WWJMRD 2017; 3(11): 198-202
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

L. Raghavendar Raju
Dept. of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

C. R. K. Reddy
Professor, Dept. of Computer Science and Engineering, CBIT, Hyderabad, India

Correspondence:
L. Raghavendar Raju
Dept. of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

Quality of Services (QoS) and Security Issues in Mobile Ad Hoc Networks (MANETs) – A Review

L. Raghavendar Raju, C. R. K. Reddy

Abstract
Mobile Ad hoc Network (MANET) is a self-governing group of mobile nodes forming a self-motivated network and communicating over wireless links. Owing to its individuality such as easy deployment and self-organizing capability, it has great potential in many civil, military, real-time and a multimedia application is growing as well. These requests have Quality of Service (QoS) requirements and Security like bandwidth, end-to-end delay, jitter, energy, availability, authentication, integrity, and confidentiality. Consequently, it becomes very necessary for MANETs to have an efficient routing and QoS mechanism to support these applications. The emphasis of this paper is on exploring existing correlations for security and QoS issues in MANEs, the current issues and future challenges that are involved in this exciting area of research are also included.

Keywords: MANETs, QoS, Security, Routing

1. Introduction
A MANET is a self-configuring collection of wireless mobile nodes that form a temporary and dynamic wireless network without any pre- infrastructure. MANET is a self-configuring; there is no central management system with configuration responsibilities. All the mobile nodes can communicate each other directly if they are in other's wireless links radio range. To enable the data transfer, they either communicate through single hop or multi-hop. As MANETs allow universal facility access, anywhere- anytime without any stationary infrastructure they can be extensively used in army battlefields, crisis management services, classrooms and conference halls, etc. Manet's ad-hoc networking fashion developments lead to the development of large multimedia applications such as video-on-demand, video conferencing, etc.
The quality of Service (QoS) is shown the level of a service presented by the network to the user. Maximum of the multimedia applications has rigorous QoS requirements that must be satisfied. The objective of QoS provisioning is to attain a more deterministic network performance so that information passed by the network can be better delivered and network properties can be better utilized. However, there remains an important challenge to provide QoS solutions and maintain end-to-end QoS with user mobility.
Maximum of the traditional routing protocols are developed either to reduce the data traffic in the network or to reduce the average hops for delivering a packet. Even some protocols designed without explicitly considering QoS such as Ad-hoc On-demand Distance Vector (AODV) [1], Dynamic Source Routing (DSR) [2] and On-demand Multicast Routing Protocol (ODMRP) [3]. When QoS is considered, some protocols may be inadequate or unfeasible due to the lack of resources and the extreme computation overhead. QoS routing commonly encompasses two farm duties: Collecting and maintaining up-to-date state information about the network and discovery available paths for a connection founded on its QoS necessities. To maintenance QoS, a service can be characterized by a set of measurable pre-specified service needs such as minimum bandwidth, delay, delay variance, packet loss rate and many other metrics are also used to quantify QoS.
Due to its extensive features, MANET invites different real world application areas where the networks topology modifications very quickly. However, researchers are trying to

minimize the drawback of MANET such as limited bandwidth, battery power, computational power, security, and QoS. The existing security and QoS solutions for wired networks cannot be applied directly to MANET, which makes a MANET greatly more vulnerable to security attacks. Firstly, MANETs face defies in secure communication. For a sample, the resource constraints on nodes in ad-hoc networks limit the cryptographic procedures that used for secure messages. So, it is susceptible to link attacks ranging from passive eavesdropping to active masquerade, message replay, and concerning misrepresentation. Secondly, mobile nodes without proper protection are easy to compromise and lead to poor quality of service.

2. Background Study

Routing protocols having to different QoS philosophies have been proposed in the literature. In 2004, Al-Karaki and Kamal published a detailed overview [4] and the progress in the QoS routing. They emphasize some extents such as security and multicast routing requiring further research attention. They have categorized the QoS routing solutions into various types of approaches: Flat, Hierarchical, Position-based and power aware QoS routing. Reddy et al. [5] provided a thorough overview of the more widely accepted MAC and routing solutions for providing better QoS in MANETs.

