A Comparative Study on Security Features in MANETs Routing Protocols

Dr. Israa Tahseen Al-attar[1]

[1]Department of Computer Science, University of Technology, Baghdad, Iraq

e-mail: israa80atar@yahoo.com

Received: 5/ 6 /2014

Accepted: 21 /1 /2015

Abstract – Mobile Ad Hoc Network (MANET) is a collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. MANETs has a wide range of applications, ranging from mobile phone application to military applications. As the application of MANETs increases, the attacks on MANETs also increase. Due to mobility of nodes, frequent link breakage carry out, and it's widely use, MANET's routing is considered as a challenging job. A vast range of research is being conducted to keep routing in MANETs robust and secure. One of the major research areas is routing privacy. This paper presents a description of routing protocols that have the major challenges in ad hoc networks with a particular focus on their characteristics, functionality, and security features and makes their comparative analysis. Further, this study will help the researchers to get an overview of the existing protocols and suggest which protocols may perform better with respect to varying network scenarios.

Keywords – MANET, routing protocol, Reactive, Proactive, security, privacy.

1. Introduction

The wireless network can be classified into two types: Infrastructured and Infrastructure-less [1]. In Infrastructured wireless networks, the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station [2]. In Infrastructure-less or Ad hoc wireless network, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act both as a router and as a host. The mobile nodes in the Ad hoc network dynamically establish routing among themselves to form their own network.

Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: nodes A, B, C, D, E, and F constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a) where nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken and the network topology changes to the one in (b). However, the network is still connected, because A can reach D through C, E, and F.

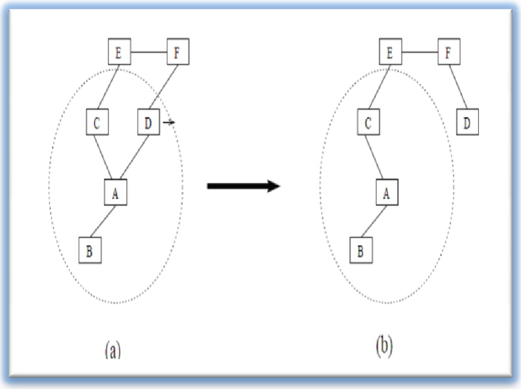

Figure 1. Topology change in ad hoc networks

The random and rapid motions of MANETs require that the nodes always find new routes. Several routing protocols have been proposed to meet the requirements of MANETs. When MANETs are being used in military operations, other issues of security also rise. Securing routing creates particular difficulties, since these networks have neither centrally administrated secure routers nor strict policies of use. Thus the aim is to study the security measures that can be included into routing which can keep the node identity safe from the adversary and also provided for routing of packets without much difficulty. Military tactical and other security-sensitive operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions [3].

2. Routing Protocol and its Classification

Routing is a process of sending a message from one mobile node to another in the network (it is also called unicast). Routing protocols for mobile ad hoc wireless networks normally call for mobility management and scalable design. The mobility management is done by exchanging the information between moving hosts in the ad hoc wireless network. Generally, when the frequent information exchanges occur, the network maintains accurate information of host locations and other relevant information. However, frequent information exchanges consume communication resources including bandwidth and power, so that it can be costly. With less frequent information exchanges, these costs decrease but there is more uncertainty about the location of host. Scalable design which works for large size networks requires both routing protocols and resource consumptions to be scalable. Routing in MANET poses special challenges because of its infrastructure-less network and its dynamic topology. Wired network uses traditional routing protocols, that generally use either link state or distance vector, but these protocols are not suitable for ad hoc wireless networks. In an environment, where mobile hosts work as routers, the network topology changes dynamically, hence the process could be expensive due to low bandwidth. A routing protocol is required, whenever a packet needs to be communicated via several nodes to arrive at its destination. A routing protocol is necessary to find a route for packet delivery and make the packet delivered to the correct destination.

The highly dynamic natures of the mobile nodes create frequent and unpredictable network topology changes. This topology change increases the routing complexity among the mobile nodes within the network. Therefore, traditional routing algorithms are not sufficient to the successful routing in MANET. Routing in a MANET depends on many other factors including topology, selection of routers, and location of request initiator and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. This makes the routing area perhaps the most active research area within the MANET domain. Especially over the last few years, numerous routing protocols and algorithms have been proposed and their performance under various network environments and traffic conditions closely studied and compared [4].

