Review of Security Approaches in Routing Protocol in Mobile Adhoc Network

Sumati Ramakrishna Gowda
Research Scholar
Vinayaka Missions University, Salem, India

P.S Hiremath
Department of Computer Science.
Gulbarga University, Gulbarga, India

***Abstract*— In this paper the objective is to present a review of routing protocols in mobile ad hoc network (MANET) exclusively from security viewpoint. In MANET, the mobile nodes often move randomly for which reason the cumulative network experiences rapid and much unpredictable topology alterations. Due to presence of dynamic topology as well as limited range of transmission, very often some nodes cannot communicate directly with each other. Because of this phenomenon, all the QoS and security issues surface. Till now there is abundant literature work being formulated towards designing routing protocols. But security features designed till now are not able to provide optimal security towards secure routing. Routing protocols, data, bandwidth and battery power are the common target of the attackers. Therefore, in this paper the attempts are to throw light on the work that were focused exclusively for maintaining security in routing protocols in MANET**

Keywords-component: Routing, MANET, security

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected wirelessly [1]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [2]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network. Therefore, this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [3]:

- Unreliability of wireless links between nodes: Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
- Constantly changing topology: Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly. The nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
- Lack of incorporation of security features that exist in statically configured wireless routing protocol and are not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate security in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities that exist in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks. In such an environment, there is no guarantee that a path between two nodes would be free of malicious nodes, which would not comply with the employed protocol and attempt to harm the network operation. The mechanisms currently incorporated in MANET routing protocols cannot cope with disruptions due to malicious behavior. For example, any node could claim that, it is one hop away from the sought destination, which is causing all routes to the destination to pass through itself. Alternatively, a malicious node could corrupt any in-transit route request (reply) packet and cause data to be misrouted. The presence of even a small number of adversarial nodes could result in repeatedly compromised routes, and, as a result, the network nodes would have to rely on cycles of time-out and new route discoveries to communicate. This would incur arbitrary delays before the establishment of a non-corrupted path, while successive broadcasts of route requests would impose excessive transmission overhead. In particular, intentionally falsified routing messages would result in a denial-of-service (DoS) experienced by the end nodes. The proposed scheme combats such types of misbehavior and safeguards the acquisition of topological information. Section 2 discusses about the preliminary study of the survey of literature on the domain followed by security issues in Section 3. Related work is discussed in Section 4, while MANET routing security is examined in Section 5 and briefing on other routing protocols in Section 6 and 7. Section 8 illustrates about scope of future research, with concluding remarks in Section 9.

II. PRELIMINARY STUDY

In MANETs, some form of routing protocol is required in order to dynamically detect the multi-hop paths through which packets can be sent from one node to another. Active research

work on MANETs is carried out mainly in the fields of Medium Access Control (MAC), routing, resource management, power control, and security. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of MANET routing protocols have been proposed in the last few years. Considering the special properties of MANET, many routing protocol, generally the following properties are expected, though all of these might not be possible to be incorporated in a single solution.

- A routing protocol for MANET should be distributed in a manner in order to increase its reliability.
- A routing protocol must be designed considering unidirectional links, because wireless medium may cause a wireless link to be opened in uni-direction only due to physical factors.
- The routing protocol should be power-efficient.
- The routing protocol should consider its security.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A routing protocol should be aware of Quality of Service (QoS).

There are basically two categories of routing protocols for MANETs:

1. Table Driven (Proactive): DSDV, GSR, WRP
2. Source Initiated On-Demand (Reactive): ABR, AODV, DSR, LAR

Based on the method of delivery of data packets from the source to destination, the classification of MANET routing protocols could be done as follows:

- Unicast Routing Protocols: The routing protocols that consider sending information packets to a single destination from a single source.
- Multicast Routing Protocols: Multicast routing is the delivery of information to a group of destinations simultaneously, using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split. Multicast routing protocols for MANET use both multicast and unicast for data transmission.

Multicast routing protocols for MANET can be classified again into two categories: Tree-based multicast protocol and Mesh-based multicast protocol. Mesh-based routing protocols use several routes to reach a destination, while the tree-based protocols maintain only one path.

Much of the research has been done focusing only on the efficiency of the MANETs. There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirement of these protocols has changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols. MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), and Secure Routing Protocol (SRP). Although researchers have proposed several secure routing protocols, their resistance towards various types of security attacks and efficiency have been primary points of concern in implementing these protocols. Hence, there is a need for review. In a MANET, attacks can be classified into Passive Attacks and Active Attacks, which are discussed below.

A. Passive Attacks

In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. The attacker only looks and watches the transmission and does not try to modify or change the data packets. Two types of passive attacks are possible:

- Traffic analysis: In this attack, attacker monitors packet transmission to infer important information such as a source, destination and source-destination pair.
- Eavesdropping: In Eavesdropping, attackers obtain some confidential information e.g. private key, public key, location or even password of the node that should be kept secret during transmission.