QoS routing protocols are classified based on their Network topology (Flat, Hierarchical, and Location-aware) and method to route find with QoS (Proactive, Reactive, and Hybrid).

2.1. Network Topology Based Protocols

One of the most popular methods to distinguish MANETs QoS protocols is based on how distribution paths among group members are constructed. Regarding this approach, existing QoS protocols can be divided into flat, hierarchical and hybrid protocols. Most of the routing protocols assume physically flat network architecture with mobile nodes having the homogeneous capability regarding network properties and computing control. However, this hypothesis may not often hold since there exist various types of mobile nodes with different roles, capacities, and mobility patterns. In an architecture-based multicast routing protocol, MANETs have physically hierarchical architectures, which are formed by different types of mobile nodes.

For example, Hierarchical QoS Multicast Routing Protocol (HQMRP) [8] for MANETs constructs a multicast structure at to each level of the hierarchy for efficient and scalable multicast message delivery. Self-Organizing Map (SOM) [9] and Core-Extraction Distributed Ad-hoc Routing algorithm (CEDAR) [10] is similarly a typically categorized architecture, which provides a way for automatically organizing the hierarchical design.

2.2. Route Discovery with QoS-based protocols

Based on the routing information bring up to date mechanism is active, the QoS methods are categorized into three groups, Proactive, on-demand, and hybrid QoS approach.

Proactive protocols are one where a routing table is maintained at every node which aids in forwarding packets. These tables are regularly to up to date routing data from each and every node. So, the source node can get a routing path instantly if it requires. There are some distinctive proactive QoS-routing protocols like QOLSR [11] and PLBQR [12] (Predictive Location-Based QoS Routing in Mobile Ad Hoc Networks).

A reactive protocol is also called as "on-demand" protocols. Reactive protocols are one which does not require the maintenance of network topology when there is no traffic. The state information is acquired when needed. However, route maintenance is a necessary operation of reactive routing protocols, because source nodes may suffer from extended delays for route searching before they can forward data packets. QoS AODV [13] (QoS Ad-hoc On-demand Distance Vector), ACMP [14] (Adaptive Core based Routing Protocol with Consolidated Query Packets) and CQMP (Mesh-based Multicast Routing Protocol with Consolidated Query Packets) [15] are typical examples of reactive routing protocols. Compared to proactive routing protocols, less control overhead is the significant advantage of the reactive routing protocols.

3. Qos Issues and Challenges in Ad-Hoc Networks

QoS provision will result in an increase in computational and communicational cost. In other disputes, it desires more time to setup a connection and preserves more state information per connection. The enhancement in network utilization counterweights the increase in state information and the connected difficulty, and several issues are needed to be challenged while providing QoS for MANETS. The key problems that are faced are as follows:

3.1. **Unreliable Channel:** The minute errors are the critical issue which arises for the untrustworthy wireless networks. These systems cause high bit error rate, and this is due to high interference, thermal noise, multipath vanishing effects and so on. This chief to small packet delivery ratio. Since the medium is wireless in the situation of MANETs, it may also result in leakage of information into the surroundings.

3.2. Maintenance of Route: The self-motivated nature of the network topology and altering the behavior of the communication standard makes the maintenance of network state information very challenging. The conventional routing paths may be ruined even during the progression of data transfer. Therefore the need for maintenance and rebuilding of routing paths with slight overhead and delay causes. The QoS- aware routing would require the reservation of resources at the intermediate nodes. The reservation maintenance with the changes in topology becomes cumbersome.

3.3. The mobility of the nodes: Here the nodes are considered as mobile nodes. That is they can move individually and randomly in any direction and speed, and the topology information has to be updated regularly and accordingly so as to provide routing to reach the final destination which results in again less packet delivery ratio.

3.4. Limited power supply: Limited power supply constrains the mobile nodes to compare nodes in the wired network. Providing QoS consume more power due to overhead from the mobility nodes which may drain the nodes power quickly.

3.5. Lack of centralized control: In Mobile networks, dynamically a node can join or leave the network. Impulsively the network is set up. Hence there may not be any facility of a centralized controller on the nodes which leads to increase algorithm's overhead and complexity, as QoS state information must be distributed efficiently.

