Volume 2, Issue 3, March 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Secure AODV For Ad Hoc Networks Routing Mechanism

Ankit Aggarwal
Department of Computer Sc. Engineering
Modern Institute of Engineering &Technology
Shahabad, Distt.Kurukshetra, Haryana (India)
Ankit.aggarwal61@gmail.com

Bhumika Garg
Department of Computer Sc.Engineering
Modern Institute of Engineering & Technology
Shahabad(M), Distt.Kurukshetra.Haryana(India)

Abstract*— Ad-hoc networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad-hoc environment. AODV is an on demand routing network protocol which is specially design for Ad hoc network. This protocol is Mixture of DSR and DSDV routing protocol. Ad Hoc network is particularly vulnerable due to the lack of any centralized infrastructure. However, the typical on demand routing protocols for Ad Hoc networks such as AODV and DSR have no security considerations and trust all the participants to correctly forward routing and data traffic. In this paper, the foundational conception of Ad Hoc networks and the routing attacks in them are introduced. A secure routing solution based on watchdog mechanism and credence value mechanism is proposed over the AODV. The watchdog mechanism is defined to judge whether a node has abnormal behaviour in process of forwarding information. The credence value mechanism is used to evaluate a node's credit standing. The performance of average end-to-end delay, packet drop ratio, routing load and average throughput are proved well by computer simulation

***Keywords*— Ad-hoc wireless network; Routing Algorithm; AODV; Forward Route; Reverse Route**

I. INTRODUCTION

Ad-hoc networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad-hoc environment. AODV is an on demand routing network protocol which is specially design for Ad hoc network. This protocol is Mixture of DSR and DSDV routing protocol. Ad Hoc network is particularly vulnerable due to the lack of any centralized infrastructure. However, the typical on demand routing protocols for Ad Hoc networks such as AODV and DSR have no security considerations and trust all the participants to correctly forward routing and data traffic. In this paper, the foundational conception of Ad Hoc networks and the routing attacks in them are introduced. A secure routing solution based on watchdog mechanism and credence value mechanism is proposed over the AODV. The watchdog mechanism is defined to judge whether a node has abnormal behavior in process of forwarding information. The credence value mechanism is used to evaluate a node's credit standing. The performance of average end-to-end delay, packet drop ratio, routing load and average throughput are proved well by computer simulation

2 AD HOC Network Attack and Security Protocol

Routing attacks in Ad Hoc networks can be classified into two types, passive and active [3]. In a passive attack, the attacker does not disrupt the operation of a routing protocol but only eavesdrops on the network. Because the passive attack does not affect the performance of network we do not discuss it in this paper. In an active attack, the attacker must be able to inject some packets into the network. The latter type of attack is particularly powerful and fatal. Some types of active attacks, including black hole, neighbour attack, wormhole, denial of service (DoS),

2.1 Security Mechanism

Mutual neighbour listening mechanism

We call a node is a mutual neighbor if it is the neighbor of two different nodes. Just as shown in Figure 1, node X is mutual neighbor it is the neighbor of both A and B. Node
Y and Z are also mutual neighbours

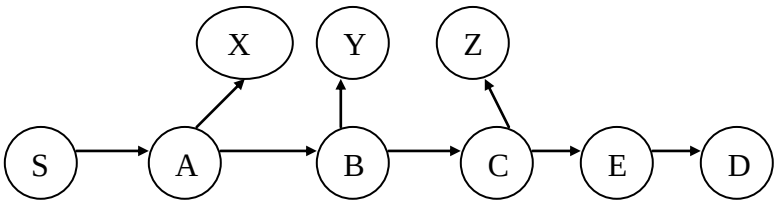

Figure 1 mutual neighbour listening mechanism

We assume node B is malicious node. S is the source node and D is the destination node. When A forwards RREQ or data packets or sends back RREP, X listens to A just like a watchdog [12], Including the information from S whether has been forwarded or not, which node receives the forwarding information, and whether the information has been tampered or not. Because X knows the next hop of A, black hole attack and wormhole attack will be detected. If just using S to listen to A, the malicious node cannot be detected when multiple nodes (node A and B for example) collude to bring the network
down for S does not know the next hop of A. This is the reason the concept of mutual neighbor is introduced.

3. Secure routing in Ad-hoc networks

3.1 Problems associated with Ad-hoc routing

.

Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing. The nodes themselves are responsible for routing packets. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them.

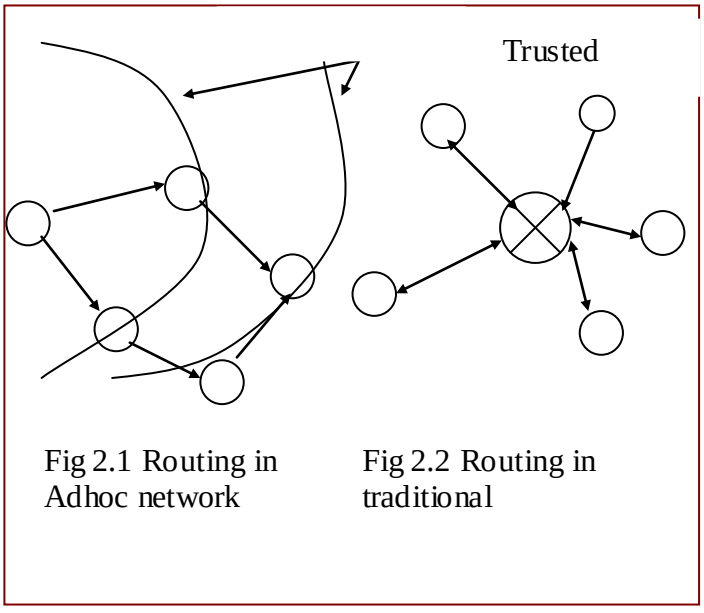

Figure-2 Problems associated with Ad-hoc routing

3.1.2 Problems associated with wireless communication

. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems

1.3 Problems with existing Ad-hoc routing protocols

3.1.3.1 Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in

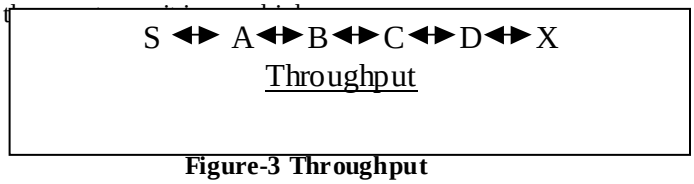

Figure-3 Throughput

3.1.3.2 Attacks using modification of protocol fields of messages

Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields.

3.2 Solutions to problems in Ad-hoc-routing Protocol

3.2.1Security-Aware Ad-hoc Routing (SAR)

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key).

A node initiating route discovery sets the sought security level for the route i.e. the required minimal trust level for nodes participating in the query/ reply propagation. Nodes at each trust level share symmetric encryption keys. Intermediate nodes of different levels cannot decrypt in-transit routing packets or determine whether the required security attributes can be satisfied and drop them. Only the nodes with the

correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level, since only they can decrypt the packet, see its header and forward it,

4. Results Analysis

4.1 Black hole attack

The performance of average end-to-end delay, packet drop ratio are evaluated by computer simulation using ns-2 [13] by putting the watchdog mechanism and credence value mechanism into AODV. We also watch carefully the differences between the normal AODV and AODV under attacks, in which some nodes are made to play the role of attackers. The nodes in the computer simulation move according to the Random Waypoint Algorithm [11]. The scenario is defined with a set of parameters as follows

- Number of nodes: 50.
- Number of malicious nodes: 5.
- Simulation area: 1000m×1000m.
- Date rate: 1 packet / s.
- Packet size: 512 byte.
- Traffic type: CBR.
- Maximum speed: 20 m/s.
- Simulation duration: 600 seconds.
- Physical link bandwidth: 2 Mbps.
- MAC layer: IEEE 802.11.

