Secure and Quality of Service Routing in Mobile Ad Hoc Network: A Survey

D.R.Jiji Mol[1] and Dr.S.Behin Sam[2]

[1]Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, India.
[2]Assistant Professor, Department of Computer Science, R.V. Government Arts College, Chengalpattu,India.

Abstract— A Mobile Ad hoc Network (MANET) is a collection of mobile nodes without any infrastructure. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Owing to multi-hop routing and absence of centralized administration in open environment, MANETs are vulnerable to attacks by malicious nodes [1].Provisioning Quality of Service QoS) and securing data in routing is a challenging issue of MANET. The goal of MANET routing protocols are to improve delay, provide reliability, reduce overhead, maximize network life and support hybrid routing. This paper describes the review of existing secure and QoS protocol solutions.

Index Terms— MANET, QoS, Routing, Security, Trust

1 INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of wireless nodes. Each node in a MANET has limited resources such as battery power, processing power and memory. Nodes are communicated each other by multi-hop fashion. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Nodes typically communicate over multiple hops, while intermediate nodes act as routers by forwarding data. Routing protocols should adapt to such dynamism, and continue to maintain connection between the communicating nodes in the presence of path breaks caused by mobility and/or node failures [2]. Due to the mobility of nodes, MANET routing protocols must be able to maintain the connectivity.

MANETs often suffer from attacks by selfish or malicious nodes, such as packet dropping attacks and selective forwarding attacks. There are two primary motivations associated with trust management in MANETs. Firstly, trust evaluation helps identify malicious entities. Secondly, trust management offers a prediction of one's future behaviors and improves network performance.Thus routing is a crucial issue to the design of a MANET. In order to overcome these limitations of MANET, an efficient routing protocol is required.

Many routing protocols have been proposed and these protocols are broadly classified into two. They are Proactive (Table Driven) routing protocols and Reactive (On Demand) routing protocols. In proactive routing, nodes are maintaining a routing table to establish a path from one node to another. This path details are obtained by exchanging control messages.

This frequent transmission of these messages produce high overhead. To overcome this problem, reactive protocols are introduced. On demand routing protocol compute the route at the time of request. The popular ad hoc on-demand protocols are Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporary Ordered Routing Algorithm (TORA).

These protocols are designed without considering security and QoS constraint path generation. Secure communication is important in ad hoc network, especially in military application. There are two types of attacks: Passive attacks and Active attacks. The passive attacks do not affect the functionality of the connection. But in contrast, the active attacks change or destroy the data of transmission.

The goal of QoS provisioning is to achieve better performance and better resource utilization. The QoS parameters can differ from application to application. Any given QoS metric can be classified as additive, concave or multiplicative. Bandwidth and energy are concave metric, whereas cost, delay and jitter are additive metrics. The reliability or availability of a link based on some criteria such as link break probability is a multiplicative metric.

Provisioning security and Quality of Service in routing protocol is a challenging issue of MANET. Remaining of this paper describes the security requirements, issues of MANET QoS routing, Quality of service metrics and existing secure and QoS routing protocols.

2 SECURITY REQUIREMENTS

In order to meet passive and active attacks, MANET expected to meet the following security requirements [4].

- *Confidentiality*
  Only the intended receivers should be able to interpret the transmitted data.
- *Integrity*
  Data should not change during the transmission process.
- *Availability*
  Network services should be available on the time and it should be possible to correct failure to correct failure to keep the connection stable.
- *Authentication*

Every transmitting or receiving node has its own signature. Nodes must be able to authenticate that the data sent by the legitimate node.

- *Non-repudiation*

  Sender of a message shall not be able to later deny sending the message and that the recipients shall not be able to deny the recipient after receiving the message.

3 Quality of Service

Quality of Service is the performance level of a service provided by the network to the user. The goal of QoS provisioning achieve better performance, so that the data delivery and resource utilization can be better. Service provided by the network or service provider can be categorized by a set of pre-specified measurable service requirements such as maximum delay, maximum bandwidth, maximum delay variance (jitter) and maximum packet loss.