B. Active Attacks

In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks. Various types of active attacks are:

- Sinkhole Attack: A sinkhole node tries to attract the data toward itself from all neighboring nodes. In this attack, a malicious node generates fake routing information and show itself as legal nodes for the route. Sinkhole node attempts to regulate all network traffic according to itself, modifies the data packets, decrease the network life time, create complicated network topology and finally destroy the network.
- Flooding Attack: In this attack, a malicious node may also inject false packets to consume the available resources onto the network, so that valid user can not be able to use the network resources for valid communication. The flooding attack is possible in most of the on demand routing protocols such as SRP, SAODV, ARAN etc.
- Replay Attack: This attack usually targets the freshness of routes. In this attack, an attacker firstly records the message and then resend the old message to the other nodes to update their routing table with stale routes.
- Rushing Attack In rushing attack, attacker forwards routing packets as quick as possible to gain access to

multicast forwarding group before the legal node .By this way, rushing attack can slow down the performance of network .The rushing attack can act as an effective DoS attack against all currently proposed on demand MANET routing protocols.

C. Common attacks in MANETs

- Denial-of-service with modified source route: In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service.
- Tunneling Attack: The tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes.
- Wormhole Attack: In wormhole attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them back into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality
- Black hole Attack: In Black hole attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept and in this way it can compromise the service.
- Spoofing Attack: In Spoofing, a single malicious node in the ad hoc network can spoof the nodes identity in order to forward packets through it. Later the information can be used to create DoS attacks.

D. Security Services

Security services include the functionality required to provide a secure networking environment. The main security services can be summarized as follows:

- Authentication: This service verifies a user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each is the entity it claims to be. Secondly, it must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates. Details of the construction and operation of digital signatures can be found in RFC2560.
- Confidentiality: This service ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such as only legitimate users can analyze and understand the transmission.
- Integrity: The function of integrity control is to assure that the data is received in verbatim as sent by authorized party. The data received contains no modification, insertion or deletion.
- Access Control: This service limits and controls the access of such a resource, which can be a host system or an application.
- Availability: This involves making the network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

As the currently available wireless networking and mobile computing hardware is now capable of fulfilling the promise of this technology, it is the need of the hour to design and develop routing protocols which should support the performance with endurance. The correct execution of these routing protocols is mandatory for smooth functioning of a MANET A variety of protocols have been proposed targeted at securing MANETs. The performance comparison of these protocols needs to be analyzed. In the present work, we have compared these protocols by highlighting their features, differences and characteristics. It can be summed up that each protocol has definite advantages and disadvantages, and can be appropriate for a particular application environment. The security in routing protocols addressed in the recent past decade has been discussed in the following sections.

The provision of security services in the MANET context faces a set of challenges specific to this new technology. The insecurity of the wireless links, energy constraints, relatively poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes have been identified. Even if such services were assumed, their availability would not be guaranteed, either due to the dynamically changing topology that could easily result in a partitioned network, or due to congested links close to the node acting as a server. The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and non-trusted. Such a distinction would have been based on a security policy, the possession of the necessary credentials and the ability for nodes to validate them.

Table 1: Exploring Research gap

Performance Parameters	ARAIDNE	ARAN	SEAD	SRP	SAODV	SAR	SLSP	SANEDNA
Type	Reactive	Reactive	Proactive	Reactive	Reactive	Reactive	Proactive	Reactive
MANET Protocol	DSR	AODV/ DSR	DSDV	DSR/ ZRP	AODV	AODV	ZHLS	DSR
Encryption	Sym	Asym	Sym	Sym	Asym	Sym/Asym	Asym	Sym
Synchronization	Yes	No	Yes	No	No	No	No	Yes
Trust Authority	KDC	CA	CA	CA	CA	CA/KDC	CA/KDC	No
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	Yes	No	No	No	Yes	No	Yes
Integrity	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Non-Repudiation	No	Yes	No	No	Yes	Yes	Yes	Yes
Anti-Spoofing	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
DoS Attacks	Yes	No	Yes	Yes	No	No	Yes	Yes

Source: Tarun Dalal, Gopal Singh [4]

III. Security Issues

The buildup of an ad hoc network can be envisaged where support of wireless access or wired backbone is not feasible. Ad hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus, it is obvious that with lack of infrastructure support and susceptible wireless link attacks, security in ad hoc network becomes inherently weak. Achieving security within a MANET is challenging due to following reasons.

- Dynamic Topologies and Membership: A network topology of ad hoc network is very dynamic as mobility of nodes or membership of nodes is very random and rapid. This stipulates the need for secure solutions to be dynamic.
- Vulnerable wireless link: Passive/Active link attacks like eavesdropping, spoofing denial of service, masquerading, impersonation are possible.
- Roaming in dangerous environment: Any malicious node or misbehaving node can create hostile attack or deprive all other nodes from providing any service.