3.6. **Channel contention:** In a MANET nodes need communicate with each other on a shared channel so as to make available the network topology. Though, this leads the difficulties of interference and channel contention. Peer-to-Peer data communications can be evaded in various ways; one technique is to endeavor complete clock synchronization as well as use a TDMA-based system anywhere each node may transmit at a predefined time. It is challenging to achieve since there is no centralized control of the ad hoc nodes. Other techniques are used to a different frequency band or else spreading code (as in CDMA) to an each respective transmitter. It involves a distributed channel selection mechanism as well as the dissemination of channel information [6].

3.7. Security: It can be considered as a QoS constraint. Without adequate security, unauthorized accesses and usages may violate the QoS conferences. The nature of transmissions in wireless networks hypothetically results in new security acquaintances. The physical medium of communication is integrally insecure. So we want to design security-aware routing algorithms for ad-hoc networks.

4. Security Challenges in Manet

MANETs are more apt to attack than wired network and high-security challenges due to the and dynamically changing network topology. The goals of the security solutions for MANETs are to provide security services, such as availability, confidentiality, integrity, authentication, non-repudiation and anonymity to mobile users in the above mention challenging environment. Security is a major problem in network chiefly in MANETs where security attacks can disturb the nodes limited properties and consume them or waste time before the route chain broke. To attaining this aim, the security solution must provide thorough protection spanning the entire protocol stack. There is no distinct mechanism that will be responsible for all the security services in MANETs. For these details, securing a mobile Adhoc network is precise challenging. The following goals are needs to maintain for security issues in ad-hoc are as follows:

4.1 Availability

Availability is concerned with the authorized node must have access to all data and services in the network and is to the survivability of network services despite the attack. Availability challenge arises due to MANET's dynamic topology and open boundary. Retrieving time, which remains the time required for a node to access the network services or information is important because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time.

4.2 Confidentiality

According to this amenity, each node or application must have access to specified services that it has the permission to access. Most of the encryption techniques provide data in secret facilities. However, then in MANET as per there is no central management, key distribution faced lots of challenges and in some cases impossible.

Confidentiality ensures that only authorized party's access computer-related assets. The goal of secrecy is to keep information secret from unauthorized user or nodes. It ensures that certain information is only readable or accessible by the authorized party. To maintain the secrecy of some confidential data, we requisite to preserve them confidentially as os all entities that do not have the opportunity to access them. The typical approach for keeping information confidential is to encrypt the data with a secret key that only proposed receivers possess, hence achieving confidentiality. Confidentiality is sometimes called secrecy or privacy.

4.3 Integrity

Integrity means that resources be able to be modified only by certified parties or only in the authorized way. The aim of integrity is to guarantee the message being transferred is never corrupted. It ensures the identity of the messages when they are transmitted. Such as confidentiality, integrity can apply to a stream of messages, a single message or selected fields within a message. However, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a flow of messages assures that messages expected, without duplication, insertion, modification, reordering, or replays. Integrity can be compromised majorly in two ways, malicious altering, and accidental altering.

4.4 Authentication

The goal of this amenity is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about the characteristics of the origin node. A unique way to provide this service is using certifications, whoever in time off of main control unit, key delivery, and key management is challengeable. In [13] the authors presented a new way based on trust model and clustering to the public certificate keys. In this case, the network can divide into some clusters, and in this clusters, the public key delivery will be safe by mechanisms. However, it has some restrictions like clustering. MANET dynamic topology and changeable nodes position, made clustering challengeable.

Authentication is the verification of claims about the identity of a source of information. It ensures that only the authorized parties do the access and supply of data. In the infrastructure-based wireless network, it is possible to implement a central authority at a point such as base station or access point. However, in MANETs no central administration, so it is hard to authenticate an entity. It is essential for the communication members to prove their characteristics as what they have claimed using some methods so as to ensure the authenticity. Authenticity is guaranteed because only the legitimate sender can produce a message that will decrypt properly with the shared key. Authentication can be providing encryption along with cryptographic hash function, digital signature, and certificates. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to a resource and sensitive information and interfering with the operations of the other nodes.

