International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.2, Mar-Apr 2012 pp-102-106 ISSN: 2249-6645

Design and Development of ACK-Based Scheme Using FSA for Ad-hoc Networks

[1]Mustafa Sadeq Jaafar , [2] H K Sawant
[1, 2] Department of Information Technology,
Bharati Vidyapeeth Deemed University
College Of Engineering, Pune-46

ABSTRACT:
Ad hoc 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 and 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.

1. INTRODUCTION

The network that uses wires is known as a wired network. Initially the networks were mostly wired networks. When there is a use of wire in a network, definitely it also requires network adapters, routers, hubs, switches if there are more than two computers in a network. The installation of a wired network has been a big issue because the Ethernet cable should be connected to each and every computer that makes a network. Definitely this kind of connection takes time, in fact more time than expected, because when we connect wires with computers we have to take care of lot of things like wire should not come under the feet, it should be under ground or it should be under the carpet if computers are in more than one room. However in new homes nowadays, the wiring is being done in such a way that it will look like as it is a wireless connection, greatly simplifying the process of cables. Similarly the wiring of a wired network depends on lot of things like what kind of devices are being used in a wired network, whether the network is using external modem or is it internal, the type of internet connection and many other issues. As we know making a wired network is not an easy task, but still there are many other tasks that are more difficult than making a wired network, but we are not going to discuss these tasks here. In configuring the wired network, the hardware implementation is a main task. Once the hardware implementation is finished in a wired network, the remaining steps in a wired network do not differ so much from the steps in a wireless network. There are some advantages of wired network that include cost, reliability and performance. While making a wired network, Ethernet cable is the most reliable one because the makers of Ethernet cable continuously improving its technology and always produces a new Ethernet cable by removing the drawbacks of previous one. That is why Ethernet cable is the most preferable in making a wired network, as its reliability is kept on growing from the past few years. In terms of performance, wired networks can provide good results. In the category of Ethernet, there is Fast Ethernet too, that provides enormous performance if a wired network is built in home for some features like data sharing, playing games and for the sake of high speed internet access. Still it is not false to say that Fast Ethernet can fulfill the need of network that is built in home for these kinds of purposes, till many years in future. Security in wired LANs can be a little problem because a network that is wired and is connected with internet must have firewall also in it, but unfortunately wired network does not have tendency to support firewalls, which is a big issue. However this problem can be solved by installing firewall software on each individual computer in a network.

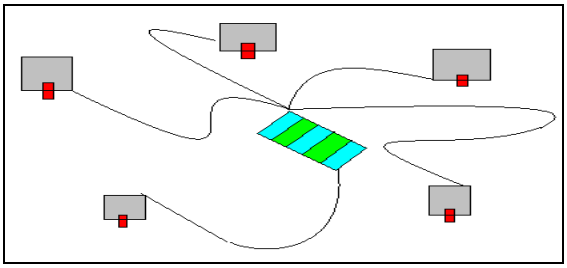


Figure 1 Wired Networks

The nodes of wired network does require power, as they get that power from the alternating current (AC) source that is present in that particular network.

1.1 Wireless Networks

On the other hand, wireless network is such kind of network that does not use wires to build a network. It uses radio waves to send data from one node to other node. Wireless networks lie under the category of telecommunications field. It is also known as wireless local area network (WLAN). It

uses the Wi-Fi as a standard of communication among different nodes or computers. There are three types of Wi-Fi communication standard.
802.11b
802.11a
802.11g

802.11b was the oldest standard that was being used in WLAN. After 802.11b, the standard being introduced was 802.11a. It offers better speed than previous one and is mostly used in business networks. The latest standard is 802.11g that removes the deficiencies of previous two standards. Since it offers best speed from other two standards, also it is the most expensive one.
The installation of this kind of network can be done by two ways. First one is ad-hoc mode and the second one is infrastructure mode. Ad-hoc mode allows wireless devices in a network to communicate on the logic of peer to peer with each other. However the second mode is the most required mode as it allows wireless devices in a network to communicate with a central device which in turn communicates with the devices that are connected with central device through wire. But both these modes have one similarity that they use wireless network adapters, termed as WLAN cards.
Wireless LAN costs more than the wired network as it requires wireless adapters, access points that makes it three or four times expensive than Ethernet cables, hubs/switches for wired network. Wireless network faces reliability problem also as compared to wired networks, because while installing the wireless network it may encounter the interference that can come from the household products like microwave ovens, cordless phone etc. Wi-Fi communication standard's performance is inversely proportional to the distance between the computers and the access points. Larger the distance between the computers and access point, smaller will be Wi-Fi performance and hence smaller will be performance of wireless network. Similarly, security wise it is less secure than the wired network because in wireless communication data is sent through the air and hence there are more chances that data can be intercepted.