The main issues for providing security in MANET are briefly discussed below.

- Identification issue: Nodes having access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate.
- Before establishing secure communication link, the node should be capable enough to identify another node. As a result, node needs to provide his/her identity as well as associated credentials to another node.
- The delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised.
- Privacy Issue: The identification issue simultaneously leads to privacy issue for MANET Mobile node uses various types of identities and that varies form link level to user/application level. Also in mobile environment very frequent mobile node is not ready to reveal his/her identity or credentials to another mobile node from privacy point of view. Any compromised identity leads attacker to create privacy threat to user device. Unfortunately the current mobile standards do not provide any location privacy and in many cases revealing identity is inevitable to generate communication link. Hence a seamless privacy protection is required to harness the usage of ad hoc networking.

Therefore, due to the issues discussed above, it is essential to provide security architecture to secure ad hoc networking. In the literature, there are many works that address the security issues in MANETs.

IV. Related Work

Panagiotis Papadimitratos et al. [5] have presented a route discovery protocol that is considered one of the standard

works on secure routing in mobile ad hoc networks. John Marshall et al. [6] have proposed the SRP algorithm for routing in ad hoc networks. Oscar F. Gonzalez et al. [7] presented a mechanism that enables the detection of nodes that exhibit packet forwarding misbehavior. Stephan Eichler et al. [8] have introduced a novel secure routing protocol based on AODV for vehicular ad hoc networks. M. Rajesh Babu et al. [9] have proposed to develop an energy efficient secure authenticated routing protocol (EESARP). Steffen Reidt et al. [10] have introduced a trust metric in the cluster head selection process to securely determine constituting nodes in a distributed Trust Authority (TA) for MANETs. Muhammad Nawaz Khan et al. [11] have proposed distributed-ID, a smart agent in each mobile node analyzes the routing packets. Lu Jin et al. [12] introduced the secure the delivery of routing packets and the strategy to determine the most secure routes. Panagiotis Papadimitratos et al. [13] have proposed the securing the delivery of routing packets and the strategy of determine the most secure routes. Shivasharanappa Allur et al. [14] have proposed a cross-layer design to achieve an unswerving data transmission in ADHOC networks. Venkat Balakrishnan et al. [15] introduced Trust Enhanced security Architecture for MANET (TEAM), in which a trust model is overlaid on the following security models key management mechanism, secure routing protocol, and cooperation model.

Kimaya Sanzgiri et al. [16] have introduced solution to one, the managed-open scenario where no network infrastructure is pre-deployed, but a small amount of prior security coordination is expected. Poonam Yadav et al. [17] have introduced the on-demand routing protocols AODV, DSR and DYMO based on IEEE 802.11 and the characteristic summary of these routing protocols are presented. Parma Nand et al. [18] have introduced the on demand routing protocols AODV, DSR and DYMO. David B. Johnson et al. [19] have presented a protocol for routing in ad hoc networks that uses dynamic source routing. Xiaodong Lin et al. [20] have presented a novel anonymous secure routing protocol for mobile ad hoc networks (MANETs). Xu Su et al. [21] have proposed mechanisms to complement the existing secure routing protocols to resist the creation of in-band tunnels. Mohd Anuar Jaafar et al. [22] introduced some evaluation and performance comparisons of AODV, SAODV and A-SAODV routing protocols in MANETs. Umang Singh et al. [23] have introduced various existing routing protocols that were reviewed. Julien Francq et al. [24] have proposed countermeasure that provides a high level of fault detection. Karim El Defrawy et al. [25] have presented the PRISM protocol which supports anonymous reactive routing in MANETs. Satoshi Kurosawa et al. [26] have proposed an anomaly detection scheme using dynamic training method. Amit N. Thakare et al. [27] made an attempt to compare the performance of two prominent on demand reactive routing protocols for MANETs. Kimaya Sanzgiri et al. [28] have proposed a solution to one, the managed-open scenario where no network infrastructure is pre-deployed.

Claude Crrepeau et al. [29] have presented secure Robust Source Routing (RSR). Liana Khamis Qabajeh et al. [30] have proposed a new model of routing protocol called ARANz, which is an extension of the original Authenticated Routing for Ad-Hoc Networks .

