ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Simulation and Review of SAODV NS2 Simulation

Er. Kamaljit Kaur[*1], Er. Amanpreet Kaur Chela[2]
[*1,2] Ramgarhia Institute of Engineering & Technology, Phagwara, Punjab, India
Lotus.kml.816@gmail.com

Abstract

Wireless mobile ad-hoc networks are networks without using any physical connections. These networks Does not have any fixed topology due to the mobility of the nodes, path loss, multipath propagation, and interference. For this task many routing Protocols have been developed. The purpose of this Review paper is to Review and understand, two mobile ad-hoc routing protocols AODV and SAODV.

AODV is a popular reactive routing protocol in MANET. The reactive indicates that a node exchanges routing information only when it has some data to transfer and keeps the routing information renew as long as the communication with the node is available. But AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to AODV rules. To make overall network secure, SAODV is being introduced.

SAODV (Secured Ad-Hoc on Demand Vector Routing) is one of the existing secured mechanisms which use digital signature and hash chain function to secure AODV packets. Secured AODV improves the AODV message format by including the security parameter for securing the routing messages.

The goal of this master thesis is to analyze and simulate AODV & SAODV routing protocols using NS2.

Keywords: AODV, SAODV, Digital Signatures, Hash Chain Function.

Introduction

` Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Figure 1.1 illustrates what MANET is. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

Wireless Ad hoc Networks are gaining its popularity day by day because the devices communicate with each other using wireless physical medium without relying on pre existing wired infrastructure.

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure.

The Adhoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the adhoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed in an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure-based wireless networks. This section discusses the security goals for an ad hoc network. Sample attacks and threats against existing MANET routing protocols are then discussed. I then discuss the working of secure routing protocol to address these threats SAODV.

Problem Formulation

A. AODV Terminology

This protocol specification uses conventional meanings for capitalized words such as MUST, SHOULD, etc., to indicate requirement levels for various protocol features.

- **Active route**: A route towards a destination that has a routing table entry that is marked as valid. Only active routes can be used to forward data packets.
- **Broadcast**: Broadcasting means transmitting to the IP Limited Broadcast address, 255.255.255.255. A broadcast packet may not be blindly forwarded, but broadcasting is useful to enable dissemination of AODV messages throughout the ad hoc network.
- **Destination**: An IP address to which data packets are to be transmitted. Same as "destination node". A node knows it is the destination node for a typical data packet when its address appears in the appropriate field of the IP header. Routes for destination nodes are supplied by action of the AODV protocol, which carries the IP address of the desired destination node in route discovery messages.
- **Forwarding node**: A node that agrees to forward packets destined for another node, by retransmitting them to a next hop that is closer to the unicast destination along a path that has been set up using routing control messages.
- **Forward Route**: A route set up to send data packets from a node originating a route Discovery operation towards its desired destination.
- **Invalid Route:** A route that has expired, denoted by a state of invalid in the routing table entry. An invalid route is used to store previously valid route information for an extended period of time. An invalid route cannot be used to forward data packets, but it can provide information useful for route repairs, and also for future RREQ messages.
- **Originating Node:** A node that initiates an AODV route discovery message to be processed and possibly retransmitted by other nodes in the ad hoc network. For instance, the node initiating a Route Discovery process and broadcasting the RREQ message is called the originating node of the RREQ message.
- **Reverse Route:** A route set up to forward a reply (RREP) packet back to the originator from the destination or from an intermediate node having a route to the destination.
- **Sequence Number:** A monotonically increasing number maintained by each originating node. In AODV routing protocol messages, it is used by other nodes to determine the freshness of the information contained from the originating node.
- **Valid Route:** See active route.