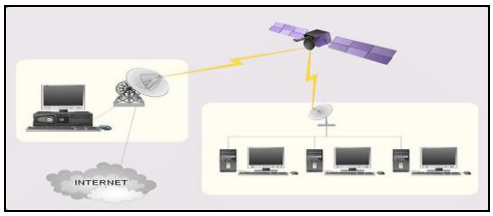


Figure 2 Wireless Networks

1.2 Advantages and Application of Ad-Hoc Networks

Ad hoc networks are wireless connections between two or more computers and/or wireless devices (such as a Wi-Fi enabled smart phone or tablet computer). A typical wireless network is based on a wireless router or access point that connects to the wired network and/or Internet. An ad hoc network bypasses the need for a router by connecting the computers directly to each other using their wireless network adapters.

Router Free

Connecting to files on other computers and/or the Internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an ad hoc network can be more affordable than a traditional network---you don't have the added cost of a router. However, if you only have one computer an ad hoc network won't be possible.

Mobility

Ad hoc networks can be created on the fly in nearly any situation where there are multiple wireless devices. For example: emergency situations in remote locations make a traditional network nearly impossible, but "The medical team can utilize 802.11 radio NICs in their laptops and PDAs and enable broadband wireless data communications as soon as they arrive on the scene."

Speed

Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution.

2. COMMON ROUTING IN MANETS

There is possibility of common protocols to be implemented in Mobile Ad-hoc networks. These protocols are commonly known as link state or distance vector kind of protocols. The major disadvantage of using these protocols in mobile Ad-hoc networks is that they are basically manipulated for static topology not for steady conditions in mobile Ad-hoc networks with great dynamic changing. Dynamic and Link sate routing can be applied efficiently with low mobility. But these routing techniques depend on messages with periodic control. Thus it shows its static nature, when the number of nodes is large, the potential destination may also be large, which can create problem. The requirement of frequent and abrupt change of data within network increases. Therefore these routing techniques should be operated in low mobility scenarios. One of the attribute of these common protocols is that they are bidirectional, for instance the transfer of data will be in both the directions between two hosts or clients. As mobile Ad-hoc networks has their own conventional routing protocols, to understand the difficulties and problems for the usage of common protocols it is necessary to develop the concept of following terms .

2.1 Link State Routing

In this state, every node develops the consistency to analyze complete topology and show the cost of each link. For the persistence of costs, every node periodically spreads costs of output links to other nodes by using the process of flooding. Flooding is the process to transfer updated version of packets to all nodes within network without any obstacle. When the node gets the information, it upgrades the network

policy and utilize shortest path to select the next hop for every target i.e. the path that delivers the lowest cost. There may be some problems may arise to view the node due to long spreader delays, distributed networks, such undetermined network topology may result into loop formation, but these loops are temporary they are vanished when the message is transferred to network.

2.2 Distance Vector Routing

In this routing scheme, every node views the cost of outgoing link. It disseminates periodically information to its neighbors and helps out to find the shortest path to every other node in the network, instead of promulgating information to all the nodes. The information received by nodes estimate routing table again through shortest path algorithm. Distance vector routing is more reliable, feasible to implement and short storage space is required for this routing, but one of the drawback of distance vector is the creation of short and large routing loops. Due to these loops nodes have to select their next hops in full distributed way depends on the information that should be refreshed.

2.3 Source Routing

In case of source routing, every packet has complete route information to the target or destination. This phenomenon or technique has the ability to remove the presence of routing loops. As source determines the routing path and information about the packet which travels through specified route, this technique is called as source routing technique. Moreover the addition of overhead in this approach is actually the larger packets which contain complete path information .

2.4 Flooding

The basic phenomenon to distribute routing or control information by usage of spreading or disseminating method, in which source nodes have the responsibility to send packets to all nodes in the network. Flooding is basically the implementation of broadcast method in wireless scenario. The source node sends the information to all neighbor nodes in wireless network. The neighbor nodes then forward this information to the entire node within their approach. So in this way, all the packets spread or flood within entire network. The packets are sequenced in number form to avoid staling information and loops.

