International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-6, June 2014

Performance Analysis of AODV and SAODV Using C++

Kamaljit Kaur, Amanpreet Kaur

***Abstract* - Wireless mobile ad-hoc networks are networks does not use any physical connections. These networks are not having with any fixed topology cause to the mobility of the nodes, path loss, multipath propagation, and interference. For this task there are many routing Protocols, have been developed. The purpose of paper is to analyse and check the performance of two mobile ad-hoc routing protocols AODV and SAODV. AODV is a very familiar reactive routing protocol in MANET. Here the reactive gives the meaning that a node send/receive routing information only under condition that it has some data to send/receive and keeps the routing information updated as long as the communication with the node is available. But the lack of security mechanisms, malicious nodes, AODV can allow many attacks to not behaving according to AODV rules. To make available network secure, SAODV is being introduced. SAODV (Secured Ad-Hoc on Demand Vector Routing) is one of the secured mechanisms using digital signature and hash chain function to keep secure AODV packets. Secured AODV improves the AODV message format by introducing the security parameter for security purpose of routing messages. The goal of this master thesis is to analyse and simulate AODV & SAODV routing protocols using C++.**
-

***Index Terms* - AODV, SAODV, Digital Signatures, Hash Chain Function**

I. INTRODUCTION

Mobile Ad-hoc network is a set of such wireless devices that are called wireless nodes that dynamically connect and transfer information. Wireless nodes can be some personal computers (e.g. desktops/laptops) which are having wireless LAN cards, Personal Digital Assistants (PDA), or some other types of wireless or mobile communication devices. In general words, a wireless node can be any computing equipment/device that uses the air as the transmission medium. The wireless node may be physically connected to a person, a vehicle, or an airplane, to make possible a wireless communication among them.

Wireless Ad hoc Networks are becoming popular day by day because the devices communicate with each other via wireless physical medium without leaving pre-existing wired infrastructure behind and in nature each node in an ad hoc network is self-configurable. Moreover, it takes help of "multi-hop" routing technique to communicate with such nodes that are not in communication range. Since the arrival of defence advanced research project agency (DRPA)

numbers of protocols have been developed for mobile ad hoc networks. These existing protocols can be generally categorized into 2 types – Table driven (Proactive) and Demand driven (Reactive). Some illustrations of table driven protocols are DSDV Destination sequence Distance Vector Routing), CGSR (Cluster Head Gateway Switch Routing), and WRP (Wireless Routing Protocol). Two most popular Demands driven routing protocols are DSR (Dynamic Resource Routing) and AODV (Ad hoc On Demand Distance Vector) protocol. These protocols are not having any security mechanism for fortification of an attacker to embrace itself in routing operation. SAODV protocol an extension of AODV routing protocol contains security features. Wireless ad-hoc network have following advantages:

Low cost of deployment: Ad hoc networks can be deployed on a low cost; no expensive arrangements like copper wires or data cables are required.

Fast deployment: Because no. of cables are involved, Ad hoc networks are very appropriate and easy to deploy. Don't take much time to deploy.

Dynamic Configuration: Ad hoc network configuration can be changed with dynamism over time. When equated to configurability of LANs, to change the network topology of a wireless network is very easy.

MANET has various prospective applications. Some usual examples are meeting events, emergency search-rescue operations, conferences, and battlefield communication between moving vehicles and/or soldiers. As the demand of mobile computation is increasing day by day, the MANET is heading very bright future.

II. BRIEF ON AODV & SAODV:

AODV performs Route Discovery with control messages route request (RREQ) and route reply (RREP) the time node requests to send packet to destination. An expanding ring search technique is used by source node to control network wide broadcasts of RREQs. Using RREP the forward path creates intermediate nodes in its route table with a lifetime association. If destination or intermediate node moves or gets some change, a route error (RERR) is sent to the exaggerated source nodes. Whenever source node receives the (RERR), it is possible to reinitiate route discovery if the route is still required. Neighbourhood information is fetched from broadcast Hello packet. A significant feature of AODV is the maintenance regarding utilization of individual routing table entries which are timer-based states in each node. A routing table entry is not in use from recent time will be "expired". A set of prototype nodes is upheld for each routing table entry, signifying the set of neighbouring nodes that custom that