Feng He et al. [31] have proposed a novel secure routing protocol S-MAODV which is based on MAODV. Arun Kumar Mondal et al. [32] have presented the analytical results for the probability of success of data transmission over the networks taking the probability of success or failure of individual paths. Pietro Michiardi et al. [33] have carried out a simulation study that identifies security issues which are specific to MANET R. Kalpana et al. [34] have addressed anonymity and trust issues for a wireless network containing selfish and malicious nodes. Mike Burmester et al. [35] have analyzed provable secure route discovery algorithm which is vulnerable to a hidden channel attack. Himani Yadav et al. [36] have carried out survey on different existing techniques for detection of black hole attacks in MANETs with their defects. Jiajia Liu et al. [37] have explored the capability of these networks to support multicast traffic. Stefaan Seys et al. [38] have studied anonymous routing protocol for mobile ad hoc networks (MANETs). Subash Chandra Mandhata et al. [39] have analyzed the black hole attack in MANET using AODV as its routing protocol. Saikat Chakrabarti et al. [40] have proposed an efficient, single round multi signature scheme, CLFSR-M, constructed using cubic (third-order) linear feedback shift register (LFSR) sequences. K.Seshadri Ramana et al. [41] have proposed a routing protocol that is based on securing the routing information from unauthorized users. Sridhar Subramanian et al. [42] have examined a trust based reliable protocol TBRAODV.

V. MANET Routing Security

In an ad hoc network, all the nodes may not be within the transmission range of each other; hence, nodes are often required to forward network traffic on behalf of other nodes. Consider for example the scenario in Fig.1. If node S sends data to node D, which is three hops away, the data traffic will reach its destination only of A and B forward it. The process of forwarding network traffic from source to destination is termed routing.

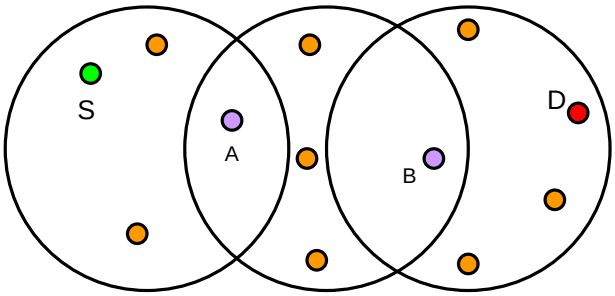

Figure 1 Multihop scenario

There are two general categories of MANET routing protocols: topology-based and position-based routing protocols. The list of some desirable qualitative properties of MANET routing protocols as adopted from an Internet Engineering Task Force (IETF) MANET Working Group memo [43] is as following:

- Loop-free: It is desirable that routing protocols prevent packets from circling around in a network for arbitrary time periods.
- Demand-based operation: In order to utilize network energy and bandwidth more efficiently, it is desirable that MANET routing algorithms adapt to the network traffic pattern on a demand or need basis rather than maintaining routing between all nodes at all time.
- Proactive operation: This is the IP-side of demand-based operation. In cases where the additional latency, which demand-based operations incur, may be unacceptable, if there are adequate bandwidth and energy resources, proactive operations may be desirable in these situations.
- "Sleep" period operation: It may be necessary, for reasons such as the need for energy conservation, for nodes to stop transmitting or receiving signals for arbitrary time periods. Routing protocols should be able to accommodate sleep periods without adverse consequences.
- Security: It is desirable that routing protocols provide security mechanisms to prohibit disruption or modification of the protocol operations.

VI. OTHER ROUTING PROTOCOLS

In addition to the above mentioned routing protocols for MANET, there are some other routing protocols that do not rely on any traditional routing mechanisms, instead rely on the location awareness of the participating nodes in the network. Generally, in traditional MANETs, the nodes are addressed only with their IP addresses. But, in case of location-aware routing mechanisms, the nodes are often aware of their exact physical locations in the three-dimensional world. This capability might be introduced in the nodes using Global Positioning System (GPS) or with any other geometric methods. Based on these concepts, several geo-cast and location-aware routing protocols have already been proposed. The major feature of these routing protocols is that, when a node knows about the location of a particular destination, it can direct the packets toward that particular direction from its current position, without using any route discovery mechanism. Recently, some of the researchers proposed some location-aware protocols that are based on such ideas. Some examples of these protocols are Geographic Distance Routing (GEDIR)[44], Location-Aided Routing (LAR)[45], Greedy Perimeter Stateless Routing (GPSR)[46], Geo-GRID[47], Geographical Routing Algorithm (GRA)[48], etc. Other than these, there are a number of multicast routing protocols for MANET Some examples of the multicast routing protocols are: Location-Based Multicast Protocol (LBM)[49], Multicast Core Extraction Distributed Ad hoc Routing (MCEDAR)[50], Ad hoc Multicast Routing protocol utilizing Increasing id-numbers (AMRIS)[51], Associativity- Based Ad hoc Multicast (ABAM)[52], Multicast Ad hoc On- Demand Distance-Vector (MAODV) routing [53],Differential Destination Multicast (DDM)[54],On-Demand Multicast Routing Protocol (ODMRP)[55], Adaptive Demand-driven Multicast Routing (ADMR) protocol [56], Ad hoc Multicast Routing protocol (AMRoute)[57], Dynamic Core-based Multicast routing Protocol (DCMP)[58], Preferred Link-Based
Multicast protocol (PLBM)[59],etc. Some of these multi cast protocols use location information and some are based on other routing protocols or developed just as the extension of another unicast routing protocol. For example, MAODV is the multicast-supporting version of AODV.