4.5 Nonrepudiation

Non-repudiation ensures that sender and receiver of a message cannot renounce that they have ever sent or received such a message. It is valuable when for detection and isolation of cooperated nodes. It ensures that dedicated actions cannot be denied. In MANETs security objectives of a system can change in different modes, e.g. peacetime, the transition to war, and wartime of a military network. It is helpful when we need to discriminate if a node with some undesired function compromised or not. The features of MANETs make them susceptible to many new attacks. Attacks can classify at the top level, according to network protocol stacks.

4.6 Anonymity

Anonymity means entirely information that can be used to identify the owner or current user of the node should the default be kept private and not be distributed to the node itself or the system program. This criterion is closely related to privacy-preserving, in which we should try to defend the secrecy of the nodes from accidental disclosure to any other entities.

5. Protocols Based On Communication

5.1. Communication between Network and MAC layer

Based on the communication with MAC layer, QoS protocols are two groups, independent and dependent. In the independent QoS protocols, the network layer is not dependent on the MAC layer for QoS provisioning. They typically estimate node, link states and try to route using those nodes and links for which more promising environments exist. Still, the possible level of performance is usually not measured or is only relative and therefore no assurances can be made to applications. The intention of such protocols is distinctive to foster an improved normal QoS for all packets allowing to more than one metrics. QOLSR (QoS-Optimized Link State Routing), DSARP (Delay-Sensitive Adaptive Routing Protocol) [16] and IAR (Interference-Aware Routing) [17] are distinctive self-determining protocols.

The dependent QoS protocol needs the MAC layer to promotion the routing protocol for QoS provisioning. It achieves implicit resource reservation and offers QoS promises. Entropy-based routing (EBR) [18], Channel Capacity-Based Routing (CCBR) [7] and Node State Routing (NSR) [19] are standard dependent protocols.

5.2. Single constrained vs. Multi-constrained QoS metrics

Utmost of the protocols concentrated on providing a guaranteed throughput service only then throughput was deemed the most significant constraint in earlier days. These single-constrained routing protocols take success in various phases; conversely, they do not always achieve best. In CEDAR, the bandwidth is used as the only QoS constraint for routing.

Maximum of the multimedia applications needs the communication to meet rigorous requirements on delay, delay-jitter, cost and other QoS metrics. In this perspective, the development is to move from single constrained routing to multi-constrained routing. The main function of multi-constrained QoS routing is to find a possible path that satisfies many limitations at the same time, which is an immense challenge for MANETs where the topology may change continually. It has been verified that such a problem is NP-complete. QMRPD (QoS Multicast Routing Protocol for Dynamic group topology) [20] GAMAN (Genetic Algorithm-based Routing for MANETs) [21] HMCOP (Heuristic multi Constrained Optimal Path) are standard multiconstrained routing protocols.

5.3. Hard QoS vs. Soft QoS approach

The QoS provisioning methodologies can be broadly classified into two classifications, hard QoS, and soft QoS methods. If QoS requirements of connection are guaranteed to be met for the whole duration of the period, the QoS approach is designated as hard QoS method. In MANETS, it is precise challenging to provide hard QoS guarantees to user applications. More or less of the protocols NSR and SIRCCR [22] (SIR and Channel Capacity based Routing).

If the QoS necessities are not assured for the entire period, the QoS method is designated as soft QoS method. Thus, QoS guarantees can only be given within certainly assured limits. Most of the protocols deliver soft QoS guarantees.

Conclusion

MANETs are expected to enlarge their applications in the future communication atmospheres. The support for QoS will thus be an important and necessary component of MANETs. Some significant research issues and open questions need to be addressed to facilitate QoS support in MANETs. It takes in admission control policies and protocols, QoS Conservancy under failure conditions, QoS support for multicast operations and security against a denial-of-service attack, etc. Power control and accommodating multiple classes of traffic requires further research attention. In this paper we have discussed the arising challenges and possibilities of security and QoS issues.