3. PROPOSED ACK-BASED SCHEME

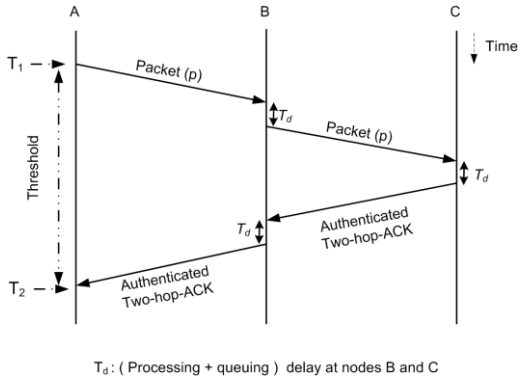
Proposed Modified Ack-Based scheme for node authentication with AODV existing protocol in MANET. Ack-Based scheme also provide facility for the detection of wormhole attack and node misbehaviors in ad hoc network. Different researcher proposed different scheme for Ack_Based for providing security in mobile ad hoc network. But all technique suffered common problem that problem is generation of huge amount of pack overhead and node ambiguity. Due to this problem the given scheme is not used in generalize form. So we proposed the Ack-Based scheme with the help of finite state machine for controlling a generation of packet and also improve performance of AODV protocol. Here first we discuss basic Ack-Based scheme and then we discuss finite state machine and finally we discuss combine approach for Ack-Based scheme.

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 in 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. The authors propose the 2Ack scheme to detect malicious links and to mitigate their effects. 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. According to the value of the acknowledgement ratio (Rack), only a fraction of data packets will be acknowledged in order to reduce the incurred overhead. This technique overcomes some weaknesses of the Watchdog/path rater such as: ambiguous collisions, receiver collision and power control transmission. Both of the previous works remain vulnerable to the attacks launched by group of nodes. To counter these attacks, provides a framework to mitigate the damage caused by the colluding black hole attack in AODV. The proposed technique has a moderate overhead induced by the ACK sent back by the destination during selected intervals of data transfer period. Throughout the data packets transmission, a flow of special packets is transmitted at random intervals along with the data. The reception of these special packets invokes the destination to send out an ACK through multiple paths. The ACK packets take multiple routes to reduce the probability that all ACK s being dropped by the malicious nodes, and also to account for possible loss due to broken routes or congestion in certain nodes. If the source node does not receive any ACK packet, then it becomes aware of the presence of attackers in the forwarding path. As a reaction, it broadcasts a list of suspected malicious nodes to isolate them from the network

All the nodes running a solution based on acknowledgment need to maintain a timeout (To) value. This timeout represents an upper bound of the time that the sender node has to wait for the ACK to arrive. The determination of this timeout value is critical since a small value induces a large number of false accusations and a large value increases the memory required to store the outgoing packets for further comparisons. Figure (3) depicts an

example of the lower bound of the timeout value maintained by node A for the reception of two hops ACK from node C. The timeout value should be greater than the estimated threshold (Th) value which can be calculated as follows

Th = T1-T2



Figuer 3: shows that state diagram of ack scheme

Where T1 and T2 are the sending (reception) time of the packet (Ack), respectively this threshold is estimated for a successful transmission at MAC layer without any retransmission, which is not a realistic assumption in MANETs, thus the timeout value should satisfy the following condition

To > Th + (avg rt × hop delay)

Where AV G RT is the average number of retransmissions of a packet at MAC layer, and hop delay is the one hop transmission delay which includes packet transmission delay, random Bakeoff delay at the MAC layer and the processing delay.

4. IMPLEMENTATION

The main code is implemented in aodv.cc and the functions are declared in aodv.h. In aodv_packet.h, the AODV message formats (RREQ, RREP, RERR and HELLO) are defined. Moreover the new message format FSAPAC (Finite state automata) has been added and defined in this file.

The main modifications have been done in aodv.cc.

a) When a mobile node is to send a data packet to a destination, it tries to find a route to the destination (FSARt_resolve).

b) If the mobile node does not have any valid route to the destination it broadcasts a RREQ message (send Request).

c) The RREQ message is eventually received by the destination or another node which knows a route to the destination (recvRequest).

d) The node sends a RREP/RREP_I message back to the originator of the RREQ (send Reply).

e) The originator of the RREQ receives the RREP/RREP_I message (recvReply) and starts sending data packets to the destination (find_send_entry if the destination is a fixed node).