3.1 QoS Metrics

The QoS metrics are different from application to application [5]. In case of multimedia application, bandwidth, delay, and delay jitter are the key QoS metrics and for military application security is the key factor. Application such as emergency and rescue operation, availability of network is the key factor. Application such as group communication in a conference hall requires energy to consume data. Hence battery life is a QoS key parameter. QoS parameters are not mainly categorized by the requirements of multimedia traffic in MANET. QoS parameters are based on the requirement constraints of the node. Some of the resource constraints are battery charge, processing power and buffer space.

3.2 Issues and challenges in provisioning QoS in MANET

MANET contains unique characteristics that create several difficulties in provisioning QoS. They are discussed below [3].

- *Mobility*

MANET has no fixed infrastructure. So nodes can be moved any location at any time. Due to the node mobility, the path may break. This will affect the QoS admission. The re-established session may miss the packet delay or deadline. This is not applicable in QoS.

- *Imprecise state information*

Node in a MANET maintains both link-specific and flow-specific state information. The link-specific state information includes bandwidth, delay, delay jitter, loss rate, error rate, stability cost and distance values for each link. The flow-specific state information includes session ID, source address, destination address, QoS requirement of flow. The state information is inherently imprecise because of its changing topology. Hence the routing decision may not be accurate and resulting in some of the real-time application packets missing their deadline.

- *Hidden terminal problem*

In MANET packets are transmitted through intermediate node when the destination is not comes under the transmission range of source. The hidden node problem occurs when two or more nodes collide at a common receiver node. They are necessitates to retransmits the packets. This will affect the quality of flow. The RTS/CTS control packets exchange mechanism and IEEE 802.11 standard reduce the hidden node problem in certain extend.

- *Error prone channel state*

The wireless links have time-varying characteristics in terms of link capacity and link-error probability. This requires that the ad hoc wireless network routing protocol should interact with the MAC layer to find alternate routes through better quality links.

- *Lack of central coordination*

There is no central system to coordinate the network. it is complicated to provisioning QoS.

- *Resource constraints*

Battery life and processing power are two essential and limited resources that form the major constraint for the nodes in an ad hoc network. Thus ad hoc wireless network routing protocols must optimally manage these resources.

- *Bandwidth constraints*

In wireless networks, the capacity of the radio band is limited and hence the data rates it can offer are much less than what a wired network can offer. That is why the routing protocol should use the bandwidth optimally to keep the overhead as low as possible.

- *Insecure medium*

The broadcast wireless medium is highly insecure. Security is very important in MANET, especially for military application. MANET is susceptible to attack such as eaves dropping, spoofing, denial of service, message distortion and impersonation. It is very difficult to provide secure communication without sophisticated security mechanism.

4 Secure Routing Protocols

The following protocols are provided security during the data transmission.

4.1 Trust –Based on-demand multipath routing in Mobile Ad hoc Networks

A simple trust model [1] is proposed to decrease the hazards from malicious nodes while forwarding packets. This protocol is able to discover multiple loop-free paths. These paths are evaluated by two parameters called hop counts and trust values. This evaluation technique is used to find flexible and feasible shortest path from source to destination.

The Simple trust model is based on packet forwarding ratio to evaluate its neighbors behavior .A node trust is represented as weighted sum of forwarding ratio of packets and a continued product of node trusts is computed as path trust. The trust model consist of three processes trust derivation, computation and application. The trust derivation process obtain packet forwarding ratio of the neighbor nodes.

The computation phase uses a linear aggregation technique to estimate the overall trust in a node and continued product is used to compute the trust of a path. Trust applications including trust-based route discovery and route selection.The protocol improves packet delivery ratio and reduce the black hole, gray hole and modification attacks.

4.2 FACES

FACES [6] algorithm provides secure routing in MANET. Friend based trust technique is used to isolate malicious nodes in a network. This algorithm has four phases. They are challenges your neighbor, Rate Friends, Share friends and Route through friends.