VII. OTHER RECENT WORKS ON MANET ROUTING

In this section, the recent works on routing in MANET that could be used as a reference by the practitioners, are considered. Some of these works have taken the major routing protocols as their bases and some of them have enhanced performances of the various previous routing protocols. Some recent works are: node-density-based routing [60], load-balanced routing [61], optimized priority based energy-efficient routing [62], reliable on-demand routing with mobility prediction [63], QoS routing [64], secure distributed anonymous routing protocol [65], robust position based routing [66], routing with group motion support [67], dense cluster gateway based routing protocol [68], dynamic backup routes routing protocol [69], gathering-based routing protocol [70], QoS-aware multicast routing protocol [71], recycled path routing [72], QoS multicast routing protocol for clustering in MANET [73], secure anonymous routing protocol with authenticated key exchange [74], self-healing on-demand geographic path routing protocol [75], stable weight-based on demand routing protocol [76], fisheye zone routing protocol [77], on-demand utility-based power control routing [78], secure position-based routing protocol [79], scalable multi-path on-demand routing [80], virtual coordinate-based routing [81], etc.

VIII. SCOPE FOR FUTURE RESEARCH

Many more efficient routing protocols for MANET might be developed in the coming future, which might take security and QoS (Quality of Service) as the major concerns. So far, the routing protocols mainly focused on the methods of routing, but in future a secured but QoS-aware routing protocol could be worked on. Ensuring both of these parameters at the same time might be difficult. A very secure routing protocol surely incurs more overhead for routing, which might degrade the QoS level. So an optimal trade-off between these two parameters could be searched. In the recent years some multicast routing protocols have been proposed. The reason for the growing importance of multicast is that this strategy could be used as a means to reduce bandwidth utilization for mass distribution of data. As there is a pressing need to conserve scarce bandwidth over wireless media, it is natural that multicast routing should receive some attention for ad hoc networks. So it is, in most of the cases, advantageous to use multicast rather than multiple unicast, especially in ad hoc
environment where bandwidth comes at a premium. Ad hoc wireless networks find applications in civilian operations (collaborative and distributed computing) emergency search-and-rescue, law enforcement, and warfare situations, where setting up and maintaining a communication infrastructure is

very difficult. In all these applications, communication and coordination among a given set of nodes are necessary. Thus, in future, the routing protocols might especially emphasize the support for multicasting in the network.

IX. CONCLUSION

This paper presents a number of routing protocols for MANET, which are broadly categorized as proactive and reactive. Proactive routing protocols tend to provide lower latency than that of the on-demand protocols, because they try to maintain routes to all the nodes in the network all the time. But the drawback for such protocols is the excessive routing overhead transmitted, which is periodic in nature without much consideration for the network mobility or load. On the other hand, though reactive protocols discover routes only when they are needed, they may still generate a huge amount of traffic when the network changes frequently. Depending on the amount of network traffic and number of flows, the routing protocols could be chosen. When there is congestion in the network due to heavy traffic, in general case, a reactive protocol is preferable. Sometimes the size of the network might be a major considerable point. For example, AODV, DSR, OLSR are some of the protocols suitable for relatively smaller networks, while the routing protocols like TORA, LANMAR, ZRP are suitable for larger networks. Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information in such case is more efficient. On the other hand, as the mobility of nodes in the network increases, reactive protocols perform better. Overall, the answer to the debating point might be that the mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. It is quite natural that one particular solution cannot be applied for all sorts of situations and, even if applied, might not be optimal in all cases. Often it is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages of both types of protocols.

