Secure Framework for Reliable QoS Routing in MANET

Dr. Tanupreet Singh(Asst. Prof)

Amritsar College of Engineering and Technology

Preeti Kamra(Asst Prof.)

M.tech (CSE)-Amritsar College of Engineering and Technology

monga.kamra@gmail.com

Abstract - Unlike the wired networks, the unique characteristics of mobile ad hoc networks creates a number of challenges to security design, such as open peer-to-peer network architecture, shared wireless medium and highly dynamic network topology. These challenges clearly make a base for creating a security solution that can provide protection and desirable network performance. We build a theoretical framework which finds a secure node and also a feasible path that utilizes minimum bandwidth and provides maximum reliability i.e probability of sending maximum data successfully

Keywords- Manets Routing, Security in MANETS, AODV, QOS in MANETS

1. Introduction

1.1 Mobile Ad Hoc Networks (MANETs)

With the emergence of real-time applications widespread use of wireless and mobile devices, providing Quality of Service (QoS) in an efficient and scalable manner in mobile ad hoc networks (MANETs) has become a challenging task. Supporting appropriate quality of service for mobile ad hoc networks is a complex and difficult issue because of the dynamic nature of the network topology, and generally imprecise network state information.. The network is expected to guarantee a set of measurable prespecified service attributes to the users in terms of end-to-end performance, such as delay, bandwidth, probability of packet loss, delay variance (jitter), etc.

Quality of service is a set of service requirements that are met by the network while transferring a packet stream from a source to a destination. The guaranteed QoS proposed in wired networks cannot be directly applied to wireless ad hoc networks, because the communication capacity between any two nodes can be dramatically changed and this could result in breaking the previously promised QoS.

Security mechanisms are utilized to preserve protected information and network resources, therefore can protect QoS from being tampered.

1.2 QOS Signalling

To achieve desired QOS we have to search for routes with sufficient resources through qos signaling , to manage resources, to set up, tear down and renegotiate flows. Without protection from a security mechanism, attacks on QoS signaling system could result in QoS routing malfunction, interference of resource reservation, or even failure of QoS provision.

2. Problem Statement

We need to build an algorithm to maintain reliability of the nodes to prevent and detect attacks on QoS signaling.[9] Without protection from a security mechanism, attacks on QoS signaling system could result in QoS routing malfunction, interference of resource reservation, or even failure of QoS provision .

3. Proposed work:

Unlike the wired networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology.[4][8] These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. For maintaining security we need both the node and the path to be reliable. If any of them is compromised it will lead to malfunctioning

In MANETs, a break of QoS parametr can result from malicious attacks as well as radio interference from the nodes who just "wandered" into the neighborhood unaware of the reservation. Moreover, communication links in MANETs are open medium and therefore subject to radio interference. Detection of intrusion on bandwidth reservation needs to distinguish these cases and apparently is not a trivial task.[8].Several monitoring techniques have been proposed to detect QoS attacks or DoS attacks on QoS resources in the Internet [6]. Already work has been published to secure bandwith however , an adversary can also target other Quality of Service parameters (such as *delay*), which will also cause violation of reserved QoS.

We take into picture the transmission time and the minimum bandwith required for the link.The time calculated to transmit the packet ensures the security of the packet, if we keep time to reach the packet to node as an QoS metric.Along with it we calculate the minimum bandwith required of the link through which the packet propagates.

3.1Reliability

We attempt to provide end-to-end reliability as QoS metric. End-to-end reliability is defined as the probability of sending data successfully within a time window [5]. We calculate the

transmission time and the propagation time.. If the node reaches within the time frame then there are less chances of it getting compromised. The end-to-end reliability is calculated from the reliabilities of the paths used for routing. The path reliability is calculated from the link availabilities[13] Link availability is defined as the probability that a link is available from time t0+t, given that it is an active link at time t0 [7]. Path reliability is the product of the link availabilities along the path, assuming the link availabilities are independent. The end-to-end reliability is defined as:

$$1-\Pi_{k\in K}(1-k)$$

where k is the path reliability of a path, and K is the set of all paths. Essentially, the end-to-end reliability is the probability that at least one path does not fail within the given time window.

3.2 Bandwidth Calculation

We attempt to find multiple paths that collectively satisfy the bandwidth requirements. The idle period of the wireless channel is a very important parameter for the calculation of bandwidth. It is determined by the traffic traveling along the mobile nodes as well as their neighborhoods. During the period the mobile nodes can successfully transmit data packets. The available bandwidth can be calculated as follow:

B(i)=Bmax (i).Tidle /Tint erval (1)

where max B (i) denotes the maximal transmission bandwidth of node i. Interval T denotes the interval for observing and idle T , the idle period of wireless channel during interval T , which is generally set to 2s. If the interval is too long, it will not reflect the changes of available bandwidth in time. On the contrary, too short interval will bring too much overhead. Obviously, the main difficulty for evaluating B(i) lies in how to calculate idle T . Carrier sense mechanism of IEEE 802.11 adopted in MANET can judge whether the wireless channel is idle or busy. So it can be used to monitor the transition of channel state. In this paper, we use virtual carrier sense mechanism provided by the MAC layer to determine whether channel is busy. In a unit interval, the period during which the channel changes its state from busy to idle is defined as busy T . Thus idle(T) can be denoted by interval (T) -busy (T) . Putting the value of idle T into Equ.(1), B(i)can be easily calculated.

3.3 Algorithm

Step 1: Calculate the bandwidth based on the formula given in **Bandwidth Requirements**.

i) Calculate the interval of the period for which the channel remains idle.
ii) Also calculate the back off period so that four way handshaking can be achieved for successful delivery.

