International Journal of Engineering Research and Development
***e*-ISSN: 2278-067X, *p*-ISSN: 2278-800X, www.ijerd.com**
Volume 2, Issue 9 (August 2012), PP. 33-36

Security Issues and Quality of Services Challenges in Mobile Ad-hoc Networks

Jogendra Kumar[1], Rajesh Kumar Varun[2], Rajesh Yadav[3]
[1]*M. Tech Student, ABES Engineering College, Ghaziabad*
[2,3]*Assistant Professor, Department of Information Technology, Northern India Engineering College, New Delhi*

Abstract—A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. The special features of MANET bring this technology great opportunity together with severe challenges. This paper describes the fundamental problems of ad hoc networking by giving its background including the concept, features, status, and applications of MANET and we have discussed security and Quality of services (QoS) challenges of Mobile ad-hoc networks.

I. INTRODUCTION

A mobile ad hoc network is a concept that has received attention in scientific research since the 1970s. A mobile ad hoc network (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the larger Internet. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network [1].

The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. MANETs are useful in many applications because they do not need any infrastructure support. Collaborative computing and communications in smaller areas (building organizations, conferences, etc.) can be set up using MANETs. Communications in battlefields and disaster recovery areas are further examples of application environments. With the evolution of Multimedia Technology, Quality of Service in MANETs became an area of great interest. Besides the problems that exist for QoS in wire-based networks, MANETs impose new constraints [2]. This is due the dynamic behavior and the limited resources of such networks. Mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network.

MANETs has shows distinct security goals, such as:

- Authentication
- Integrity
- Confidentiality
- Non-Repudiation

Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

A. QoS in MANETs

Quality of Service (QoS) means that the network should provide some kind of guarantee or assurance about the level or grade of service provided to an application. The actual form of QoS and the QoS parameter to be considered depends upon specific requirements of an application. For example, an application that is delay sensitive may require the QoS in terms of delay guarantees [3, 4]. Some applications may require that the packets should flow at certain minimum, bandwidth.

In that case, the bandwidth will be a QoS parameter. Certain application may require a guarantee that the packets are delivered from a given source to destination reliably, then, reliability will be a parameter for QoS.

B. Categories of QoS constraints

A constraint makes the job of a protocol more stressful as compared to the scenario when there is no constraint specified. For example, in case of routing, a route will be considered if it satisfies the specified constraints. The overall value of a constraint from a source to a destination may be expressed in terms of the values of its constituents. Let there be a multihop path between nodes u and v consisting of nodes $u1, u2, \ldots, uk$. Let $c(i, j)$ denotes the value of constraint c between nodes i and j or link (i, j). Alternatively, the value of a constraint along a path depends upon the individual values of the constraint along the links that form the path. Based on how the values of path constraints are related to the values of their corresponding link constraints, QoS constraints are classified into the following three broad categories

• ***Additive:*** A constraint whose overall value is summation of the values of its constituents. In other words,
$c(u, v) = c(u, u1) + c(u1, u2) + \cdots + c(uk, v)$.
For example delay, jitter, hop count are additive constraints.

• ***Multiplicative*****:** A constraint whose resulting value is a product of the values of its constituents. In other words,
$c(u, v) = c(u, u1).c(u1, u2). \ldots .c(uk, v)$.
For example, reliability, and the probability of packet loss are multiplicative constraints.

• ***Concave*****:** A constraint is concave if
$c(u, v) = \min\{c(u, u1) + c(u1, u2) + \cdots + c(uk, v)\}$.
For example, bandwidth along a path is minimum of the bandwidths of the links that constitute the path. Therefore, bandwidth is a concave QoS constraint.

In other words, there may exist a combination of QoS constraints that may not be satisfied by an underlying algorithm in a reasonable amount of time. Such a problem falls into a specific class of problems called NP-complete problems. If a combination of QoS constraints can be satisfied within a reasonable amount of time, then such a problem is said to be a polynomial (P) class of problem. There is a specific procedure to determine whether a problem is in P or NP.

Figure 1 shows a pictorial representation of QoS constraints and their combinations that fall in NP and P classes of problems. The symbols used are as follows: A for additive, M for multiplicative and C for concave. Note that finding an optimal path subject to a combination of two or more additive and/or multiplicative1 constraints is an NP complete problem. As a result, the problem of selecting any combination of two or more QoS parameters (such as delay, jitter, hop count, and loss probability) and optimizing them is an NP-complete problem. The only combinations of QoS parameters or metrics that are computationally feasible are bandwidth (which is a concave constraint) and any one of the additive/multiplicative constraints mentioned above.

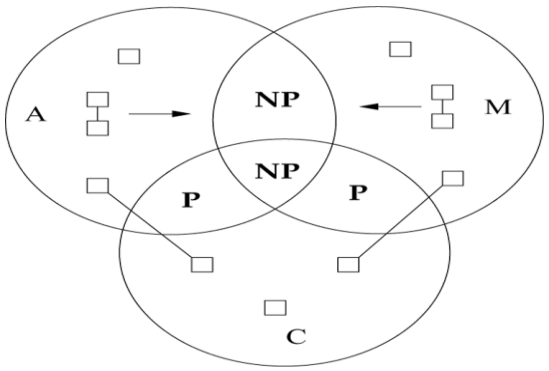

Figure 1 Constraints and their combination that lie in P or NP

In addition to the usual network operations, the functionalities that are to be incorporated for QoS of MANETs are as follows:

- Traffic classifier
- Resource reservation
- Scheduling
- Admission control.