B. SECURITY THREATS IN AODV

In this section, the security threats are illustrated and analyzed for AODV routing protocol. A node is malicious if it is an attacker that cannot identify itself as a legitimate node due to the lack of valid cryptographic information. A node is compromised if it is an inside attacker who is behaving maliciously but can be identified by the network as a legitimate node and is trusted by other nodes. A node is called selfish when it tends to deny its own resources for the benefits of other nodes in order to save its own resources. Since AODV has no security mechanisms several attacks can be launched against the AODV routing protocol:

- **Message tampering attack:** An attacker can alter the content of routing messages and forward them with falsified information, for example, when forwarding a RREQ generated by a source node to discover a route to the destination node, an attacker can reduce the hop count field to increase the chances of being in the route path between source and destination so it can analyze the communication between them. A variant of this is to increment the destination sequence number to make the other nodes believe that this is a ‘fresher’ route. Simulations results show that a single attacker can drop up to 75% of packets by manipulating destination sequence numbers in some scenarios.
- **Message dropping attack:** Both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. Since all the mobile nodes within a MANET function as both end hosts and router, this attack can paralyze the network completely as the number of message dropping increase.

- **Message reply (or wormhole) attack:** Attackers can retransmit eavesdropped messages again later in a different place. One type of reply attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets.

C. SECURITY REQUIREMENTS FOR AODV ROUTING PROTOCAL

- **Source authentication:** To be able to verify that the nodes the one it claims to be.
- **Neighbor authentication:** The receiver should be able to confirm that the identity of the sender (i.e. one hop previous node) is indeed who or what it claims to be.
- **Message integrity:** To be able to verify that the routing information that is being send, has arrived unaltered.
- **Access control:** It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights

D. PROPOSED SOLUTION

Several security aware routing protocols have been proposed. In this thesis, I have chosen to work with two of them, ARIADNE and Secure Ad hoc On-demand Distance Vector (SAODV), both of which are fairly popular and represent state-of-the-art secure routing solutions in MANETs

E. SAODV

The Secure Ad hoc On-Demand Distance Vector (SAODV) is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation. Manet protocols are being designed without having security in mind. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each node is capable of securely verifying the association between the address of other node and the public key of that node. A key management scheme is needed for SAODV. Two mechanisms are used to secure the AODV messages:

Digital signatures to authenticate the non-mutable fields of the messages, and Hash chains to secure the mutable hop count field of the message. For the non-mutable fields, authentication can be performed in a point-to-point manner, but the techniques cannot be applied to the mutable information. Route error messages are protected in a different manner because of a big amount of mutable information. According to the author, it is not important which node started the route error and which nodes are just forwarding it. The important information is that a neighbor node is informing other nodes that it is not able to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole RERR message and that any neighbor that receives RERR verifies the signature. The RREQ and RREP have the following extension fields

<Type, Length, Hash function, Max Hop Count, Top hash, Signature, Hash >

The RERR has the following extension fields

<Type, Length, Reserved, Signature >

Objective

The purpose of this master thesis is to study, understand and analyze two mobile ad-hoc routing protocols AODV and SAODV. Both are reactive protocols, they find a route to a destination on demand, whenever communication is needed.

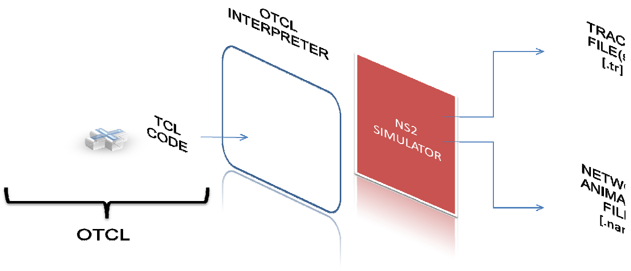
The general objectives can be outlined as follows:

- Get a general understanding of ad -hoc networks.
- Literature review of AODV and SAODV.
- Generate a simulation environment that could be used for further studies.
- Implement AODV and SAODV routing protocols for Mobile ad-hoc networks.
- Analyze the protocols through simulation and verify it on the basis of literature review.