As shown in Figure 2, the classification is based on the mechanism of routing information that used to route packets. The emphasis in this paper is concentrated on the comparison of various On-Demand/Reactive and Table-Driven/Proactive Protocols based on their routing methodology, security features and other network characteristics.

In Table-Driven ***/Proactive*** routing protocols each node sends periodic beacon messages spreading information of the neighboring nodes. Thus, routes are stored in the routing table, and when there is a need to communicate, an appropriate route is selected from the routing table and packets are routed. Each node maintains one or more tables containing routing information to every other node in the network. All nodes are updating these tables to maintain latest view of the network. Some of the table driven or proactive protocols are listed as follows: OLSR, SPAAR and ALARM. All these protocols are quite insecure because attackers can easily obtain information about the network topology [5].

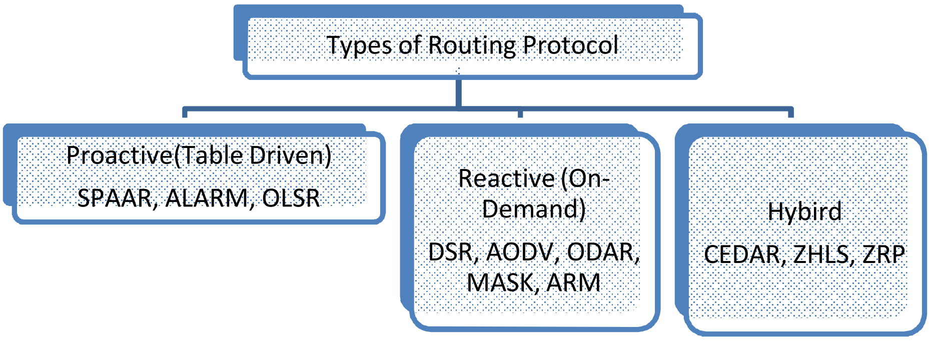

Figure 2. Shows the categories of Ad hoc Routing Protocols and various Protocols under each category

- **On-Demand/*Reactive*** Protocols: In these protocols, routes are created only when they are needed. While a transmission starts from source to destination, the route discovery procedure is initiated. The route remains valid until the route is no longer needed. Some of the on-demand routing protocols are listed as follows: DSR, AODV, ODAR, MASK and ARM [6].
- **Hybrid Protocols**: Hybrid protocols make use of both reactive and proactive protocols features to balance the delay which was the disadvantage of Table driven protocols and control overhead (in terms of control packages). Main feature of Hybrid Routing protocol is that the routing is proactive for short distances and reactive for long distances. The common disadvantage of hybrid routing protocols is that the nodes have to maintain high level topological information which leads to more memory and power consumption. Different Types of Hybrid Routing Protocol are: ZRP (Zone Routing Protocol), CEDAR (Core Extraction Distributed Ad Hoc Routing) [5].

3. Routing Security in MANET

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Attacks against MANET can be classified into passive and active attacks. A ***passive attack*** does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic, which makes it very difficult to detect. An ***active attack*** is an attempt to improperly modify data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Active attack can be further divided into external attacks and internal attacks. An ***external attack*** is one caused by nodes that do not belong to the network. An ***internal attack*** is one from compromised or hijacked nodes that belong to the network.

Internal attacks are typically more severe, since malicious nodes already belong to the network as authorized parties. Therefore, such nodes are protected with the network security mechanisms and underlying services. Next, some types of attacks will be described which are performed against a MANET [7]:

3.1. Wormhole Attack

In wormhole attack is one of the most complicated attacks in MANETs mainly for reactive type of routing protocols. In this type of attack a pair of malicious nodes creates tunnel between two groups of nodes. One malicious node receives the packet from the one end and tunnels them to another location in the network. The tunnel between two malicious nodes is called wormhole. It could be reputable through a single long range wireless link.

The attacker nodes may create a wormhole even for the packets which are not addressed to itself because of the broadcast nature of MANETs.