There are two lists maintained in each node to challenge the neighbor. The Nodes which have completed the challenge in Friend List, Nodes which does not complete the challenge is shifted to the question mark list. Nodes which are placed in the question mark list are considered as malicious nodes. Friends are rated on the basis of the amount of data they transfer through themselves and according to the rating of other friends which is obtained during the friend list sharing process.

When a node decides to transmit data, it broadcasts a route request message. Each intermediate node forwards route request message only if sending node is not in the question mark list. On receiving the route reply message the source node evaluates the root by checking for friends in the route. Finally the data is routed through the route with greatest number of trusted friends. To defeat the eavesdropping, the source encrypts the data using public key cryptography. Using these techniques FACES provide better performance and secure data delivery.

4.3 USOR

An efficient privacy-preserving routing protocol Unobservable Secure On-demand Routing (USOR) [7] achieves content unobservability by employing anonymous key establishment based on group signature. Working of USOR is the combination of group signature and ID-based encryption. This combination is used for route discovery.

USOR protocol has two phases. First is an anonymous key establishment process to construct secret session key. Next is an unobservable route discovery process .USOR protocol protect all parts of a packets content provide solutions on traffic pattern unobservability. It can be used with appropriate traffic pending schemes to achieve truly communication unobservability.

It is not only providing strong privacy protection and also more resistant against due to node compromise. While analyzing the performance of USOR,it gives better performance in packet delivery ratio, latency and normalized control bytes.USOR is not preventing wormhole attack and DOS attack.

4.4 Risk-Aware Mitigation for MANET Routing attacks

Dempster-Shafer mathematical theory has been adopted as a valuable tool for evaluating reliability and security in information system. Dempster's rule in combination has several limitations. So new Dempster's rule of combination with a notion of importance factor (IF) is discovered. The proposed model is an extension of D-s evidence model, which is non-associative and weighted [8].

Another method used in the model is risk-aware response. This risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Combinations of above two methods are tested against six metrics. They are packet delivery ratio, Routing cost, packet overhead, byte overhead, mean latency and average path length.

The experiment result clearly demonstrated the effectiveness and scalability of risk aware approach.

4.5 Regression-based trust model for Mobile Ad Hoc Networks

Providing security to infrastructure less mobile ad hoc network is a challenging task. All the mobile nodes in the network must co-operate each other to exchanging routing information, forwarding data packets etc. these nodes are legitimate devices, but they behave maliciously. The behavior of malicious node degrades the performance of the network. Vector Auto Regression (VAR) based trust model overcome these problems [9].

A malicious node may launch multiple attacks. So the proposed technique uses a regression model for each functional aspect of a neighboring node is captured as a vector item and multiple attacks launched by a malicious node are easily identified. The VAR trust model mitigates content modification attack, flooding attacks, rushing attacks and no/selective forwarding of data packets.

The trust and confidence value in the path computation improves the performance of network in the presence of malicious nodes. The performance results show high throughput with minimal overhead. Alternate trustworthy path discovery is also done quickly.

4.6 High Reliable disjoint path

Multiple disjoint paths are discovered to forward data between source and destination, because single path may increase the overhead and frequent route failure. The multiple paths are both node disjoint and link disjoint. Flooding mechanism is used to discover multiple paths. Finding multiple paths in a single route discovery reduces the routing overhead [10].

Hopfield neural network algorithm is used to select multiple paths that maximize the network reliability. Path stability is considered for reliability and resistance for failure computation. Link Expiration Time (LET) between two nodes is used to estimate the link reliability. The reliability of each path is obtained by multiplication of those links which constitute the path.

Simulation results show link-disjoint path have more reliability than node-disjoint path and provide higher reliability than existing protocols.