Methodology Used

NS2 is being used a research methodology to simulate AODV and SAODV routing protocols. The network simulator *ns-2* is an object-oriented, discrete event-driven network simulator. It is a very useful tool for conducting networks simulations involving local and wide area networks, but its functionality has grown during recent years to include wireless networks and ad-hoc networking as well. The ns-2 network simulator has gained an enormous popularity among participants of the research community, mainly because of its simplicity and modularity. It allows *simulation scripts*, also called *simulation scenarios*, to be easily written in a script-like programming language, OTcl. More complex functionality relies on C++ code that either comes with ns-2 or is supplied by the user. This flexibility makes it easy to enhance the simulation environment as needed, although most common parts are already built-in, such as wired nodes, mobile nodes, links, queues, agents (protocols) and applications. Most network components can be configured in detail, and models for traffic patterns and errors can be applied to a simulation to increase its reality. There even exists an emulation feature, allowing the simulator to interact with a real network. Simulations in ns-2 can be logged to *trace files*, which include detailed information about packets in the simulation and allow for post-run processing with some analysis tool. It is also possible to let ns-2 generate a special trace file that can be used by *NAM (Network Animator)*, a visualization tool that is part of the ns-2 distribution. This allows simulations to be replayed on screen, which can be useful for complex simulations.

F. COMPONENTS OF NS/2



Facilities Required By Proposed Work

A. PERFORMING SIMULATION

The starting point for performing simulations in ns-2 is to build an OTcl simulation scenario script file that specifies the components to be used and the events that should occur. An example scenario could e.g. set up a network topology consisting of two nodes, connect these two using a 10 Mbps duplex link, set up FTP traffic over TCP, and start and stop this traffic at certain points in time.

B. MAIN BUILDING BLOCKS

In general, a simulation scenario consists of three main components:

- A network topology
- Connections, traffic and agents (protocols)
- Events and failures

A network topology defines the number of nodes and their connectivity, and can either be created manually or with special topology generators such as GT-ITM. Connections and traffic are set up by traffic generators and agents (protocols) at a node. Events and failures include connection set-ups/tear-downs, packet flow, packet loss, congestion and mobile node movements.

C. SIMULATION & EXECUTION

A simulation scenario script is executed (i.e., a simulation is performed) by supplying the file name on the command line to the ns-2 simulator. The simulator acts as an OTcl interpreter, interpreting the simulation scenario script line by line. Any error messages or messages generated by the script will be printed to the console. When the simulation has finished, the simulator exits and the command shell prompt returns. No graphical user interface is supplied with ns-2 for performing simulations. After successfully performing a simulation, the trace files that may have been produced by the simulation scenario script can be analyzed. Depending on the objectives of the simulation, this can either be done with a full-fledged analysis tool such as Trace graph or with simpler, hand-made scripts (usually Perl, sed orawk scripts) or programs.

D. OTCL/C++ ENVIRONMENT

To increase flexibility and efficiency, ns-2 uses *two* programming languages for its operation; C++ and OTcl. C++ is mainly used for event handling and per-packet processing; tasks for which OTcl would become too slow. OTcl is commonly used for simpler routing protocols, general ns-2 code and simulation scenario scripts. The usage of OTcl for simulation scenario scripts allows the user to change parameters of a simulation without having to recompile any source code. The two programming languages are tied together in the sense that C++ objects can be made available to the OTcl environment (and vice versa) through an OTcl linkage. This linkage creates OTcl objects for C++ objects and allows variables of C++ objects to be shared as well. In addition, it offers access to the OTcl interpreter from C++ code. This makes it possible to implement network components in OTcl, C++ or both. Furthermore, these components can easily be configured from the simulation scenario script because of the OTcl linkage, so the choice of programming language used for the implementation is completely transparent to the user.

References

[1] MANET,.http://www.ietf.org/html.charters/ manet charter.

[2] Manel Guerrero Zapata, "Secure Ad hoc On Demand Distance Vector (SAODV) Routing", Nokia Research Center, Mobile Ad Hoc Networking Working Group, Internet Draft, 12 August, 2001.