3.2. Packet Replication Attack

In packet replication attack an attacker replicate stale packet. This consumes battery power resources available to the nodes and their additional bandwidth.

3.3 Denial-of Service Attack

A Denial-of Service Attack is one of the attacks in MANETs that affects proactive type routing protocols. The main goals of this type of attack are:

1) Modifying the packet header.
2) Inducing Junk packets into the network.
3) Routing table overflow.

Denial-of-service attacks can essentially disable your computer or your network. They come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- Consumption of scarce, limited, or nonrenewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

3.4. Byzantine Attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior.

3.5. Blackhole Attack

Blackhole Attack is one of the major attacks in MANETs mainly for proactive & reactive type of routing protocols. A malicious node provides fake routing information by advertising itself having shortest path to the source node. When malicious node receives the route request to the destination node, it sends a reply consisting of a definite shortest route. If the reply request sent by the malicious node it reaches the source node before the reply from the genuine node. As the malicious node able to insert itself between the genuine communicating nodes, it will be able to drop or can change the destination address of the packets passing through them.

3.6. Gray-hole Attack

This attack is also known as routing misbehavior attack. It leads to messages dropping. It has two phases. In the first phase a valid route to destination is advertise by nodes itself. In second phase, with a certain probability nodes drops intercepted packets.

4. Routing Protocols in MANET

The following subsections present a few existing routing protocols in MANETs, and how routing protocols have evolved to provide security. A few reactive and proactive protocols have been discussed and location based routing protocol has also been mentioned.

a. OLSR

Clausen and Jacquet proposed the Optimized Link-State Protocol, a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying. It optimizes the pure link state routing protocol. Optimizations are done in two ways: by reducing the size of the control packets and by reducing the number of links used for forwarding the link state packets. Here each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. OLSR is based on the following three mechanisms: neighbor sensing, efficient flooding and computation of an optimal route using the shortest-path algorithm. Neighbor sensing is the detection of changes in the neighborhood of node. Each node determines an optimal route to every known destination using this topology information and stores this information in a routing table. The shortest path algorithm is then applied for computing the optimal path. Routes to every destination are immediately available when data transmission begins and remain valid for a specific period of time till the information is expired [8].

All nodes in OLSR need to maintain a consistent view of the network topology. They are also vulnerable to a number of disruptive attacks in the presence of malicious nodes (identity wormhole attack and Black hole attack). As a result, this drawback is solved by a security mechanism based upon signing each OLSR control packet with a digital signature for authenticating the messages. The digital signature is based on symmetric keys.

b. SPAAR

Secure Positions Aided Ad-hoc Routing, as the name suggest implements routing based on location of the nodes in the network. SPAAR is an on demand routing protocol. In the Route request along with the destination ID also the distance from the source node and the exact coordinates are included, all the information is encrypted with a group encryption key. The receiving node attempts to decrypt, successful nodes indicate that sending node is a one hop neighbor. Then the intermediate nodes checks to see if it or any of its neighbors is closer to the destination, if it so it forwards the route request with addition of its ID and its distance to the source. The route cache is maintained for reverse path. The route reply contains the RREQ sequence number, destination's coordinates, velocity, and a timestamp, all encrypted with public key. Fabricated routing messages cannot be injected into the network by malicious nodes, routing messages cannot be altered in transit and routing loops are not formed. SPAAR suffers from a lot of overhead need to encrypt and decrypt at each and every node. It also needs an online server to provide nodes with certificate [9].

c. ALARM

ALARM is a table driven protocol, which implements security and privacy with the aid of location based routing. The presence of group signature ensures that only valid members who have registered with the group manager can decrypt and read the packets. The protocol initially sends out Location Announcement Messages (LAM) to inform all the nodes of the network topology from time to time. The LAM messages contain the nodes current position, a time stamp and a key which will be later used as a session key. Also each node has a pseudonym, which is the nodes temporary ID defined by the node's current location concatenated with its Group signature .The routes are saved in the routing table. The source node encrypts the data packets with its Session key from the LAM message [10].