4.7 Trust-based minimum cost opportunistic routing

The opportunistic routing exploits the broadcast nature and special diversity of the wireless medium by involving multiple one-hop neighbors for packet forwarding. The increase in packet forwarding reliability improves throughput and energy efficient. Wang et al, concentrate to provide security in opportunistic routing of MANET.

A simple trust model [11] is built to evaluate the neighbors forwarding behavior to select the trust forwarding list and illustrate the new metric of opportunistic routing taken the wireless quality into consideration. Then the proposed forwarding model can be applied to the existing opportunistic routing. A trusted minimum cost routing (MCOR) algorithm is used to monitor neighbors forwarding character correctly and determine the optimal forwarder from the trusted forwarding list to mitigate node misbehavior.

The main benefit of the opportunistic routing are, it can combine multiple weak link into one strong link and it can sip some hop to reduce the number of transmission and increasing throughput during the transmission.

4.8 Fighting against packet dropping misbehavior

A.Baadache et al, [12] focus on an attack in which an intermediate node drops packet passing through it. The motivation of dropper is to preserve its resources or launch of denial of service. The proposed approach verifies the correct forwarding of packet by an intermediate node. The Markle tree principle is used for implementation in packet by an intermediate node.

A Markle tree is a binary tree in which, each leaf carries a given value and the value of an interior node including root node is a one-way cryptographic hash function of the node's children values. In this approach, channel is considered as bidirectional.

The core of this idea is that all the intermediate nodes need to acknowledge the reception of the packet. Using this acknowledgement, the source node construct Markle tree. Then compare the value of the root of the tree with the precalculated value. If both values are equal then the end-to-end packet is dropped free.

5 QoS Routing Protocols

5.1 Quality of Service enabled ant colony based multipath routing

QoS-enabled routing algorithm for MANET (QAMR) [13] based on Ant Colony Optimization (ACO) approach. QAMR solve bandwidth problem of MANET. An ant-like agent called forward ants (FANT) and backward ants (BANT) are used to measure various parameters such as next hop availability (NHA), delay, and bandwidth.

Path selection in QAMR is based on stability of the nodes and the path preference probability. QAMR discover multiple disjoint paths between source and destination with QoS requirements. NHA considers both mobility and energy factor for checking the availability of next hop.

Deposition of pheromone substance on a link helps to get a best path. Path which has highest path preference probability is selected for data transmission. QAMR provide better performance for throughput and packet delivery ratio.

5.2 Distributed Fault-tolerant Quality of wireless networks

Distributed fault tolerant quality of service routing protocol is a cluster based routing protocol. This protocol addresses stability and recoverability problem of MANET. Aim of Extended Fully Distributed Cluster-Based (EFDCB) [14] protocol is to providing fault tolerance, which is a critical feature in providing QoS feature in providing QoS in the link failure-prone environment of MANET.

Cluster-head has connectivity awareness for all cluster nodes. When a cluster node leaves a cluster, due to mobility or failure, and a QoS path supported by that node are broken, the cluster head reestablish the connection.

To reestablish the connection with minimal delay, cluster head has connection awareness for all cluster nodes. These knowledge are collected via two processes: communication with the other clusters via Clustered Fisheye State routing (CSFR) and local clustered information exchange. These processes of EFDCB ensure with high probability, low overhead, low QoS disruption time, minimal packet drop and improved throughput.

5.3 Energy-Efficient Real-time multicast routing

Multicasting through Time Reservation using Adaptive Control for Energy Efficiency (MC-TRACE) [15] is an energy efficient real time data multicasting architecture for MANET. MC-TRACE is a cross-layer design protocol, where MAC layer and network layer functionality are performed in a single integrated layer.

There are five phases in MC-TRACE to reach the goal. First, Initial Flooding (IFL) is used create a redundant multicast mesh through network wide flooding. It is also a technology discovery mechanism. The redundancy introduced by IFL is pruned by the PRN mechanism using receiver based and transmitter based feedbacks. Tree branches broken primarily due to leaf node mobility are repaired by the maintain branch (MNB) mechanism. Relay node mobility-induced tree branch breakages are repaired by the RPB mechanism. Finally, Create Branch (CRB) mechanism is designed to recreate totally collapsed tree branches.