REFERENCES

[1] Azzedine Boukerche (Ed.), Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, John Wiley and Sons, New Jersey, 2009.
[2] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, July-August 1999, pp. 63-70.
[3] Mohammad Ilyas (Ed.), The Handbook of Ad Hoc Wireless Networks CRC Press LLC, Florida, 2003.
[4] Tarun Dalal, Gopal Singh, An Analysis of ASRP Secure Routing Protocol for MANET, IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, Apr. 2012, pp. 132-137.
[5] Panagiotis Papadimitratos et al., Secure Routing for Mobile Ad hoc Networks, Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, Jan.2002.
[6] Marshall, j et al., Identifying flaws in the secure routing protocol. IEEE Conference on Performance, Computing, and Communications, 2003.
[7] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks, Springer-Verlag Berlin Heidelberg 2007.
[8] Eichler, S. et al., Secure Routing in a Vehicular Ad Hoc Network. IEEE Vehicular Technology Conference, Sep. 2004.
[9] M. Rajesh Babu et al., An Energy Efficient Secure Authenticated Routing Protocol for Mobile Ad hoc Networks. International Journal of Reviews in Computing, Vol. 7, Sep. 2011.
[10] Steffen Reidt et al., Efficient, Reliable and Secure Distributed Protocols for MANETs. 2nd International Conference on Mobile Technology, Applications and Systems, Nov. 2005.
[11] Muhammad Nawaz Khan et al., Intrusion Detection System for Ad hoc Mobile Networks. Int. Conf. on Information Technology: Research and Education, Jun.2005.
[12] Lu Jin et al., Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad Hoc Network. Wireless Telecommunications Symposium, Apr. 2006.
[13] Panagiotis Papadimitratos et al., How to Specify and How to Prove Correctness of Secure Routing Protocols for MANET, IEEE-CS Broad Nets, San Jose, CA, USA, Oct. 2006
[14] Shivasharanappa Allur et al., Efficient SNR/RP Attentive Routing Algorithm: Cross-Layer Design for Ad hoc Networks, IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), Oct.2006.
[15] Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, and Phillip Lucs, TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks, IEEE International Conference on Networks, Nov. 2007, pp. 182-187.
[16] Kimaya Sanzgiri, Bridget Dahill, A Secure Routing Protocol for Ad Hoc Networks, IEEE Conference on Network Protocols, Nov. 2002, pp. 78-87.
[17] Poonam Yadav, Rakesh Kumar Gill, Naveen Kumar, A Fuzzy Based Approach to Detect Black Hole Attack, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, Jul. 2012.
[18] Parma Nand et al. (2007) Performance study of Broadcast based Mobile Adhoc Routing Protocols AODV, DSR and DYMO, International Symposium on Wireless Pervasive Computing, Feb.2007.
[19] David B. Johnson et al., Dynamic Source Routing in Ad Hoc Wireless Networks, International Conference on Wireless Communications, Networking and Mobile Computing Sep.2007.
[20] Xiaodong Lin et al., ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks, IEEE International Conference on Communications, Jun. 2007.

[21] Xu Su et al., On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks, IEEE International Conference on Communications, Jun.2007.
[22] Mohd. Anuar Jaafar et al., Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment. Communications Magazine, IEEE ,Feb. 2008.
[23] Umang singh et al., Secure Routing Protocols in Mobile Ad Hoc Networks-A Survey and Taxonomy, IEEE Conference on Wireless Communications and Networking, Mar.2008.
[24] Julien Francq et al., Error Detection for Borrow-Save Adders Dedicated to ECC Unit. , 5th Workshop on Fault Diagnosis and Tolerance in Cryptography, Aug.2008.
[25] Karim El Defrawy et al., Privacy-Preserving Location-Based On-Demand Routing in MANETs, Third International Conference on Risks and Security of Internet and Systems, Oct.2008.
[26] Satoshi Kurosawa et al., Detecting Black Hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, 16th IEEE International Conference on Networks, Dec. 2008.
[27] Amit N. Thakare et al., Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks, International Conference on Advanced Information, Networking and Applications, May. 2009.
[28] Kimaya Sanzgiri et al., A Secure Routing Protocol for Ad Hoc Networks, 18th International Conference on Computer Communications and Networks, Aug.2009.
[29] Claude Crrepeau et al., A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes. IEEE Transactions on Vehicular Technology, Jan.2009
[30] Liana Khamis Qabajeh et al., A Scalable, Distributed and Secure Routing Protocol for MANETs, International Conference on Computer Technology and Development, Nov. 2009.
[31] Feng He et al., S-MAODV: A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol, 3rd IEEE International Conference on Computer Science and Information Technology, Jul. 2010.
[32] Arun Kumar Mondal et al., The Success of Data Transmission in Multipath Routing for MANET, 2nd International Asia Conference on Informatics in Control, Automation and Robotics, Mar. 2010.
[33] Pietro Michiardi et al., Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks, 2nd International Conference on Education Technology and Computer (ICETC), Jun. 2010.
[34] R. Kalpana et al., Mobile Anonymous Trust Based Routing Using Ant Colony Optimization, IEEE Asia-Pacific Services Computing Conference (APSCC), 2010.
[35] Mike Burmester et al., Towards provable security for route discovery protocols in mobile ad hoc networks. Global Information Infrastructure Symposium(GIIS),2011, Aug. 2011.
[36] Himani Yadav et al., A Review on Black Hole Attack in MANETs., 13th International Conference on Advanced Communication Technology (ICACT), Feb.2011
[37] Jiajia Liu et al., Multicast Capacity, Delay and Delay Jitter in Intermittently Connected Mobile Networks. IEEE Global Telecommunications Conference (GLOBECOM 2011),Dec.2011.
[38] Stefaan Seys et al., ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks, International Symposium on Computer Networks and Distributed Systems (CNDS), Feb. 2011.
[39] Subash Chandra Mandhata et al., A counter measure to Black hole attack on AODV based Mobile Ad-Hoc Networks, IEEE International Conference on Networking, Sensing and Control (ICNSC), Apr. 2011.
[40] Saikat Chakrabarti et al., Authenticating DSR Using a Novel Multi signature Scheme Based on Cubic LFSR Sequences. Date of Conference: 26-28 Sept. 2011
[41] K.Seshadri Ramana et al., A Trust-Based Secured Routing Protocol for Mobile Ad hoc Networks. , International Conference on Recent Trends In Information Technology (ICRTIT), Apr.2012.
[42] Sridhar Subramanian et al., Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks, Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), May 2012.
[43] S. Corson and J. Macker. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. Internet Request for Comments (RFC 2501), January 1999.
[44] Lin X, Stojmenovic I ,GEDIR: Loop-Free Location Based Routing in Wireless Networks, International Conference on Parallel and Distributed Computing and Systems, pp.1025–1028
[45] Ko Y-B, Vaidya NH, Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. Wireless Networks, Volume 6, pp.307–321
[46] Karp B, Kung HT , GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. ACM MOBICOM 2000, pp. 243–254
[47] Liao W-H, Tseng Y-C, Lo K-L, Sheu J-P, GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks based on GRID, Journal of Internet Technology, Volume 1, Issue 2,pp. 23–32.
[48] Jain R, Puri A, Sengupta R , Geographical Routing Using Partial Information for Wireless Ad Hoc Networks. IEEE Personal Communications, Volume 8, Issue 1, pp. 48–57.
[49] Ko Y-B, Vaidya NH , Location-based multicast in mobile ad hoc networks. Technical Report, Texas A&M University
[50] Sinha P, Sivakumar R, Bharghavan V, MCEDAR: Multicast Core-Extraction Distributed Ad Hoc Routing, IEEE WCNC, Volume 3, pp. 1313–1317.
[51] Wu CW, Tay TC, AMRIS: A Multicast Protocol for Ad Hoc Wireless Networks, IEEE MILCOM 1999, Volume 1, pp. 25–29
[52] Toh C-K, Guichal G, Bunchua S, ABAM: On-Demand Associativity-Based Multicast Routing for Ad Hoc Mobile