Refrences

1. C.Perkins, “Ad-hoc On-Demand Distance Vector (AODV) routing”, RFC3561[S], 2003.
2. D.B.Johnson, D.A.Maltz, Y.C.Hu, “The Dynamic Source Routing protocol for mobile ad hoc networks”, Internet Draft, 2004.
3. J.Hong, “Efficient on-demand routing for mobile ad hoc wireless access networks”, IEEE journal on selected Areas in Communications 22(2004), 11-35.
4. J.N. Al-Karaki and A.E.Kamal, “Quality of Service routing in mobile ad hoc networks: Current and future trends” in Mobile Computing Handbook, CRC Publishers, 2004.
5. T.B.Reddy I.Karthigeyan, B.Manoj and C.S.R.Murthy, “Quality of service provisioning in ad hoc wireless networks: a survey of issures and solutions.” Vol.4, pp.83-124, 2006.
6. Y.Yang and R.Kravets “Contention-aware admission control for ad hoc networks”, IEEE Trans.Mobile Comput., vol.4, 363-377, 2005.
7. C.R.Lin and J.S. Liu., “QoS routing in ad hoc wireless networks”, IEEE J.Select.Areas Commun., vol.17, pp.1426-11438, 1999.
8. L.Li, C.Li, “A hierarchical QoS multicast routing protocol for mobile ad-hoc networks”, Chinese Journal of Electronics 15(4) (2006), 573- 577.
9. M.S.Kumar, C.Venkatesh, A.M.Ntarajan, “Performance comparison of multicast protocol for physically hierarchical ad-hoc networks using neural Concepts”, 7th International conference on Signal Processing Proceedings ICSP, 2004, 1581-1584.

10. R.Sivakumar, P.Sinha and V.Bharghavan, “CEDAR: a core-extraction distributed ad hoc routing algorithm” IEEE J.Select.Areas Commun., vol.17, pp.1454-1465, 1999.
11. H.Badis and K.A.Agha, “QOLSR, QoS routing for ad hoc wireless networks using OLSR”, Wiley European Trans. Telecomunications, vol.15 (4), pp.427-422, 2005.
12. S.H.Shah, K. Nahrstedt, “Predictive location-based QoS routing in mobile ad-hoc networks”, in: Proceeding of IEEE ICC 2002, vol.2, pp.1022-1027, 2002.
13. E.M. Royer C.E.Perkins, A R Das “Quality of service for ad-hoc on-demand distance vectorrouting”, IETF Internet draft, July 2000.
14. B.Kaliaperumal, A.Ebenezer, Jeyakumar, “Adaptive Core-based scaleable multicasting networks”, INDICON, Annual IEEE (2005), 198-202.
15. H.Dhillon, H.Q.Ngo, “CQMP: a mesh-based multicast routing protocol with consolidated query packets”, in: IEEE wireless communications and networking conference WCNC 2005, pp.2168-2174.
16. M.Sheng, J.Li and Y.Shi, “Routing protocol with QoS guarantees for ad-hoc network” Electronic Letters, vol.39, pp.143-145, 2003.
17. R.Gupta, Z.Jia, T.Tung and J.Walrand, “Interference aware QoS routing for ad-hoc networks” in Proc.IEEE Canadian Conf. on Electrical and Computer Engineering, vol.3, pp.1535-1538, 2003.
18. H.Shen, B.Shi, L.Zou etal., “A distributed entropy based long-life QoS ruting algorithm in ad-hoc network”, IEEE J.Select.Areas Commun., vol.17, pp.1454-1465, 1999.
19. J.Stine and G.de Veciana, “A paradigm for QoS in wireless ad hoc networks using synchronous signaling and node state”, IEEE J.Select.Areas Commun., vol.17, pp.1454-1465, 1999.
20. Li Layuan and Li Chunlin, “A QoS Multicast Routing Protocol for Dynamic group topology”, Information Sciences 169 (2005) 113-130.
21. L.Barolli, A.Koyama et al., “A QoS routing method for ad-hoc networks based on genetic algorithm”, in Proc.14th Int.Wksp. Database and Expert Systems Applications, pp.175-179, 2003.
22. D.Kim, C.H.Min et al., “On-demand SIR and bandwidth guaranteed routing with transmit power assignment in ad hoc mobile networks” IEEE Trans. Veh. Technol., vol.53, pp.1215-1223, 2004.