Manuscript received June 20, 2014.
Kamaljit Kaur, Department of Computer science and engineering, Ramgariah Institute of Engg. & Technology, Phagwara,Punjab(INDIA)
Amanpreet Kaur, Department of Computer science and engineering, Ramgariah Institute of Engg. & Technology, Phagwara,Punjab(INDIA)

entry to route data packets. When the next hop link breaks these set of prototype nodes are reported with RERR packets. In turn, each prototype node, forwards the RERR to its own set of prototypes, which effects with erasing all routes using the broken link. In contrast to DSR, RERR packets in AODV are projected to report to all sources using a link if a failure occurs. Route error transmission in AODV can be imagined abstractly as a tree whose root is the node which is at the point of failure and all sources that were using the failed link as the leaves.

SAODV is an addition in AODV routing protocol that can be projected to protect the route discovery mechanism having security features like integrity, authentication and non-repudiation. As Manet protocols are being considered having no security in mind.

SAODV take responsibility to keep each ad hoc node a signature key pair from a suitable asymmetric cryptosystem. In addition, each node is accomplished a securely verification of the association between the address of other node and the public key of that node. For this purpose the SAODV needs a key management scheme. Following two mechanisms are used to secure the AODV messages:

1. Digital signatures to authenticate the non-mutable fields of the messages, and
2. Hash chains to secure the mutable hop count field of the message.

In the non-mutable fields authentication can be done in a point-to-point mode, but these techniques cannot be implemented on the mutable information/fields. Because of a huge amount of mutable information a different mode is used to protect route error messages. According to the other authors, it does not matter which of the node is started the route error and which of that nodes are just keep it forwarding. In fact the important point is that a neighbour node informs other nodes that it is unable to transmit messages to specific destinations anymore. Therefore, every node either generating or forwarding a route error message rely on digital signatures to sign the whole RERR message and any neighbour that receives RERR message verifies the signature first.

A. Performance Metrics:

Some important performance metrics can be weighed as:-

Number of nodes: Performance testing generally needs to be accessible in the number of nodes and network transmitting packets.

Packet delivery rate: This equivalents to “Total packets(p) successfully received”/”Total packets(p) send”

Average delay: This can be evaluated as “Sum (for each p equal to packet number), (packet p received time- packet p send time)/ Total packets transmitted”.

Average routing overhead: This equals to “Total routing control packets (p)/Simulation time (t)”.

Essential parameters that should be varied:

Network size--evaluated in the number of nodes.

Network density--average gradation of a node, i.e. the average number of neighbours of a node.

Mobility-- the most applicable model for simulating node mobility in a MANETS.

Transmission Range: circular degree of the networking volume of individual node.

B. Simulation:

The start the performing simulations in C++ are to form a C++ simulation development script file that identifies the components to be used and the events that should occur. An example that a scenario could be e.g. set up a network topology residing two nodes, connect both having a 10 Mbps duplex link, set up FTP traffic over TCP, then start and stop this traffic at definite points in time.

Usually, a simulation scenario contains main these three components:

a) A network topology
b) Connections, traffic and agents (protocols)
c) Events and failures

III. SIMULATION EXECUTION AND ANALYSIS:

A simulation development script is accomplished which means a simulation is performed, by delivering the file name to the C++ editor. For simulation C++ interpreter, interprets the simulation development script line by line. Any error message or messages generated by the script will be printed to the error console. The simulator exits, the time simulation has finished and the command prompt returns to the main script again. For performing simulations no graphical user interface is supplied with C++ editor.

After a success full performance of this simulation, the produced trace files by the simulation development script can be analysed. According to the objectives of this simulation, this analysis can be done with an analysis tool either Trace graph or with simpler, hand-made scripts or programs.