d. AODV

The Ad Hoc On-Demand Distance Vector routing protocol was suggested by C.E. Perkins. It is a reactive protocol, and works to minimize the requirement of system-wide broadcasts to its extreme. The AODV protocol has three phases, the route discovery phase, the route reply phase and the route maintenance phase. In the route discovery phase, when a source wants to initiate transmission with another node as destination in the network, AODV broadcasts a RREQ packet as a control messages to find a route to the destination node in the network. The neighboring nodes in turn broadcast to their neighbors and the process continues until it reaches the destination. It will provide topology information (like route) for the node. The node of network needs a connection broadcasts and request for connection. During the process of forwarding the RREQ, intermediate nodes records the address of the neighbor from which packets received while broadcasting. This route information is stored in route tables, which helps for establishing reverse path. If additional copies of same RREQ are received later it simply discards it. Then reply RREP is sent using reverse path. Once the communication is over the route is discarded from the route table of the nodes. The Route Error (RERR) message is sent to notify the source if the link to any intermediate node is broken. This broken link is detected by nodes periodically sending hello messages. Figure 3 shows the route discovery phase.

For Route Maintenance phase, when a source node moves, it can re-initiate a route discovery process. If any intermediate node moves with in a particular route, the neighbor of the drifted node can detect the link failure and sends a link failure notification to its upstream neighbor. After receiving the failure notification, source again re-initiate a discovery phase.

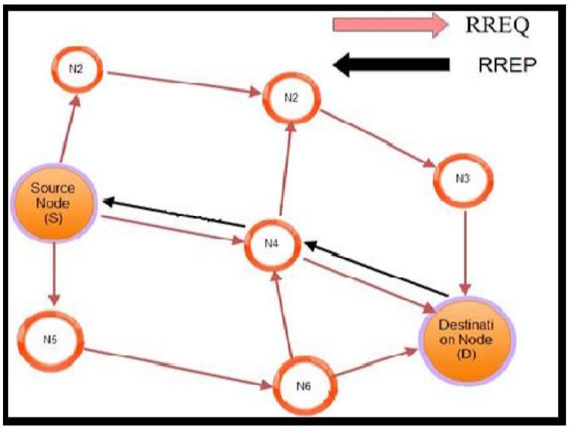

Figure 3 AODV Route Discovery

A security extension is applied to AODV using one-way hash functions to serve metric fields in Route Request (Route Discovery). He introduced Secure-AODV (SAODV) where he suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. It is used to protect Route Discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation [11]. AODV does not repair a broken path locally. When a link breaks, which is determined by observing the periodical beacons or though ACK messages, the source and the destination nodes are notified (end nodes). The source node then reestablishes the route with the destination using higher layers. AODV does not provide any type of security.

The advantages of this protocol are, nodes need to store only active routes, reduction in the memory requirements, breakage in the links are detected soon and acted upon, quick responses to link breakage in active routes, loop free routes, can be used with a large number of nodes.

e. DSR

The Dynamic Source Routing protocol is a simple and efficient routing protocol, which was designed specifically for use in multi-hop wireless ad-hoc networks of mobile nodes. It was designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table update messages required in the proactive routing protocols. Without the need for any existing network infrastructure or administration, DSR allows the network to be completely self-organizing and self-configuring. DSR uses source-based routing means that the source must know the complete hop sequence to the destination. A route cache is maintained by each node. Only if the desired route cannot be found in the route cache, the route discovery process is initiated [12].

The protocol uses two main mechanisms of Route Discovery and Route Maintenance, works together to allow nodes to discover and maintain routes to destinations in the ad-hoc network. Route discovery phase floods the network with RREQ packet if a suitable route is not available in the route cache. A RREQ message includes the senders address, the target address, a unique number to identify the request and a route record listing the addresses of each intermediate node through which the RREQ is forwarded. On receiving RREQ packet, the destination replies to the originator with a RREP packet. DSR uses a source routing strategy to generate a complete route to the destination, this will then be stored temporarily in nodes route cache [13]. DSR addresses mobility issues through the use of packet acknowledgements. Failure to receive an acknowledgement causes packets to be buffered and route error messages to be sent to all upstream nodes. Route error messages trigger the route maintenance phase which removes incorrect routes from the route cache and undertakes a new route discovery phase [14]. Figure 4 shows how neighboring nodes overhear on bidirectional links, and maintain a cached copy of the route for further use. As depicted in Figure 4 Source node N1 floods the request in the network. Node N2 observes the request and caches the route for future reference.

