

ACK BASED SCHEME FOR PERFORMANCE IMPROVEMENT OF AD-HOC NETWORK

Mustafa Sadeq Jaafar¹, H. K. Sawant²

^{1,2}Department of Information Technology, Bharati Vidyapeeth Deemed University
College of Engineering, Pune-46, India
goblin.yankee@gmail.com

ABSTRACT

Dynamic topology and without infrastrure provide a great facility for adhoc network. Such facility generates easy installation of adhoc network and provides node mobility without loss of connection. In such facility packet dropping is a serious challenge for quality performance of adhoc network. Adhoc network suffered some security attack 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 huge overhead due to extra Acknowledgment packet and also suffered decision ambiguity if the requested node refuse to send back Acknowledgment. In this paper we modified ack-based scheme for decision ambiguity for requested node on the basis of finite state machine. Finite state machine is an automata of theory of computation here we used deterministic finite automate for the decision making of node and improved node authentication and minimize packet dropping in adhoc network.

KEYWORDS: wireless local area network, Wi-Fi communication standar, FSA, ns-2 , ACK based Scheme protocol for Ad-hoc networks.

I. 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.

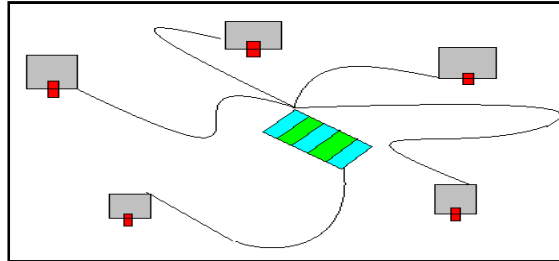


Figure 1 Wired Networks

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.

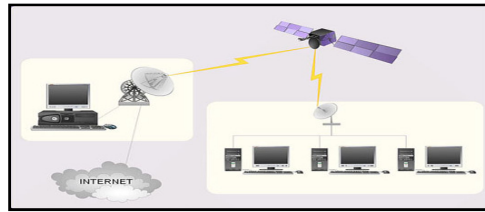


Figure 2 Wireless Networks

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.

II. PROPOSED SYSTEM

Dynamic topology and without infrastructure provide a great flexibility of adhoc network. These networks are usually constructed by using mobile and wireless hosts with minimum or no central control point of attachment, such as a base station. These networks can be useful in a variety of applications, such as one- off meeting networks, disaster and military applications, and the entertainment industry. Because the network topology of adhoc frequently changes, and there is no central management entity, all of the routing operations must be performed by the individual nodes in a collaborative fashion. In this environment two types of routing protocol are available one is table driven protocol and another one is on-demand routing protocol these protocols are AODV, DSR and DSDV[2]. AODV routing protocol is an on-demand routing protocol and DSDV is table driven routing protocol. Ad hoc On-Demand Distance Vector, AODV, is a distance vector routing protocol that is reactive. The reactive property of the routing protocol implies that it only requests a route when it needs one and does not require that the mobile nodes maintain routes to destinations that are not communicating. AODV guarantees loop-free routes by using sequence numbers that indicate how new, or fresh, a route is. The AODV protocol is one of the on-demand routing protocols for ad-hoc networks which are currently developed by the IETF Mobile Ad-hoc Networks (MANET) working group. It follows the distance vector approach instead of source routing. In AODV, every node keeps a local routing table that contains the information to which of its neighbors it has to forward a data packet so that it reaches eventually the desired destination. In general, it is desirable to use routes which have minimal length according to hop-count as a distance metric. However, AODV provides the functionality like DSR, namely to transport data packets from one node to another by finding routes and taking advantage of multiple hop communication. AODV is based on UDP as an unordered transport protocol to deliver packets within the ad-hoc network. Moreover, it requires that every node can be addressed by a network wide unique IP address and sends packets correctly by placing its IP address into the sender field of the IP packets [6]. This means also that AODV is expected to run in a