Networks. Proceedings of IEEE VTS-Fall VTC 2000, Volume 3, pp. 987–993
[53] Royer EM, Perkins CE, Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing. IETF Draft, draft-ietf-manet-maodv-00, 15 Jul. 2000,
[54] Ji L, Corson MS, Differential Destination Multicast-A MANET Multicast Routing Protocol for Small Groups, IEEE INFOCOM 2001, Volume 2, pp. 1192–1201.
[55] Lee S, Su W, Gerla M, On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks, ACM/Kluwer Mobile Networks and Applications (MONET), volume 7, Issue 6,pp. 441–453.
[56] Jetcheva JG, Johnson DB, Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks. ACM MobiHoc 2001, pp. 33–44.
[57] Xie J, Talpade RR, Mcauley A, Liu M, AMRoute: Ad Hoc Multicast Routing Protocol. ACM Journal of Mobile Networks and Applications, Dec.2002, Volume 7, Issue 6, pp. 429–439.
[58] Das SK, Manoj BS, Murthy CSR, A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks, ACM MobiHoc 2002,pp. 24–35.
[59] Sisodia RS, Karthigeyan I, Manoj BS, Murthy CSR,A Preferred Link Based Multicast Protocol for Wireless Mobile Ad Hoc Networks, IEEE ICC 2003, Volume 3, pp. 2213–2217.
[60] Quintero A, Pierre S, Macabe´o B, A routing protocol based on node density for ad hoc networks. Ad Hoc Networks, Volume 2, Issue 3,pp. 335–349.
[61] Saigal V, Nayak AK, Pradhan SK, MallR, Load balanced routing in mobile ad hoc networks, Computer Communications,1995, Volume 27, Issue 3, pp. 295–3054.
[62] Wei X, Chen G, Wan Y, Mtenzi F, Optimized priority based energy efficient routing algorithm for mobile ad hoc networks, Ad Hoc Networks, Volume 2, Issue 3, pp. 231–239.
[63] Wang N-C, Chang S-W, A reliable on-demand routing protocol for mobile ad hoc networks with mobility prediction. Computer Communications, 2005, Volume 29, Issue 1, pp. 123–135.
[64] Bu¨ r K, Ersoy C, Ad hoc quality of service multicast routing, Computer Communications, 2005, Volume 29, Issue 1, pp. 136–148.
[65] Boukerche A, El-Khatib K, Xu L, Korba L An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. Computer Communications, 2005, Volume 28, Issue 10, pp. 1193–1203.
[66] Moaveninejad K, Song W-Z, Li, X-Y Robust position-based routing for wireless ad hoc networks, Ad Hoc Networks, 2005, Volume 3, Issue 5, pp. 546–559.
[67] Rango FD, Gerla M, Marano S, A scalable routing scheme with group motion support in large and dense wireless ad hoc networks. Computers & Electrical Engineering, 2006 Volume 32, Issues 1–3, pp. 224–240.
[68] Ghosh RK, Garg V, Meitei MS, Raman S, Kumar A, Tewari N, Dense cluster gateway based routing protocol for multi-hop mobile ad hoc networks. Ad Hoc Networks, 2006, Volume 4, Issue 2, pp. 168–185.
[69] Wang Y-H, Chao C-F, Dynamic backup routes routing protocol for mobile ad hoc networks. Information Sciences, 2006, Volume 176, Issue 2, pp. 161–185.
[70] Ahn CW, Gathering-based routing protocol in mobile ad hoc networks. Computer Communications, 2006, Volume 30, Issue 1, pp. 202–206.
[71] Sun B, Li L, QoS-aware multicast routing protocol for Ad hoc networks, Journal of Systems Engineering and Electronics, 2006, Volume 17, Issue 2, pp. 417–422.
[72] Eisbrener J, Murphy G, Eade D, Pinnow CK, Begum K, Park S, Yoo SM, Youn J-H, Recycled path routing in mobile ad hoc networks. Computer Communications, 2006, Volume 29, Issue 9, pp. 1552–1560.
[73] Layuan L, Chunlin L, A QoS multicast routing protocol for clustering mobile ad hoc networks, Computer Communications, 2007, Volume 30, Issue 7, pp. 1641–1654.
[74] Lu R, Cao Z, Wang L, Sun C, A secure anonymous routing protocol with authenticated key exchange for ad hoc networks, Computer Standards & Interfaces, 2007, Volume 29, Issue 5, pp. 521–527.
[75] Giruka VC, Singhal M, A self-healing On-demand Geographic Path Routing Protocol for mobile ad-hoc networks, Ad Hoc Networks, 2007, Volume 5, Issue 7, pp. 1113–1128.
[76] Wang N-C, Huang Y-F, Chen J-C, A stable weight-based on demand routing protocol for mobile ad hoc networks, An International Journal of Information Sciences, 2007, Volume 177, Issue 24, pp. 5522–5537.
[77] Yang C-C, Tseng L-P, Fisheye zone routing protocol: A multilevel zone routing protocol for mobile ad hoc networks, Computer Communications, 2007, Volume 30, Issue 2, pp. 261–268.
[78] Min C-H, Kim S, On-demand utility-based power control routing for energy-aware optimization in mobile ad hoc networks. Journal of Network and Computer Applications, 2007, Volume 30, Issue 2, pp. 706–727.
[79] Song J-H, Wong VWS, Leung VCM, Secure position-based routing protocol for mobile ad hoc networks, Ad Hoc Networks, 2007, Volume 5, Issue 1, pp. 76–86.
[80] Reddy LR, Raghavan SV, SMORT: Scalable multipath ondemand routing for mobile ad hoc networks, Ad Hoc Networks, Volume 5, Issue 2, pp. 162–188.
[81] Zhao Y, Chen Y, Li B, Zhang Q, Hop ID: A Virtual Coordinate-Based Routing for Sparse Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, 2007, Volume 6, Issue 9, pp. 1075–1089.