[3] C. Perkins, E. Belding-Royer, S. Das ," Ad hoc On-Demand Distance Vector (AODV) Routing" Network Working Group.

[4] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song "Experimental Comparisons between SAODV and AODV Routing Protocols, WMuNeP'05, October 13.

[5] Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment" European Journal of Scientific Research, Vol No 32, pp. 430-443, 2009.

[6] Nidhi Sharma, (Student M.Tech.), R.M. Sharma, "Provisioning of Quality of Service in MANET"s performance Analysis & Comparison (AODV & DSR)", IEEE,2010, V7-243.

[7] M. F. Juwad, and H. S. Al-Raweshidy, "Experimental Performance Comparisons between SAODV & AODV", IEEE Second Asia International Conference on Modeling & Simulation, 2008..

[8] Tuan Anh Nguyen, B.S."Evaluations of MANET Routing Protocols in Maicious Environment" University of Houston-Clear Lake, May 2006.

[9] Patroklos G. Argyroudis, Donal O"Mahony, "Secure Routing for Mobile Ad hoc Networks", Department of Computer Science University of Dublin.

[10] Junaid Arshad and Mohammad Ajmal Azad, Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks", 1-4244-0626-9/06 © 2006 IEEE.

[11] Syed Md. Ashraful Karim," Simulation of New Security Elements in an Ad Hoc Network" Norwegian University of Science & Technology.

[12] Prof. Dr. Horst F. Wedde, ME Muddassar Farooq BeeAdHoc Efficient/Secure/Scalable Routing Framework fur AdHoc Netze" University of Dortmund, Project Group 460.

[13] L.Ertaul, D.Ibrahim, "Evaluation of Secure Routing Protocols in Mobile Ad Hoc Networks (MANETs)", Department of Mathematics & Computer Science, California University.

[14] The NS Manual, http://www.isi.edu/nsnam/ns.

[15] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/Tutorial/index.html

[16] M.S. Corson, J. Macker, Mobile ad hoc networking: routing protocol performance issues and evaluation considerations. Internet RFC January 1999, ttp://www.ietf.org/rfc/rfc2501.txt.

[17] Azzedine Boukerche, Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks, Mobile Networks and Applications 9, 333–342, 2004 Kluwer Academic publishers. Manufactured in The Netherlands.

[18] M. Guerrero Zapata, "Key Management and Delayed Verification for Ad Hoc Networks", J. High Speed Networks, vol. 15, no. 1, Jan. 2006, pp. 93–109.

[19] Manel Guerrero Zapata, "Secure Ad hoc On Demand Distance Vector (SAODV) Routing", Technical University of Catalonia (UPC), Mobile Ad Hoc Networking Working Group, Internet Draft, 15 September 2005.

[20] Manel Guerrero Zapata, N. Asokan, "Securing Ad Hoc Routing Protocols", WiSe'02, September 28, 2002, Atlanta, Georgia, USA, ACM 1-58113-585-8/02/0009 Copyright 2002.

[21] Seung Yi, Prasad Naldurg, Robin Kravets, "A Security-Aware Routing Protocol for WirelessAd Hoc Networks", Dept. of Computer Science, University of Illinois at Urbana-Champaign Urbana, Illinois.

[22] Patroklos G. Argyroudis, Donal O'Mahony, "Secure Routing for Mobile Ad hoc Networks", Department of Computer Science University of Dublin.

[23] Sonali Bhargava and Dharma P. Agrawal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks", 0-7803-7005-8/01 © 2001 IEEE

[24] Stephan Eichler and Christian Roman, "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC", 1-4244-0507-6/06 © 2006 IEEE

[25] J. Martin Leo Manickam, R. Bhuvaneswari, M.A. Bhagyaveni and S.Shanmugavel, "SecureRouting Protocol for Mobile Ad-Hoc Networks", ISBN # 1-56555-316-0, SCSC 2007

[26] N.Shanthi and Dr. L.Ganesan, "Security In Multicast Mobile Ad-Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008

[27] Krishna Gorantala, —Routing in Mobile Ad-hoc Networks Umea University, Sweden, June-2006.