II. RESEARCH ON QOS SUPPORT IN MANETs

In the literature, the research on QoS support in MANETs spans over all the layers in the network:

- *QoS models* specify an architecture in which some kinds of services could be provided. It is the system goal that has to be implemented.
- *QoS Adaptation* hides all environment-related features from awareness of the multimedia-application above and provides an interface for applications to interact with QoS control.
- Above the network layer *QoS signaling* acts as a control center in QoS support. The functionality of QoS signaling is determined by the QoS model.
- *QoS routing* is part of the network layer and searches for a path with enough resources but does not reserve resources.

- *QoS MAC* protocols are essential components in QoS for MANETs. QoS supporting components at upper layers, such as QoS signaling or QoS routing assume the existence of a MAC protocol, which solves the problems of medium contention, supports communication, and provides resource reservation [5, 6, 7].

III. MANET ISSUES AND CHALLENGES

Providing QoS support in MANETs is an active research area.

A. Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. In most cases, the nodes in an ad hoc wireless network maintain both the link-specific state information 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 [8, 9]. The flow specific information includes session ID, source address, destination address, and QoS requirements of the flow (such as maximum bandwidth requirement, minimum bandwidth requirement, maximum delay, and maximum delay jitter). The state information is inherently imprecise due to dynamic changes in network topology and channel characteristics. Hence routing decisions may not be accurate, resulting in some of the real-time packets missing their deadlines.

B. Security and Reliability: Due to the broadcast nature of the wireless medium, communication through a wireless channel is highly insecure. Hence security is an important issue in AWNs, especially for military and tactical applications. AWNs are susceptible to attacks such as eavesdropping, spoofing, denial of service, message distortion, and impersonation [10]. Without sophisticated security mechanisms, it is very difficult to provide secure communication guarantees.

C. Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services [11].

D. Limited resource availability: Resources such as bandwidth, battery life, storage space, and processing capability are limited in MANETs. Out of these, bandwidth and battery life are very critical resources, the availability of which significantly affects the performance of the QoS provisioning mechanism. Hence efficient resource management mechanisms are required for optimal utilization of these scarce resources.

E. Internetworking: In addition to the communication within an ad hoc network, internetworking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management. In most cases, the nodes in an ad hoc wireless network maintain both the link-specific state information 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 [12]. The flow specific information includes session ID, source address, destination address, and QoS requirements of the flow (such as maximum bandwidth requirement, minimum bandwidth requirement, maximum delay, and maximum delay jitter).The state information is inherently imprecise due to dynamic changes in network topology and channel characteristics. Hence routing decisions may not be accurate, resulting in some of the real-time packets missing their deadlines.

F. Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

IV. SECURITY PROBLEM WITH EXISTING MANETs

The existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers. Authentication, Confidentially, Integrity, Availability, Non-repudiation, Access Control are main security goals for MANETS.

V. METHODOLOGY

A QoS support methodology for MANETS that would allocate resources to individual flows needs the following ingredients:

- A QoS metric
- A MAC protocol that supports QoS
- A method to identify flows
- A method to indicate QoS requirements
- A method to identify nodes with sufficient resources (QoS routing)
- A method to reserve resources
- A method to release resources.

VI. CONCLUSION AND FUTURE WORK

In this paper, we try to inspect the security issues and Quality of Services (QoS) Challenges in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Mobile ad hoc networking is a challenging task due to the lack of resources resides in the network as well as the frequent changes in network topology. Although lots of researches have been done on supporting QoS in the Internet and other networks, they are not suitable for mobile ad hoc networks and still QoS support for such networks remains an open problem.

REFERENCES

[1]. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 2009.

[2]. P. Papadimitratos and Z.J. Haas. "Secure routing for mobile ad hoc networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2008.

[3]. L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 2008.

[4]. Jaydeep Punde, Nikki Pissinou, and Kia Makki, "On Quality of Service Routing in Adhoc Networks, " Proc. 28th Annual IEEE Conference onLocal Area Network (LCN'03), IEEE Comp. Society, pp 276-278, 20-24 Oct, 2003.

[5]. B.S. Manoj, C. Siva Ram Murthy, Real-time traffic support for ad hoc wireless networks, in: Proceedings of IEEE ICON 2002, August 2002, pp. 335–340.

[6]. S. Chakrabarti and A. Mishra, "QoS issues in ad hoc wireless networks," *IEEE Communications Magazine*, 2001, 39(2), pp. 142–148.

[7]. M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," *Ericsson Review*, No.4, 2000, pp. 248-263.

[8]. L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network Journal*, 1999, 13(6), pp. 24-30.\

[9]. S. Chen and K. Nahrsted, "Distributed Quality of Service Routing in Adhoc Networks, " IEEE JSAC 17(8): 1488-1505, Aug 1999.

[10]. C.R. Lin, J. Liu, QoSrouting in ad hoc wireless networks,IEEE Journal on Selected Areas in Communications 17 (8) (1999) 1426–1438.

[11]. D.B. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks, in: T. Imielinski, H. Korth (Eds.), Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996, pp. 153–181.

[12]. G. Theodorakopoulos and J. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE* Journal on Selected Areas in Communications, **24**, (2), (February 2006).