Sumati Ramakrishna Gowda has obtained B.E Dégrée in Computer Science from Mysore, Master of Science in Information Technology from KSOU Mysore, and she also obtained Master of Philosophy in Computer Science from Madhurai Kamraj University, Madurai. She is currently working as a Lecturer, DOS in Computer Science, at the Karnataka State Open University, Mysore, India. KSOU was inspired by the concept of open learning and distance education, also providing IT education to a host of students at different levels. Currently pursuing her research work in the area of Security Approaches in Routing Protocol.

Dr. P. S. Hiremath is Ph.D. in Applied Mathematics , from Karnataka University, Dharwad, Karnataka, India. He is Masters of Science in Applied Mathematics, Karnataka University, Dharwad, Karnataka, India. He had been in the Faculty of Mathematics and Computer Science of various institutions in India, namely, National Institute of Technology, Surathkal (1977-79), Coimbatore Institute of Technology, Coimbatore (1979-80), National Institute of Technology, Tiruchinapalli (1980-86), Karnatak University, Dharwad (1986-1993) and has been presently working as Professor and Chairman of Computer Science in Gulbarga University, Gulbarga(1993 onwards). His research areas of interest are Computational Fluid Dynamics, Optimization Techniques, Image Processing and Pattern Recognition, and Computer Networks. He has published 156 research papers in peer reviewed International Journals and proceedings of International Conferences.