friendly network, where security is a minor concern. It should be mentioned that there are some attempts to extend AODV to prevent malicious nodes from attacking the integrity of the network by using digital signatures to secure routing control packets. Due to the lack of physical protection and reliable medium access mechanism, packet dropping attack represents a serious threat to the routing function in MANETs. A foe can easily join the network and compromise a legitimate node then subsequently start dropping packets that are expected to be relayed in order to disrupt the regular communications consequently, all the routes passing through this node fail to establish a correct routing path between the source and destination nodes. Dropping data packets leads to suspend the ongoing communication between the source and the destination node. More seriously, an attacker capturing the incoming control packets can prevent the associated nodes from establishing routes between them. Two hop ACK based scheme is proposed in [10] to 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. For the minimization of packet overhead and node ambiguity we used FSA (finite state automata) in ack-based routing protocol in aodv routing protocol for packet dropping.

III. ACK-BASED SCHEME AND LIMITATION

In security concern adhoc network is a challenging task to maintain security due to node mobility. Adhoc suffered various attack problem such as black hole attack, wormhole attack and sinkhole attack all attack arise a packet dropping in adhoc network. For this problem various authors deals a different –different approach such as node authentication, node feedback system and ack-based scheme. Ack-based scheme are suitable approach for minimization of packet dropping problem but it also suffered. Ack-based scheme used for OLSR routing protocol but in this paper we used for AODV protocol. ACK-based scheme deals as two hops ACK based scheme is proposed in [1] to 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 [30] 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. 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. The reception of these special packets invokes the destination to send out an ACK through multiple paths [12]. The ACK packets take multiple routes to reduce the probability that all ACKs 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.

AODV has the combined approach of DSR and DSDV protocol. DSDV maintains routes to all destinations, with periodical route information flooding and uses sequence numbers to avoid loops. AODV inherits the sequence numbers of DSDV and minimizes the amount of mute information flooding by creating routes on-demand, and improves the routing scalability and efficiency of DSR[3], which carries the source route in the data packet. In AODV protocol, to find a route to the destination, the source broadcasts a route request packet (RREQ). Its neighbors relay the RREQ to their neighbors until the RREQ reaches the destination or an intermediate node that has fresh route information. Then the destination or this intermediate node will send a mute reply packet with respect

to the source node along the path from which the first copy of the RREQ is received. AODV uses sequence numbers to determine whether route information is fresh enough and to ensure that the routes are loop free.

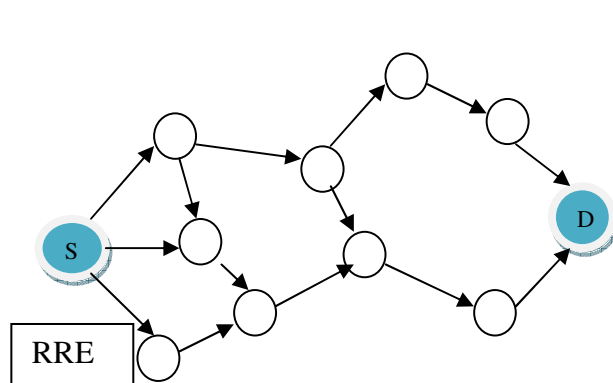


Figure 1 :(a) Source node S initiates the path

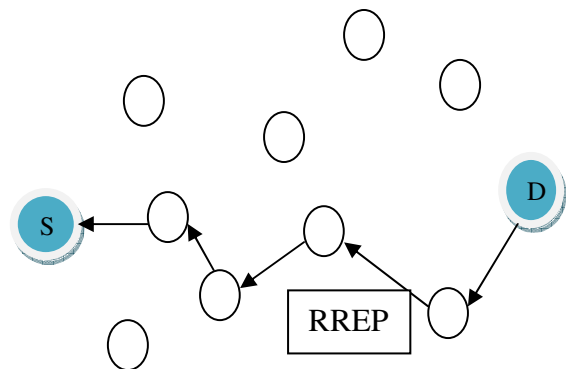


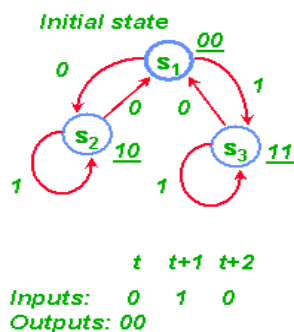
Figure 1 :(b) A RREP sent back to the source