Simulation is run for 100 seconds of simulated time. 10 of the 25 mobile nodes are constant bit rate traffic sources. They are distributed randomly within the mobile ad hoc network.

The time when the ten traffic sources start sending data packets is chosen uniformly distributed within the first ten seconds of the simulation. After this time the sources continue sending data until one second before the end of the simulation. The destination of each of the sources is one of the two hosts, chosen randomly.

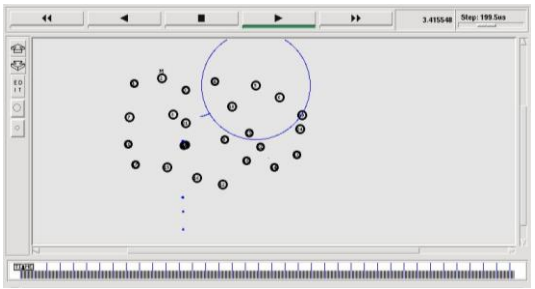


Figure 4: Simulation scenario of ACK-Based scheme on pause time 10 s

Figure 4 shows that the simulation scenario of ACK-Based scheme on pause time 10s that mans node mobility starting on this time and flow of control packet started.

5. CONCLUSION AND FUTUREWORK

Without infrastructure and node mobility in adhoc network is a great challenge as concern to the security. For security concern various method are used 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.

Suggestion of future work is to apply modified Ack-Based FSA add with other protocol to requirement of memory. During path discovery and path establishment it take much time in compression of normal Ack-Based schemes in future minimized route calculation with finite state machine.

REFERENCES

[1] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang" Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE Communication and survey 2010.

[2] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, In Proc. 6th annual international conference on Mobile computing and networking (MOBICOM '00), Boston, Massachusetts, USA, August 2000

[3] Y. C. Hu, A. Perrig and D. B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks, In Proc. 8th ACM International Conference on Mobile Computing and Networking, Westin

Peachtree Plaza, Atlanta, Georgia, USA, September 2002.

[4] D. Djenouri and N. Badache, New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks, In Proc. Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecurComm'05), Athens, Greece, September 200

[5] E. Gerhard's-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, In Proc. of the 33rd IEEE Conference on Local Computer Networks (LCN), Dublin, Ireland, and October 2007.

[6] Y. Zhang, W. Lou, W. Liu and Y. Fang, A secure incentive protocol for mobile ad hoc networks, Wireless Networks journal, 13(5): 569-582, October 2007.

[7] S. Kurosawa, H. Nakayama, N. Kato, A. jamalipour and Y. Nemoto, Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, International Journal of Network Security, 5(3): 338-346, November 2007.

[8] P. Agrawal, R. K. Ghosh and S. K. Das, Cooperative black and gray hole attacks in mobile ad hoc networks, In Proc. of the 2nd International Conference on Ubiquitous Information Management and Communication (ICUIMC 2008), SKKU, Suwon, Korea, Jan/Feb 2008.

[9] M. Amitabh, Security and quality of service in ad hoc wireless networks, Cambridge University Press; 1st edition, March 2008.

[10] Z. H. Zhang, F. Na¨ıt-abdesselam, P. H. Ho and X. Lin, RADAR: a ReputAtion-based scheme for Detecting Anomalous nodes in wireless mesh networks, In Proc. IEEE Wireless Communications and Networking Conference (WCNC2008), Las Vegas, USA, March 2008.

[11] B. Kannhavong, H. Nakamaya, Y. Nemoto, N. Kato and A. Jamalipour, SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks, In Proc. International Conference of Communication (ICC 2008), beijing, China, May 2008.

[12] S. Djahel, F. Na¨ıt-Abdesselam and A. Khokhar, An Acknowledgment- Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol, In Proc. of the International Conference on Communication (ICC 2008), beijing, China, May 2008.

[13] Z. Li, C. Chigan and D. Wong, AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs, In Proc. Global Communications Conference (IEEE GLOBECOM 08), New Orleans, LA, USA, NOV/DEC 2008

[14] www.cs.montana.edu/webworks

Author Profile

Mustafa Sadeq Jaafar persuing Mtech from Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. His areas of interest are Software Engineering and networks .

Mr. H K Sawant is working as an Professor in Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. He was awarded his Master of Technology Degree from IIT Mumbai. He is persuing his PhD from JJTU. His areas of interest are Computer Network, Software Engineering and Multimedia System. He has nineteen years experience in teaching and research. He has published more than twenty research papers in journals and conferences. He has also guided ten postgraduate students**.**