Reengineering of the tree and mesh structure make them highly energy efficient and robust for real time data multicasting in MANET. MC-TRACE provides superior energy efficiency while producing competitive QoS performance and bandwidth efficiency.

5.4 Link Availability prediction-based reliable routing

Q.Han et al present a link availability-based routing protocol (LBRP) [16]. Unpredictable topology and frequent link failure are taken as a problem. Probabilistic and statistical computing is used to derive link availability. Random walk mobility is used.

Based on this model, each nodes movement consist of sequence of random length intervals called mobility epoch, during which a node moves in a constant direction at a constant speed. The speed and direction of each node varies randomly from epoch to epoch.

To analyze the link availability, they assumed that the node has a bidirectional communication link with any other node within a distance of R meters from it. The link breaks if the node moves to a distance greater than R, failure link recovery process take place. The simulation result shows, LBRP improves the availability and reliability of upper layer services and quality of services.

5.5 QoS-Aware Multipath Routing Scheme

Author proposes a new QoS-aware shortest multipath source (Q-SMS) [17] routing scheme to offer significant network improvements with QoS requirements. In Q-SMS, nodes use their residual capacity to make better admission control decisions.

It is an on-demand QoS-aware routing scheme with cross layer design. The required capacity (C_{req}) and minimum capacity (C_{min}) fields are included in the route request packet QRREQ, minimum available capacity of a link is used for better path selection. Bottle neck paths are avoided with the help of these constraints.

In case QoS route breakage, the source node selects a route with largest bottle neck capacity (C_{min}). The Q-SMS routing scheme achieve high throughput, low delay and overhead. There is no provisioning of any predictive way to anticipate a route break which causes performance degradation particularly in mobile scenarios.

5.6 Light-Weight Trust-Based QoS Routing

The proposed Trust based QoS routing (TQR) [18]algorithm ensures the forwarding of packets through the trusted and least link delay routs only by monitoring the behavior of each other and meet the QoS constraints accordingly. Once the malicious node discovered, it is isolated from the network such that no packet is forwarded through or from it. The trust model is discovered by a node using trust degree value of its neighbors.

5.7 QoS Oriented Distributed Routing

The QoS Oriented Distributed (QOD) [19] routing protocol enhance the QoS support capability of hybrid networks. QOD incorporates five algorithms. A QoS guaranteed neighbor selection algorithm selects qualified neighbors and employs deadline driven scheduling mechanism to guarantee QoS routing.

The distributed packet scheduling algorithm reduces the packet transmission delay. A mobility based segment resizing algorithm adjusts segment size according to node mobility to reduce transmission time. The traffic redundant elimination algorithm improves the transmission throughput and the data redundancy elimination based transmission algorithm eliminates the redundant data and improves the transmission QoS.

5.8 Topology – Transparent Scheduling

The author presents Topology – Transparent Scheduling (TTS) and QoS routing scheme for ad hoc network[20]. The Bandwidth Estimation (BWE) and Bandwidth Allocation (BWA) are the essential components of the proposed joint scheme for a mixture of QoS and best effort flows. Combination of bandwidth information and congestion control achieves effective admission control and QoS support.

6 Conclusion

In this paper, importance of security and QoS metrics routing in MANET were demonstrated. This work motivates to discover efficient routing algorithm with reliability, energy efficient with low overhead. The surveyed routing protocol showed the on-demand routing can improve the performance of the network such as delay, throughput, reliability, and life time.

7 References

[1] X. Li Z. Jia P. Zhang R. Zhang and H. Wang, Trust-based on-demand multipath routing in mobile ad hoc networks, IET Inf. Secur, Vol. 4, Iss. 4, pp. 212–232., 2010.

[2] L. Reddeppa Reddy and S.V. Raghavan, SMORT: Scalable multipath on-demand routing formobile ad hoc networks, Science Direct, Ad Hoc Networks 5, 162–188, 2007.