OTcl/C++ environment:

For a flexible and efficient environment, ns-2 practices two programming languages for its setup; C++ and OTcl. C++ is usually castoff features like event handling and per-packet processing; OTcl would become too slow for these tasks. OTcl is generally castoff for simpler routing protocols, general ns-2 code and simulation scenario scripts.

Problems while writing OTcl scripts to run simple wireless simulations:

Performance testing typically needs to be accessible in the no. of nodes and network transmitting packets. Assume for single network, there are hundreds of nodes, we want to set all of these nodes, positions and their movement, it will be a huge amount of workload, likewise, suppose we want to setup all the probable sources and destinations and even connections, this is also a huge workload, additionally, even if we could set them all, we cannot be assure of our input will be randomly selected, which is essential for a fair comparison.

A. Performance comparison on AODV & SAODV:

The following will be a comparison between AODV and SAODV, the test results will be the main focus which were got from the performance evaluation code.

A. Simulated Scenario and Environment settings:

The scenario and environment situations are stable. It has been done on purpose to see the reasonable results between the routing protocols. These routing protocols AODV, Secure AODV are objectively compared. Here is some of the details on the setup:-

- Number of nodes = 50 nodes
- Maximum connections = 40 traffic sources
- Mobility Model = Random Waypoint
- Mobility Speed = 40 m/s
- Rate = 8kbps (2 packets per load)
- Topology Size = 500m x 500m
- Time = 100 seconds (results are collected every 10s of pause time)

B. Performance Metrics & Evaluation:

The simulation result sake, 4 performance metrics have been used as shown below:-

Packet Delivery fraction (PDF):

The ratio of the data packets supplied to the destinations, generated by the CBR sources. Following Figure1 shows the experimental results of packets delivery Fraction.

Calculated as,

PDF (%) = (Received Packets/sent Packets)*100

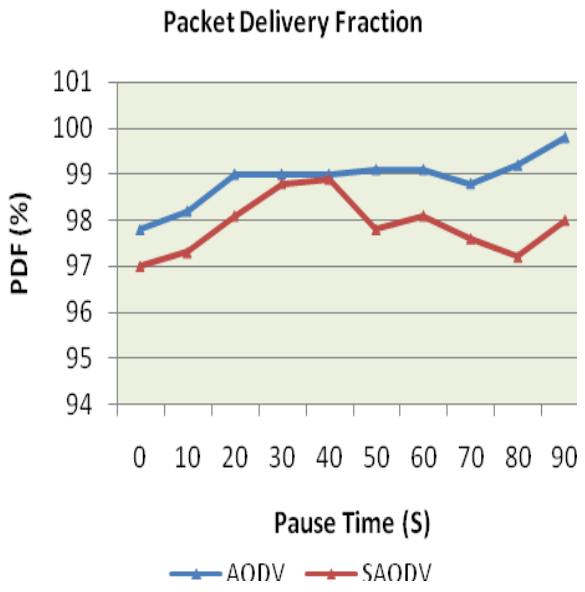

Figure 1 : PDF Vs Pause Time

Average End-to-End Delay:

This embraces all probable delays triggered by buffering throughout route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times. To get the results for each packet sent, calculate the send time of packet and receive time of packet, then average it.

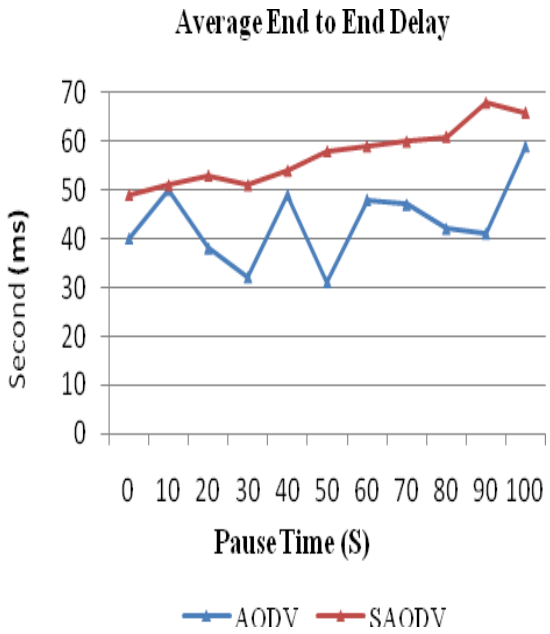

Figure 2:Average End to End Delay Vs Pause Time

Number of Dropped Packets:

To calculate the number of dropped packet is needed to subtract the number of received packets from packets generated by the source/sender.

