International Journal of Engineering & Scientific Research
Vol.4 Issue 10, October 2016,
ISSN: 2347-6532 Impact Factor: 5.900
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

MANET ROUTING PROTOCOL FOR EFFICIENTLY TRANSFERRING THE DATA

Ravinder Choudhary*

Raman Manocha*

Er. Deepti Garg(Research Supervisor)*

ABSTRACT:

Wireless technology based on the IEEE 802.11 standard is used to support multiple types of communication services (data, voice, and image) with different QoS requirements. Node mobility creates a continuously changing communication topology in which paths break and new one form dynamically. The routing table of each router in an ad-hoc network must be kept up-to-date. MANET uses Distance Vector or Link State algorithms which insure that the route to every host is always known. However, this approach must take into account the ad-hoc networks specific characteristics: dynamic topologies, limited bandwidth, energy constraints, and limited physical security. Two main routing protocols categories are studied in this paper: proactive protocols (e.g. Optimized Link State Routing - OLSR) and reactive protocols (e.g. Ad hoc On Demand Distance Vector - AODV, Dynamic Source Routing - DSR). The present paper focuses on study and performance evaluation of these categories using NS2 simulations. We have considered qualitative and quantitative criteria. The first one concerns distributed operation, loop-freedom, security, sleep period operation. The second are used to assess performance of different routing protocols presented in this paper. We can list end-to-end data delay, packet delivery ratio, routing load. Comparative study will be presented with number of networking context consideration and the results show the appropriate routing protocol for two kinds of communication services (data and voice).

* Dept of Electronics and Communication Engineering, YIET, Gadholi,Yamuna Nagar Haryana

INTRODUCTION:

Wireless communication technology is increasing daily; with such growth sooner or later it would not be practical or simply physically possible to have a fixed architecture for this kind of network[1]. Ad hoc wireless network must be capable to self -organize and self configure due to the fact that the mobile structure is changing all the time. Routing protocols are divided into two categories: Proactive and Reactive-Proactive routing protocols are table-driven protocols and they always maintain current up-to-date routing information by sending control messages periodically between the hosts which update their routing tables. The proactive routing protocols use link-state routing algorithms which frequently flood the link information about its neighbors[2]. Reactive or on-demand routing protocols create routes when they are needed by the source host and these routes are maintained while they are needed. Such protocols use distance-vector routing algorithms. Our goal is to carry out a systematic performance study of two routing protocols for ad hoc networks namely Ad hoc On Demand Distance Vector (AODV)[3] routing protocol and Optimized Link State Routing (OLSR) protocol. The rest of the paper is organized as follows:

II. AD HOC ON DEMAND DISTANCE VECTOR (AODV)

A. Introduction to AODV

The information in this section concerning AODV protocol is taken from the RFC. AODV is a reactive protocol, i.e., so the routes are created and maintained only when they are needed .The routing table stores the information about the next hop to the destination and a sequence number which is received from the destination and indicating the freshness of the received information. Also the information about the active neighbors' is received throughout the discovery of the destination host[4]. When the corresponding route breaks, then the neighbors' can be notified. The route discovery is used by broadcasting the RREQ message to the neighbors' with the requested destination sequence number, which prevents the old information to be replied to the request and also prevents looping problem, which is essential to the traditional distance vector protocols .The route request does not add any new information about the passed hosts only it increases its hop metric. Each passed host makes update in their own routing table about the requested host. This information helps the destination reply to be easily routed back to the requested host [5].The route reply use RREP message that can be only generated by the

destination host or the hosts who have the information that the destination host is alive and the connection is fresh.

B. Sequence numbers:

The sequence numbers are the key idea for removing the old and invaluable information from the network [6] . The sequence number act as timestamps and prevent this distance vector protocol from the loop problem. The destination sequence numbers for each possible destination host are stored in the routing [7] .

***C. Advantages*:**

Because the AODV protocol is a flat routing protocol it does not need any central administrative system to handle the routing process. In addition, AODV tries to keep the overhead of the messages small [8] . If host has the route information in the Routing Table about active routes in the network, then the overhead of the routing process will be minimal. The AODV has great advantage in overhead over simple protocols which need to keep the entire route from the source host to the destination host in their messages. The RREQ and RREP messages, which are responsible for the route discovery, do not increase significantly the overhead from these control messages [9] . The AODV protocol is a loop free and avoids the counting to infinity problem, which were typical to the classical distance vector routing protocols, by the usage of the sequence numbers [10] .

