Migrating Packet Dropping in Mobile Ad-hoc Network Based on Modified ACK-Based Scheme

Shalini Sharma, Proff. Mr. Hitesh Gupta, Proff. Mr. Pankaj Kawadkar

Abstract
Dynamic topology and infrastructure less behavior provide a great facility for adhoc network. Such facility generates easy connection of adhoc network and provides node mobility without loss of connection. In such ability packet dropping is a serious challenge for quality performance of adhoc network. The adhoc network suffered some serious security threats such attacks are black hole attack, malicious attack and worm hole attack that attack occurred a packet dropping problem in adhoc network. For the minimization of attack and packet dropping various authors built various method such method is node authentication, passive feedback scheme, ack-based scheme, reputation based scheme and incentive based scheme, ack-based scheme suffered a problem of massive overhead due to extra acknowledgment packet and it also suffered decision ambiguity if the requested node refuse to send back Acknowledgment. In this dissertation we uses modified ack-based scheme using secure channel for overcoming the problem of decision ambiguity for requested node, improved node authentication and minimize packet dropping in adhoc network.

Keywords mobile ad-hoc network, routing misbehaviour, AODV routing protocol, ACK based approach, network security.

1. Introduction
Adhoc network is a group collection of mobile node. During the last few years we have all witnessed steadily increasing growth in the deployment of wireless mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations as do the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network-layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols. Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic.

Fig.1 Shows that scenario of ad-hoc network
The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; secondly, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; thirdly, mobile devices tend to have limited power consumption and computation capabilities.
which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; fourthly, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks.

MANET stands for Mobile Ad-hoc Network. It infrastructureless wireless network. A MANET can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes randomly associate with each other forming arbitrary topologies. They act as both routers and hosts. The ability of mobile routers to self-configure makes this technology suitable for provisioning communication to, for instance, disaster-hit areas where there is no communication infrastructure, conferences, or in emergency search and rescue operations where a network connection is urgently required. The need for mobility in wireless networks necessitated the formation of the MANET working group within The Internet Engineering Task Force (IETF) for developing consistent IP routing protocols for both static and dynamic topologies.

There are five main security services for MANETs: authentication, confidentiality, integrity, non-repudiation, availability. Authentication means that correct identity is known to communicating partner; Confidentiality means certain message information is kept secure from unauthorized party; integrity means message is unaltered during the communication; no repudiation means the origin of a message cannot deny having sent the message availability means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the communicating parties agree on. Note that these security services may be provided singly or in combination. In security concern node authentication scheme is better option for secured communication in mobile adhoc network. The most efficient node authentication is ACK-Based scheme. The ACK-Based scheme provides a node authentication security in adhoc network. But this scheme generates a
huge amount of packet load in network; the generated packet generates a packet dropping in network. The
generation of huge amount of wastes the bandwidth of network and performance of network decreases.

2. Routing protocol in wireless ad hoc network
2.1 Routing Concept
Routing is the act of moving information from source to a destination in an internet work. During this process, at
least one intermediate node within the internetwork is encountered.
The routing concept basically involves two activities: firstly, determining optimal paths and secondly, transferring
the information groups (called packets) through an internetwork. The latter concept is called as packet switching,
which is straight forward, and path determination is very complex. Routing protocol uses several matrices to
calculate the best path for the routing the packet to its destination. These matrices are a standard measurement that
could be number of hops, which is used by the routing algorithm to determine the optimal path for the packet to its
destination. The process of path determination is that, routing algorithms initialize and maintain routing tables,
which contain the total route information for packet. This route information varies form one routing algorithm to
another. Routing tables are filled with a variety of information which is generated by routing algorithms. Most
common entries in the routing table are ip-address prefix and the next hop. Routing tables Destination/next hop
associations tell the router that a particular destination can be reached optimally by sending the packet to router
representing the "next hop" on its way to final destination and ip-address prefix specifies a set of destinations for
which the routing entry is valid for.

In mobile ad-hoc network every node is having routing capability. Nodes are within the radio range (transmission-
range) are called its Neighbors. When the destination node is neighbor of source node, packets are transferred with
single hop. When the destination node is neighbor of source node, packets are transferred with single hop. When
the destination node is out of radio-range (not a neighbors of source node) then packet are transferred in multiple
hops using intermediate nodes. These intermediate nodes (neighbors of source node) forward packets to their
neighbors and so on till destination is reached. This is shown below:

![Figure 4(a): Single hop transfer when S & D in a radio range](image1)

![Figure 4(b): Multiple hops when S & D are not in radio range](image2)
3. ACK-based schemes

ACK based scheme overcome the limitation of passive-feedback technique when power control transmission is used. To implement this scheme, an authentication mechanism is used to prevent the next hop from sending a forged ACK packet on behalf of the intended two hop neighbor. The main drawback of this scheme is the huge overhead. In order to reduce the overhead, the authors have proposed that each node asks its two hop neighbor to send back an ACK randomly rather than continuously. Likewise, this extension also fails when the two hop neighbor refuses to send back an ACK. In such situation, the requester node is unable to distinguish who is the malicious node, its next hop or the requested node. To overcome the previous ambiguity in determining the true malicious node, focuses on detecting malicious links instead of malicious nodes. This scheme is based on 2ACK packet that is assigned a fixed route of two hops in the opposite direction of the received data traffic’s route. In this scheme, each packet’s sender maintains the following parameters; (i) list of identifiers of data packets that have been sent out but have not been acknowledged yet, (ii) a counter of the forwarded data packets, (iii) and a counter of the missed packets.