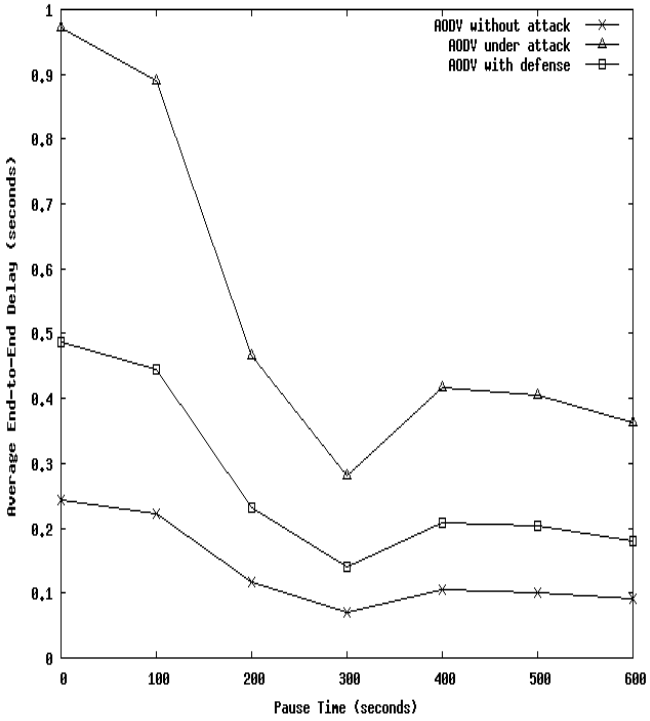

Figure 4- average end-to-end delay Vs pause time

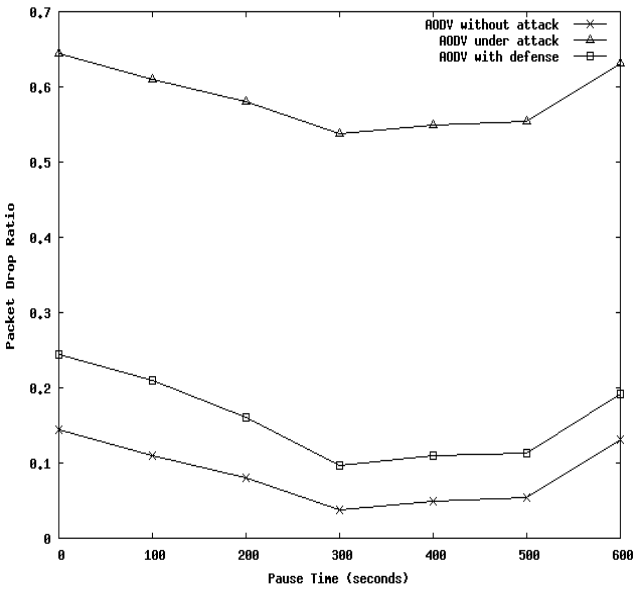

Figure5- packet drop ratio Vs pause time

5. CONCLUSIONS AND FUTURE WORK

In this paper, a secure mechanism in AODV for Ad Hoc networks is proposed to detect attack behaviours. We presented a novel approach to prevent the maliciously packet dropping with considering the number of neighbor each node should have. The paper presents the solution for further attacks (both passive and active) which were implemented in network layer.

Ad-hoc networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. In this paper we attempt to analyze the demands of Ad-hoc environment.

Reference.

[1] C. E. Perkins and E. M. Royer. "The Ad Hoc On-Demand Distance Vector Protocol," in Proc. C. E. Perkins (Ed.), Ad Hoc Networking, pp. 173–219. Addison-Wesley, 2000
.

[2] C. E. Perkins and P. Bhagwat. "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in Proc. SIGCOMM 94: Computer Communications Review, 24(4), pp. 234–244, October 1994

[3] C. E. Perkins, E. M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[4] C.E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Workshop, Mobile Comp. Sys. And Apps. Feb. 1999, pp. 90 – 100.

[5] N. Uushona and W T Penzhorn, "Towards the Security of Routing in Ad Hoc Networks," IEEE ISIE 2005, June 20-23, 2005
.

[6] Yih-Chun Hu, Adrian Perring and David B. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[7] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," IEEE ICNICONSMCL'06, 2006

[8] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer , "A Secure Routing Protocol for Ad Hoc Networks," In Proceedings of 2002 IEEE International Conference on Network Protocols(ICNP), November 2002

[8] Yih-Chun Hu, Adrian Perrig, David B. Johnson "Ariadne A secure On-Demand Routing Protocol for Ad Hoc Networks," in Proceedings of the MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA

[9] M. G. Zapata, "Secure ad hoc on-demand distance vector AODV)," [S]. Routing. Mobile Ad Hoc Networking Group, INTERNET DRAFT, Aug, 2001.

[10] P. Papadimitratos, Z. Haas, "Secure routing for mobile Ad Hoc networks," in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 27-31,2002

[11] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," In: Proceedings of MOBICOM'98, Dallas, TX, 1998 pp. 85-97.