[3] LoayAbusalah, AshfaqKhokhar, and Mohsen Guizani, A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.

[4] LoayAbusalah, AshfaqKhokhar, and Mohsen Guizani, A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials, vol. 10, no. 4, fourth quarter 2008.

[5] T. Bheemarajuna Reddy, I. Karthigeyan, B.S Manoj, C. Siva Ram Murthi, Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. Science Direct ad hoc networks 4, pp.83-124, 2006.

[6] Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, Pushkar Gupta, andPravinaDhurandher, FACES: Friend-Based Ad Hoc Routing UsingChallenges to Establish Security in MANETs Systems, IEEE Systems Journal, Vol. 5, No. 2, June 2011

[7] Zhiguo Wan, KuiRen, and Ming Gu, USOR: An Unobservable Secure On-DemandRouting Protocol for Mobile Ad Hoc Networks, IEEE Transactions On Wireless Communications, Vol. 11, No. 5, May 2012.

[8] Ziming Zhao, Hongxin Hu, Gail-JoonAhn, and Ruoyu Wu, Risk-Aware Mitigation forMANET Routing Attacks, IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 2, March/April 2012.

[9] R. Venkataraman, M. Pushpalatha and T. Rama Rao, Regression-based trust model for mobile ad hoc Networks, IET Inf. Secur, Vol. 6, Iss. 3, pp. 131–140, 2012.

[10] M. Sheikhan E. Hemmati, High reliable disjoint path set selection in mobilead-hoc network using Hopfield neural network, IET Commun., Vol. 5, Iss. 11, pp. 1566–1576, 2011.

[11] Wang Bo, Huang Chuanhe, Li Layuan, and Yang WenzhongXv, Trust-based minimum cost opportunistic routing for Ad hoc networks, The Journal of Systems and Software 84, 2107– 2122, 2011.

[12] Abderrahmane Baadache, and Ali Belmehdi, Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks, Journal of Network and Computer Applications 35, 1130–1139, 2012.

[13] P. Venkata Krishna V. Saritha G. Vedha A. Bhiwal A.S. ChawlaQuality-of-service-enabled ant colony-based multipath routing for mobile ad hoc networks, IET Commun., Vol. 6, Iss. 1, pp. 76–83, 2012.

[14] Larry C. Llewellyn, Kenneth M. Hopkinson, and Scott R. Graham, Distributed Fault-Tolerant Quality of Wireless Networks, IEEE Transactions On Mobile Computing, Vol. 10, No. 2, February 2011.

[15] BulentTavli and Wendi B. Heinzelman, Energy-Efficient Real-Time Multicast Routingin Mobile Ad Hoc Networks, IEEE Transactions On Computers, Vol. 60, No. 5, May 2011.

[16] Q. Han1,3 Y. Bai 2,3 L. Gong4 W. Wu, Link availability prediction-based reliable routingfor mobile ad hoc networks, IET Commun., Vol. 5, Iss. 16, pp. 2291–2300, 2011.

[17] HaseebZafar, David Harle, Ivan Andonovic, LaiqHasan and AmjadKhattak, Qos-Aware Multipath Routing Scheme For Mobile Ad Hoc Network. IJCNIS, vol.4, no.1, April 2012.

[18] Bo Wang, Xunxun Chen, and Weiling Chang, A light-weight trust-based QoS routing algorithm for ad hoc networks, Pervasive and Mobile Computing 13 (2014) 164–180.

[19] Ze Li and Haiying Shen, A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks , IEEE Transactions on Mobile, Vol.13, Iss.3, pp.693 – 708, March 2014.

[20] Yi-Sheng Su, Szu-Lin Su and Jung-Shian Li, Joint Topology-Transparent Scheduling and QoS Routing in Mobile Ad Hoc Networks, IEEE Transactions On Vehicular Technology, Vol. 63, No. 1, January