4. Modified ACK-based scheme

In the existing ack-based scheme uses 2ack process for the node authentication process in attack scenario in ad-hoc network. These 2ack based scheme generate a huge amount of ack packet in the network and also give decision ambiguity for requested node and then effect quality of service. now we modified these scheme used finite state automata. Finite state automate provide a state of route ack, due to this node ack packet maintain state between node to request and respond node. In this process we used some extra buffered memory for maintain a state of node.that memory area maintain a path state due to given request and response. For maintaining a request packet acknowledgment we calculate the next hop with dsdv protocol concept. Path state maintains a sequence of ack packet.

5. Simulation parameter & simulation result: simulation setup

<table>
<thead>
<tr>
<th>Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation used</td>
</tr>
<tr>
<td>Topology area</td>
</tr>
<tr>
<td>No. of Mobile Nodes</td>
</tr>
<tr>
<td>Max. No. of Connection</td>
</tr>
<tr>
<td>Simulation Time</td>
</tr>
<tr>
<td>Speed</td>
</tr>
<tr>
<td>Communication Link Capacity</td>
</tr>
<tr>
<td>Traffic Intensity</td>
</tr>
<tr>
<td>Routing Protocol</td>
</tr>
</tbody>
</table>

In order to simulate the scenarios described above, the implementation was done in NS-2.34 Network Simulator. The simulation scenario to simulate MANET, which uses AODV without packet drop and with packet drop are given in table.

results:

This set contains result of comparisons of Graph b/w Throughput with secure channel and without secure channel, Average E- E Delay, Packet Delivery Ratio and Avg. Jitter and Routing Load in Ad Hoc network.

Comparison b/w packet delivery ratio between with secure channel without secure channel
The result shows both the cases, with the secure channel and without the secure channel it is measured that the packet delivery ratio is dramatically decreases when the network are not using secure channel. Hence, for better delivery of packet a secure channel is must in the network.

**Comparison b/w throughput with secure channel without secure channel**

![Figure 6: Effect on throughput using secure channel in mobile adhoc network](image)

This result shows that throughput of the network with secure channel is greater as compared to the throughput of the network without containing secure channel. Decrease in throughput indicates that the resources are not utilized in the most efficient manner, it also points out that the available resources can be utilized in a more efficient manner. Clearly it shows that without using secure channel in a network has detrimental effect on throughput.

**Comparison b/w Routing load with secure channel witho ut secure channel**

![Figure 7: Effect on Routing Load using secure channel in mobile adhoc network](image)

This result also shows that, routing load increases without using secure channel as compared to the network using secure channel. Due to this, if the network does not use secure channel then the overhead and traffic load or congestion increases. So the network must use secure channel.

### 6. Conclusion & Recommendation

Without infrastructure and node mobility in adhoc network is a great challenge in security concern. For security concern various method are proposed for node authentication in mobile adhoc network. The authentication scheme of leader agent and member surveillance greatly reduces the relative calculating overheads and communication costs. Generally speaking, when leader agent node and surveillance nodes are not destroyed, the united nodes can ensure the reliability, the authentication result is reliable. The dissertation proposes a novel scheme for migrating packet dropping in mobile adhoc network. Our proposed method uses secure channel to overcome the decision ambiguity in requested node and node authentication. In this dissertation secure channel maintain a state of request and reply such fashion minimize packet overhead in network. Our proposed method also removes the node ambiguity in 2ACK hop for authentication process. And minimize a packet dropping in mobile adhoc network. Our proposed mechanism has overcome some of the limitations like it has the required some extra buffer memory for maintain a state of request/reply automata. It also introduces little bit computational overhead during route advertisement and path establishment.
References


[5]. Zonghua Zhang, Farid Na¨ıt-Abdesselam Pin-Han Ho, Xiaodong Lin;” RADAR: a ReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks”, 1525-3511/08©2008 IEEE.


[17]. Mr. Ankur Khetrapal, “ Routing techniques for Mobile Ad Hoc Newtorks Classification and Qualitative/Quantitative Analysis”.


This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE’s homepage: http://www.iiste.org

CALL FOR JOURNAL PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There’s no deadline for submission. Prospective authors of IISTE journals can find the submission instruction on the following page: http://www.iiste.org/journals/ The IISTE editorial team promises to the review and publish all the qualified submissions in a fast manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Recent conferences: http://www.iiste.org/conference/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digital Library, NewJour, Google Scholar