International Journal on Emerging Technologies **2**(2): 102-105(2011)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Migrating Packet Dropping in Adhoc Network Based on Modified ACK-based Scheme Using FSA

Satyendra Tiwari, Anurag Jain and Gajendra Singh Chowhan

Department of Computer Science and Engineering, RITS, Bhopal, (MP)

(Received 10 August, 2011, Accepted 14 September, 2011)

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 droping 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 a 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: Adhoc network, aodv , FSA, ns-2

I. INTRODUCTION

Dynamic topology and without infrastrure 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 on is table driven protocol and another one is on-demand routing protocol these protocol are AODV,DSR and DSDV[2]. AODV routing protocol is a 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 it 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. The remainder of this paper is organized as follows. Section II ACK-based Scheme and limitation. Section III explains AODV and FSA. Section IV explains modified ack-based scheme with FSA. Section V explains simulation parameter and result analysis. Section VI conclusion and future scope.

II. 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 suck as blackhole 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 droping problem but it also sufferd. Ack-based scheme used for OLSR routing protocol but in this paper we used for AODV protocol. ACK-based scheme deals as Two hop 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 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/pathrater 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.

III. AODV AND FSA

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 cames 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.

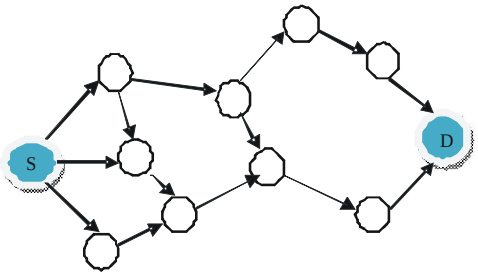

Fig. 1. (*a*) Source node S initiates the path.

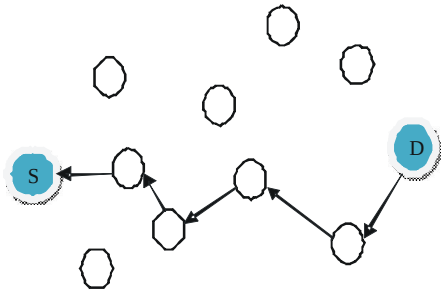

Fig. 1. (*b*) A RREP sent back to the source.

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 an 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 δ: $Q \times \Sigma \rightarrow Q$, $q_0 \in Q$, $F \subseteq Q$ (F is a subset of Q)].

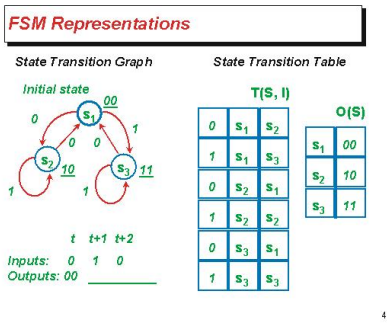

Fig. 2. shows FSM with table.

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 maintaing a state of node .that memory area maintain a path state due to given request and response. For maintaoing a reqest 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 1: process state of ack with FSM.

Node	*Path*	*RREQ PACK*	*RREP*	*FSA*
A	Source	Broadcast	None	Q_0
B	*A-B*	*B* receive	*A* wait	Q_0
C	*A-C*	*C* receive	*B* reply	Q_1
D	*B-D*	*D* receive	*B* wait	Q_0
E	Destination	*E* receive	*D* reply	Q_1

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 2: 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

Result graph of AODV routing protocol with ack-based scheme and modified scheme.

Fig. 3. Shows that the comparative packet delivery ratio between ack and modified ack.

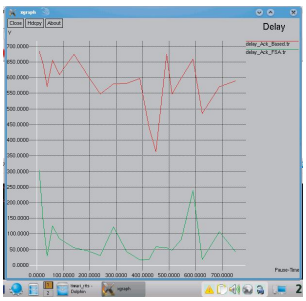

Fig. 4. Shows that the comparative delay rate between ack and modified ack.

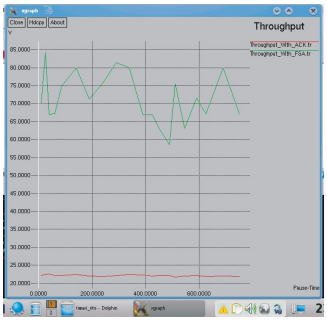

Fig. 5. Shows that the Throughput between ack and modified ack.

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 manitaing the state of node request and reply of responeding node. Finite state machine maintain a path link between source and destination during broadcasting. Here use of finite state mahine need some extra memory for the maintaining the state of finite state machine.our simulation find better result in comprasion of old ack-based node authentication technique. In future we minimise the 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 (Secur Comm'05), Athens, Greece, September (2000)

[5] E. Gerhards-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, 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