[28] Geetha Jayakumar and Gopinat Ganapathy,—Performance Comparison of Mobile Adhoc Network Routing Protocol,

International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.11, pp. 77-84 November 2007.

[29] *Laura Marie Feeney, —A taxonomy for routing protocols in mobile ad hoc networks, Technical report, Swedish Institute of Computer Science, Sweden, 1999.*

[30] *C.E.Perkins and E.M. Royer,—Ad-hoc On-Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.*

[31] *E. M. Royer and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications Magazine, vol. 6, no. 2, pp. 46–55, 1999.*

[32] *S. Corson and J. Macker, "Mobile ad-hoc networking (manet): Routing protocol performance issues and evaluation considerations," IETF MANET, RFC 2501, 1999.*

[33] *Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure ondemand routing protocol for ad hoc networks," Proceedings of the EighthAnnual International Conference on Mobile Computing and Networking (MobiCom), pp. 12–23, 2002.*

[34] *B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," Proceedings of the International Conference on Network Protocols (ICNP), pp. 78–87, 2002.*

[35] *A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," Proceedings of the 27th Australasian Computer Science Conference (ACSC), vol. 26, no. 1, pp. 47–54, 2004.*

[36] *W. Wang, Y. Lu, and B. Bhargava, "On vulnerability and protection of ad hoc on-demand distance vector protocol," Proceedings of the International Conference on Telecommunication (ICT), pp. 375–382, 2003.*

[37] *L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, 1999.*

[38] *L. Klein-Berndt. Kernel AODV from National Institute of Standards and Technology (NIST). http://w3.antd.nist.gov/wctg/aodv kernel/*

[39] *V. Kawadia, Y. Zhang, and B. Gupta, "System Services for Implementing Ad-Hoc Routing: Architecture, Implementation and Experiences," in Proc. of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys), San Francisco, CA, June 2003.*

[40] *Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure Ondemand Routing Protocol for Ad-hoc Networks," in Proc. Of ACM MobiCom, Atlanta, GA, Sept. 2002.*

[41] *S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," in Proc. of ACM MobiCom, Boston, MA, Aug. 2000.*

[42] *K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad-hoc Networks," in Proc. of International Conference on Network Protocols (ICNP), Paris, France, Nov. 2002.*

[43] *P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad-hoc Networks," in Proc. of SCS Communication Networksand Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, Jan. 2002.*

[44] *C.K. Toh, M. Delwar, and D. Allen, "Evaluating the Communication Performance of an Ad Hoc Wireless Network," IEEE Trans. on Wireless Communications, vol. 1, no. 3, pp. 402-414, July 2002.*

[45] *E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Personal Communications, Apr. 1999.*

[46] *L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, Nov. 1999.*

[47] *W. Stallings, Network and Internetwork Security Principles and Practice, Prentice Hall, Englewood Cliffs, NJ, 1995.*

[48] *J. Broch, D. A. Maltz, D. B. Johnson, Yih-Chun Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in The Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Dallas, TX, USA, Oct. 1998.*

[49] *P.Pratik, P.Venkataram, "A Method of Secure Route Finding in Mobile Adhoc Networks," In Proc.of IASTED Conference on Wireless Networks and Engineering Technologies, 2004, pp.71-79.*

[50] *A.Boukerche, "Performance Comparison and Analysis of Adhoc Routing Algorithms," In Proc.of IEEEICPCC, 2001, pp.171- 178*

ISSN: 2277-9655
Impact Factor: 1.852

[51]I.D.Aron, S.K.S.Gupta, "On the Scalability of On-Demand Routing Protocols for Mobile Adhoc Networks: An Analytical Study," Journal of Interconnection Networks, vol.2, no.2, 2001, pp.5-29.