Step 2: Calculate the transmission and propagation time for the packet to reach all the intermediate nodes.(Keeping the impact of the bottlenecks during the transmissions)

Step 3: If the time to reach the packets differs from the calculated time that implies the malicious packet.

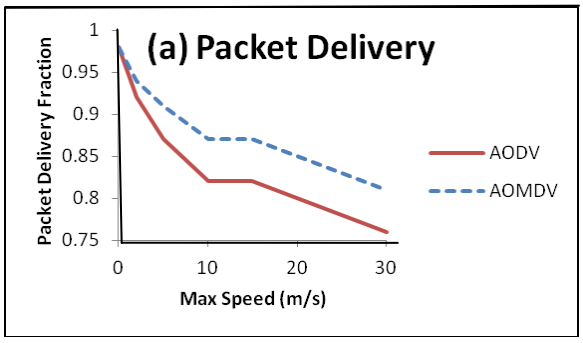
Step 4: If IP spoofing or masquerading happens, that could also be checked by scanning

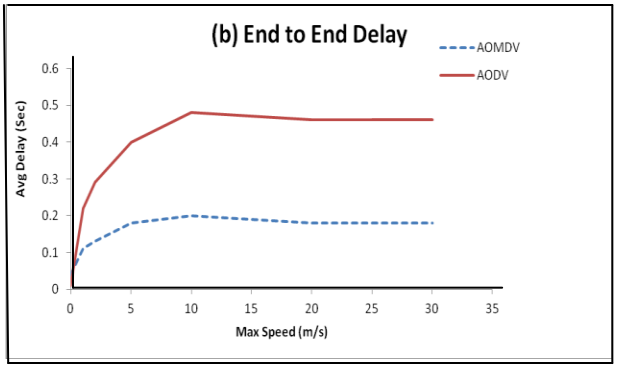
the HEC field of the packet, which was set during the route discovery and was stored in the node local buffer.

Step 5: Calculate the reliability so that the security metrics does not mar the efficiency of the transmission

4 SIMULATIONS

The effects of selfish nodes are studied on four different scenarios where the two parameters that define each scenario are node density and node mobility. We define node density as the number of nodes that form the MANET deployed over .We define node density as the number of nodes that form the MANET deployed over an 800 by 800 meter flat space. On the other hand, node mobility is defined as the average speed each node moves at in the simulation space. Simulation results are given below:





With the increasing traffic load, the burden of intermediate nodes will be aggravated and in turn resulting the failure of resource reserving.. By using multipath method, our proposed method can balance the traffic load through sending data along different paths which is responsible for reducing the packets collision.

Hence, Our version of AODV protocol with minimum bandwith calculation and transmission time parameters we can always keep higher packet delivery ratio.

Furthermore, using alternate paths reduce the impact brought by routing failure, the routing overhead . We observe that AODV provides lower end-to-end delays when the traffic load is below some threshold. In higher load case, however, the traffic allocation adopted by our protocol will improve the delay.

The measurements of the network performance were made by the ns-2 software.Analyzing the results it is possible to evaluate the total number of packets sent by every node of the MANET as well as the total number of packets that have

been dropped. We used the following definition for the aggregate network throughput.

$$\frac{\text{Total no of received packets}}{\text{Total no. of sent packets}}$$

5.Conclusion-

Security and reliability are significant aspects for QoS routing. In this paper we addressed the security and reliability issues for MANET QoS routing.

We proposed a Secure Mechanism for QoS routing, which finds the minimum bandwith and transmission time inorder to prevent misbehaviors on nodes while QoS signaling. .

It has been showed that node mobility improves throughput (network performance) when set to an higher range. It can be used as a parameter which can cooperative mechanism as we envision to study in future work. Future work will be to conduct an analytical study of the impact of node mobility on network performance with misbehaving nodes. We plan then to design and evaluate a collaborative security scheme that solves the selfishness problem, analyzing the effects of such mechanism on network throughput and communication delay.

6. References

[1] S. Murthy and G. L. Aceves, "An Efficient Routing Protocol for Wireless Networks," Mobile Networks and Applications, 1996, Vol. 1, No. 2.

[2] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proceedings of ACM SIGCOMM,

[3] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999.

[4] D. B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, 1996, pp. 153-181.

[5] S. Mueller, R. P. Tsang and D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges," In Performance Tools and Applications to Networked Systems, vol. 2965 of LNCS, 2004.

[6]B. Bhargava, "Detecting Service Violations in Internet and Mobile Ad Hoc Networks," talk at Purdue University

[7] Z. Ye, V. Srikanth and K.Tripathi, "A Framework for Reliable Routing in Mobile Ad hoc Networks," IEEE INFOCOM 2003, IEEE, San Francisco, 2003, pp. 270-280.

[8].Quality Of Service (Qos) Security In Mobile Ad Hoc Networks by Bin Lu, B.S.; M.S., Harbin Institute of Technology-Aug ,2005

[9].Yasmin Jahir and Mohammed Atiquzzaman and Hazem Refai and Peter G.Lo Prest," AODVH:Ad-hoc on demand distance vector routing for hybrid nodes", in the preceeding of IEEE2010.

[10] .Feng Xian and Jianzhi Wang," An efficient Ad-hoc on demand vector routing Protocol "IEEE2010.

[11].Fahim Mann and Nauman Mazhar," MANET routing protocol vs Mobility Models:A performance exaluation",IEEE 2011.

[12].Osama Younes and nigel Thomas," Analysis of the expected number of hopes in mobile ad-hoc network with random waypoint mobility", electronic notes in theoretical computer science 2011.

[13].Junhu zhang and hui peng and fengjing shao,"How node mobility impact reactive ad-hoc routing protocol",ScienceDirect 2011.

