ghorpade P. Mobile Ad Hoc Networking: Imperatives and Challenges," IJCA Special Issue on MANETs. 2010; 3:153-158.
18. Arma Amir Mehdi. Performance Evaluation with Throughput, Packet Delivery on Routing Protocols in MANETs", in: International Journal of Advanced Research in Computer Science and Software Engineering. 2016; 6(2).
19. Parasher R. Rathi Y. A AODV: A Modern Routing Algorithm for Mobile Ad-Hoc Network" in: International Research Journal of Engineering and Technology (IRJET). 2015; 2(1), e-ISSN: 2395-0056, p-ISSN: 2395-0072.
20. Vajed M, Jamali S. Performance Comparison of AODV, DSDV, DSR and TORA Routing Protocols in MANETs" in: International Research Journal of Applied and Basic Sciences. 2012; 3(7):1429-1436.
21. Kumar GV, Reddyr YV, Dr. Nagendra M. Current Research Work on Routing Protocol for MANET: A Literature Survey", in: International Journal on Computer Science and Engineering (IJCSE). 2013; 2(3).
22. Nachammai M, Radha N. Survey on Black Hole and Gray Hole Attacks in MANET", International Journal of Computer Sciences and Engineering. 2016; 4(5):66-70.
23. Pal L, Sharma P, Kaurav N, Mewada SL. Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks", International Journal of Scientific Research in Network Security and Communication. 2013; 1(1):1-4.
24. Mawada S, Singh UK, Sharma P. A novel security based model for wireless mesh networks, Int. J Sci. Res. Network Security and Communication. 2013; 1(1):11-15,.