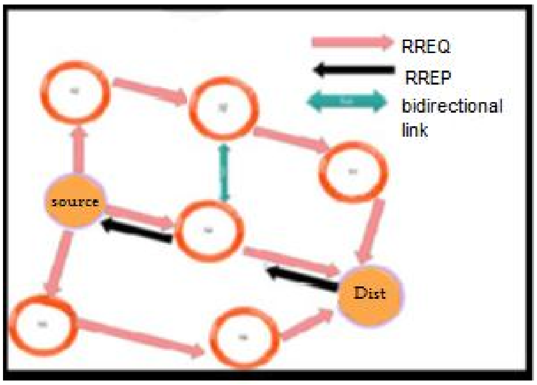

Figure 4 DSR Routing Table updates

The age information of the entry is maintained in the node, so it is useful to know whether the cache is fresh or not. It first checks whether the packet is belongs to it or not when a data packet is received by any intermediate node. If it is meant for itself (i.e. the intermediate node is the destination), then the corresponding packet is received otherwise the same will be forwarded using the path attached on the data packet

The advantages of DSR are that intermediate nodes can learn routes from the source routes in the packets they receive, and there is no need to keep routing table so as to route a given data packet as the entire route is contained in the packet header. Generally, finding a route is a costly operation in terms of time, bandwidth and energy, hence this is a strong argument for using source routing. The limitations of DSR protocol are lack of security and increase of packet size. And it is not scalable to large networks and even requires significantly more processing resources than most other protocols. Each node must spend lot of time to process any control data it receives to obtain the routing information, even if it is not the intended recipient [14].

f. ODAR

On-Demand Anonymous Routing makes use of bloom filters to achieve strong anonymity against attacks such as address spoofing and route forgery, by concealing the true identity of the traffic. Bloom filters are data structure which store a set of elements, and test whether an element is a member of the set or not. Elements once added to a bloom filter cannot be removed. ODAR initially finds the source route using DSR algorithm. The source hashes the entire route information and puts it into the bloom filter; which is then attached to the packet and forwarded. Figure 5 illustrates the packet forwarding in a network. Where the *Mtpye* indicates the data to be sent, *bSize* is the size of the bloom filter and *bDest* contains the hashed value for each intermediate node. Each intermediate node will check for its ID in the bloom filter, if present it will forward he packet else will drop the packet. Fig 5, depicts how the route information is hashed and stored in bloom filters. This algorithm provides three levels of anonymity, node identity is kept anonymous, route details are also anonymous and topology information is also not revealed. When using bloom filters, the possibility of false positives leads to unnecessary packet forwarding. Nodes on the source path can inject packets into the network [15].

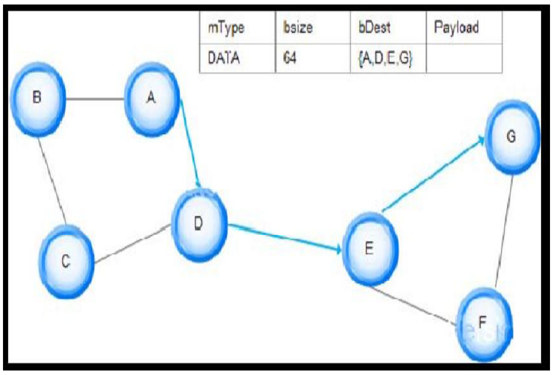

Figure 5 ODAR use of Bloom filters

g. MASK

Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK) is a routing protocol suggested by Yanchao Zhang, Liu, Wenjing Lou, and Yuguang Fang, in [16]. This protocol tries to masks the identities of nodes by the use of pseudonyms each node belongs to a group and each node has a set of predefined pseudonyms. When a node wishes to communicate first it authenticates the neighboring node by sending a challenge to the node along with a randomly chose pseudonym. The challenged node calculates the master session key and send authentication back. Both generate link IDs and session keys based on the master session key. Thus in MASK node identities are secured. MASK guarantees anonymity of senders, receivers and sender-receiver relationships. Also ensure end-to-end flow cannot be tracked. It is also resilient to a wide range of attacks. The Route request message is clearly mentions the final destination ID.