Number of dropped packet = Sent Packet -Received Packet.

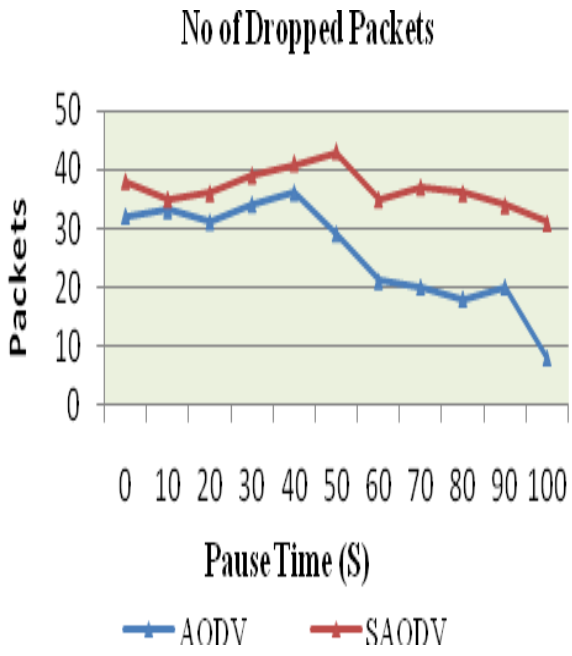

Figure 3: No of dropped Packets Vs Pause Time

Routing Overhead:

Getting Normalized routing load with the number of routing packets transmitted per data packet delivered at the destination. For the calculation,

Normalized Routing Load = routing packets sent / packet received.

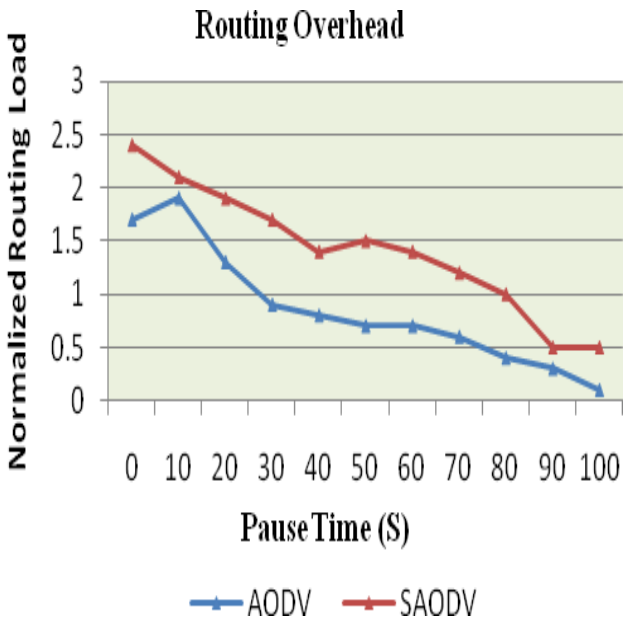

Figure 4: Routing Overhead Vs Pause Time

IV. Conclusion and Future Work

In this research paper some estimations & judgments of AODV & SAODV routing protocols are done. To weigh the performance of these two routing protocols the simulations are centred on the 4 different performance metrics. To provide authentication some security techniques corresponding to Digital signatures and Hash chains are being used.

Centred on the performance metric, SAODV performs similar to AODV having lower number of nodes and with less mobility but getting higher number of nodes and having increased mobility, it tends to *break down.* Consequently to provide the security in any protocol concerned protocol should sacrifice the performance of data transmission.

In future work on SAODV, SAODV can be improved by practicing some other operations to overcome break down in performance even with higher number of nodes and increased mobility.

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.