The path discovery is established whenever a node wishes to communicate with another, provided that it has no routing information of the destination in its routing table. Path discovery is initiated by broadcasting a route request control message “RREQ” that propagates in the forward path. If a neighbor knows the route to the destination, it replies with a route reply control message “RREP” that propagates through the reverse path. Otherwise, the neighbor will re-broadcast the RREQ. The process will not continue indefinitely, however, authors of the protocol proposed a mechanism known as “Expanding Ring Search” used by Originating nodes to set limits on RREQ dissemination. AODV maintains paths by using control messages called Hello messages, used to detect that neighbors are still in range of connectivity [6, 7]

A finite state machine is a machine (or computer) that has only a finite, fixed number of states that it can be in during any point of a calculation [14]. A coke machine only has a finite number of states representing how much money has been inserted so far (if more than the maximum amount possible is input, the change is simply returned). A car wash has a state for each phase of the wash. It is reasonable to require that any model of a computer we analyze for solving real problems be restricted to having only a finite number of states. After all, in real life nothing is infinite, so we could never expect to build a computer with an infinite number of anything, states included. Formally, a finite state machine can be defined as follows: A finite state machine (FSM) is a five-tuple, $M = (Q, \Sigma, \delta, q_0, F)$ (Where $\delta: Q \times \Sigma \rightarrow Q$, $q_0 \in Q$, $F \subseteq Q$ (F is a subset of Q))

FSM Representations

State Transition Graph



State Transition Table

T(S, I)			O(S)	
0	1		s ₁	s ₂
s ₁	s ₂	s ₃	s ₁	00
s ₂	s ₁	s ₃	s ₂	10
s ₃	s ₂	s ₁	s ₃	11

Figure 2: shows FSM with table

IV. MODIFIED ACK-BASED SCHEME WITH FSA

In the existing ack-based scheme uses 2ack process for the node authentication process in attack scenario in adhoc 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 maintaoing a request packet acknowledgment we calculate the next hop with dsdv protocol concept. Path state maintains a sequence of ack packet. Here give a simple table for ack based FSA machine.

Table-I process state of Ack with FSM

Node	path	RREQ PACK	RREP	FSA
A	source	broadcast	none	Q0
B	A-B	B receive	A wait	Q0
C	A-C	C receive	B reply	Q1
D	B-D	D receive	B wait	Q0
E	destination	E receive	D reply	Q1

In this fashion maintain a path state between sources to destination node and remove the overhead of packet of acknowledgment with finite state machine. Also remove node ambiguity due to request node because the request node maintain a state machine on the time of reply then node state are chanced over that new request are generate. From that fashion we remove packet overhead in ack-based scheme.

V. SIMULATION PARAMETER AND RESULT ANALYSIS

In the simulation of modified ack-based scheme we used ns-2 simulator and find the performance of technique on the given parameter.

Table-II simulation parameter

Parameter	value
Simulation duration	100 sec
Simulation area	1000*1000
Number of mobile node	25
Traffic type	Cbr(udp)
Packet rate	4 packet/sec
Abnormal node	2
Host pause time	10sec

VI. CONCLUSION AND FUTURE SCOPE

In this paper we modified ack-based scheme for migrating packet dropping in adhoc network. In The modification process we used finite state machine for maintain the state of node request and reply of responding node. Finite state machine maintain a path link between source and destination during broadcasting. Here use of finite state machine need some extra memory for the maintaining the state of finite state machine. Our simulations find better result in comparison of old ack-based node authentication technique. In future we minimise the memory capacity for maintaining the finite state and also reduced delay rate of our modification.

REFERENCES

- [1] Soufiene Djahel, Farid Na`it-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 2005
- [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`it-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`it-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

Authors

Mustafa Sadeq Jaafar pursuing 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 .



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 pursuing 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.