h. ARM

Anonymous Routing Protocol for Mobile ad hoc networks. This protocol proposed by Stefaan Seys and Bart Preneel in [17], aims at overcoming the draw backs of ASR [18], ANODR [19], SDAR [20] and MASK [16]. The RREQ message is formed such that only the destination can recognize that RREQ was targeted at it, all other nodes can only verify that it was not targeted at them. The source *S* and destination *D* shared a secret key *kSD* and *D* has a current pseudonym which only D can be recognized. Intermediate nodes verified if the RREQ was targeted to them or not with the help of the pseudonym. The RREP message from the destination is encrypted with the broadcast ID of *D*. The cryptographic operations are simple and done only by the source and destination node. Intermediate nodes do not need complex operations to decide if the message was targeted to them. ARM maintains privacy of the destination node's identity. ARM depends on various assumptions which may not be plausible in a real-time environment, some of the assumptions are, that every node has a permanent ID know by all other node, source and destination share a secret key and a secret pseudonym and that links between nodes are symmetric.

5. Comparison Table

A comparison table (Table 1) of the protocols based on the various security and privacy techniques is presented.

Table 1 Protocol Comparison Table

	OLSR	SPAAR	ALARM	AODV
category	proactive	Proactive	proactive	reactive
scalable	No	Yes	Yes	No
Encryption method	Packet Signature	Third party certificates	Group signature	Nil
Privacy	Packet privacy	Nil	Node and communication privacy	Nil
Routing table	Selected 2-hop neighbor information	Node public/private keys and certificates	Topological Information	Next hop information, not the entire
Message overhead	Low	Medium	Moderate	High
Periodic broadcast	possible	Needed when the topology changes	possible	No
Advantage	Reduces flooding overhead	Provides security	Rapid route finding	Detect link failure
Disadvantage	Exposes network topology	Require on-line location server	Eposes Topology Information	No security and privacy

Table 1 Continued

	DSR	ODAR	MASK	ARM
category	reactive	reactive	reactive	reactive
scalable	No	No	Yes	Yes
Encryption method	Nil	Public/ private key encryption	Group signature	Nil
Privacy	Nil	Nil	Pairing based cryptography	Secret key and Pseudonym
Routing table	Entire Route Information	Hashed value of node identities	• Forwarding route table: Destination ID, Sequence number, pervious link and next link • Reverse route table: Destination ID, Sequence number, prehop- pseudonym • Target LinkID table: LinkIDs shared with neighbors.	Pseudonyms of next hop neighbor
Message overhead	Low	Moderate	High	Low
Periodic broadcast	No	possible	No	possible
Advantage	Faster route recovery	Provides anonymity and using of bloom filters	It can withstand a variety of attacks	Provides node identity security
Disadvantage	No security and privacy	Require on-line public key destination server	Contains the final destination in each RREQ message	Assumes that each authorized source-destination pair pre-shares a unique symmetric key

6. Conclusion

In this research, an effort has been made to concentrate on the comparative study of various routing protocols on the basis of the above mentioned parameters (see table 1). The main differentiating factor among the protocols is the ways of finding and maintaining the routes between source destination pairs. It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized characteristics, security and power awareness is hard to achieve in mobile ad-hoc networks. By observing table 1, it is found that:

- Each routing protocol has unique features. AODV has maximum throughput under low traffic. As network becomes dense OLSR, DSR perform well in terms of Throughput than AODV.
- The comparison between the routing protocols indicates that the design of a secure ad-hoc routing protocol constitutes a challenging research problem against the existing security solutions. At last the overall characteristic features of all routing protocols have been provided and described which one of the protocols may perform best in large networks.
- Still mobile ad-hoc networks have posed a great challenge for the researchers due to changing topology and security attacks, and none of the protocols is fully secured and research is going on around the globe.
- The basic routing protocols like AODV, DSR and OLSR provide efficient way of route discovery and maintenance but they lack in security. ODAR and ARM are some protocols which have implemented security in various ways, such as the use of pseudonyms, hashed values only transmitted and various encryption algorithms.

Further, this study will helps researchers to get an overview of the existing protocols and suggest which protocols may perform better with respect to varying network scenarios.

References

[1] A. K. Gupta, H. Sadawarti, and A. K. Verma, “A Review of Routing Protocols for Mobile Ad Hoc Networks, *SEAS Transactions on Communications”*, ISSN: 1109-2742, Issue 11 Vol.10, November 2011, pp. 331-340.

[2] Sunil Taneja and Ashwani Kush “A survey of Routing Protocols in Mobile Ad Hoc Networks” , International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248.

[3] Umang Singh “Secure Routing Protocols in Mobile Ad hoc Network-A Survey and Taxonomy” International Journal of Reviews in Computing 30th September 2011. Vol. 7.

[4] Dr. Shuchita Uphadhyaya & Anil Saini “Improving the Quality of CGSR Routing Protocol by Electing Suitable Cluster-Head Using Fuzzy Logic System in MANET” International Journal of Advanced Research in Computer Science and
Software Engineering , ISSN: 2277 128X Vol. 6, Issue-3, June 2013.

[5] Zehua Wang, Yuanzhu Chen and Cheng Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 63, no. 2, February 2014.

[6] Robinpreet Kaur & Mritunjay Kumar Rai “A Novel Review on Routing Protocols in MANETs”, Undergraduate Academic Research Journal (UARJ), ISSN : 2278 –

1129, Volume-1, Issue-1, 2012.

[7] Kaur Sharndeep, Gupta Anuj " A review of Different Secure Routing Protocols and Security Attacks in Mobile ad hoc Networks", International Journal of Advanced Engineering Topology, 2014

[8] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", INRIA, October 2003.

[9] S. Carter and A. Yasinsac, “Secure position aided ad hoc routing,” Proc. IASTED International Conference on Communications and Computer Networks (CCN02), pp. 329–334, 2002.

[10] K. El Defrawy and G. Tsudik, “Alarm: Anonymous location-aided routing in suspicious MANETs,” IEEE ICNP 2007, pp. 304–313, Oct. 2007

[11] Seema Vilas Bhujade, Prof. S. D. Sawant, "Evaluation AODV, DSR and DSDV Protocol of MANET by USING NS-2‖, IJET, Volume 4 Issue 8- August 2013.

[12] D. B. Johnson, D.A. Maltz and J. Broch, "DSR: the dynamic Source Routing Protocol for Multi-hop wireless ad hoc Networks" in the ad hoc networking. Addison-Wesley, 2001 pp. 139-172.

[13] D. GEETHA, T. SARIKA, "Performance Analysis of TORA & DSR Routing Protocols in Mobile Ad-hoc Networks", IJECSE, Volume 2, Number 1, 2013.

[14] D. Johnson and Y. Hu, D. Maltz, "The Dynamic Source Routing (DSR) for Mobile ad Hoc Networks for IPv4", Microsoft Research, February 2007.

[15] D. Sy, R. Chen, and L. Bao, “Odar: On-demand anonymous routing in ad hoc networks,” Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on, pp. 267–276, Oct. 2006.

[16] Y. Zhang, W.Lou, and Y. Fang, "Mask: anonymous on-demand routing in mobile ad hoc networks", IEEE trans. Wireless communication, vol.5, no 9, 2006

[17] S. Seys and B. Preneel, "Arm: anonymous routing protocol for mobile ad hoc networks", International Journal vol. 3, no. 3, 2009

[18] B. Zhu, Z, Wan. Kankanhalli, F. Bao and R. Deng. , " Anonymous secure routing in ad hoc networks", proceeding of the 29th annual IEEE International Conference on local computer networks, 2004

[19] J. Kong and X. Hong, "ANODR: anonymous on-demand routing with untraceable routes for mobile ad hoc networks", Proceeding of the 4th ACM International Symposium on Mobile ad hoc networks, 2003

[20] Aa. Boukerche, K. El-Khatib, L. Xu and L. Korba, "A nobel solutionfor achieving anonymity in wireless ad hoc networks", Proceeding of the 1st ACM, 2004