III. RELATED WORK

In four different routing protocols AODV, TORA, DSDV and DSR are compared. DSR generates less routing load than AODV. AODV suffers from end to end delay while TORA has very high routing overhead. The better performance of DSR is because it exploits caching aggressively and maintains multiple routes to the destinations. Performance comparison of AODV and DSR routing protocols in a constrained situation is done. AODV outperforms DSR in normal situation but in the constrained situation DSR outperforms AODV, where the degradation is as severe as 30% in AODV whereas DSR degrades marginally as 10%. A comparison of Link State, AODV and DSR protocols for two different traffic classes, in a selected environment is done. AODV and DSR perform well when the network load is moderate.

Perkins et al. show the performance of two on demand routing protocols namely DSR and AODV. It is observed that for application oriented metrics such as delay, throughput DSR outperforms. AODV when the numbers of nodes are smaller. AODV outperforms DSR when the number of nodes is very large.

IV. SIMULATION ENVIRONMENT

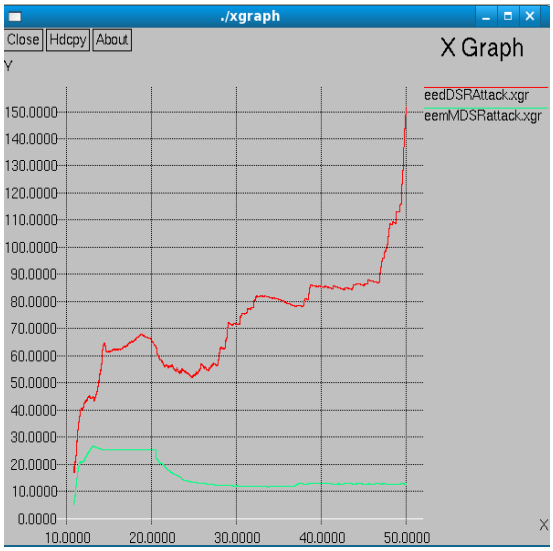
A. Simulation Setup

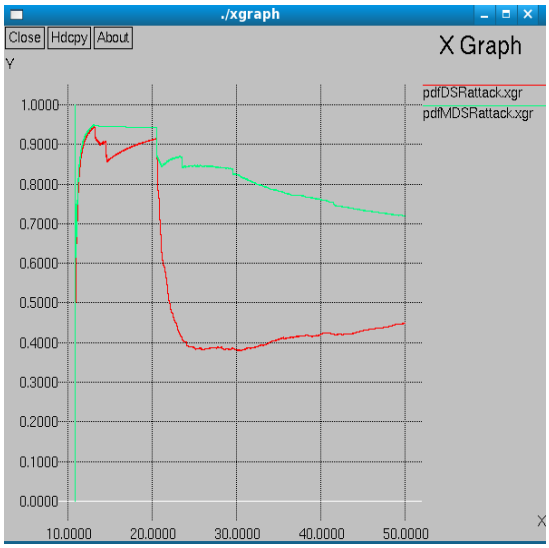
The MANET network simulations are implemented using NS-2 simulator. Nodes in the simulation move according to a model that we call Random Way point Mobility model. Each node is then assigned a particular trajectory .The number of nodes which we take in this is of about 30. The simulation period for each scenario is 100 seconds and the simulated mobility network area is 500 m x 500 m. In each simulation scenario, the nodes are initially located at the center of the simulation region. The nodes start moving after the first 20seconds of simulated time. The MAC layer protocol IEEE 802.11 is used in simulations with the data rate of 512 M bps in UDP and of 1024 M bps in TCP. The application used to generate is Constant Bit Rate (CBR) traffic and Internet Protocol (IP) is used as Network layer protocol. The performance evaluation, as well as the design and development of routing protocols for Manet's, requires additional parameters which is addressed in RFC developed by Internet Engineering Task Force (IETF).

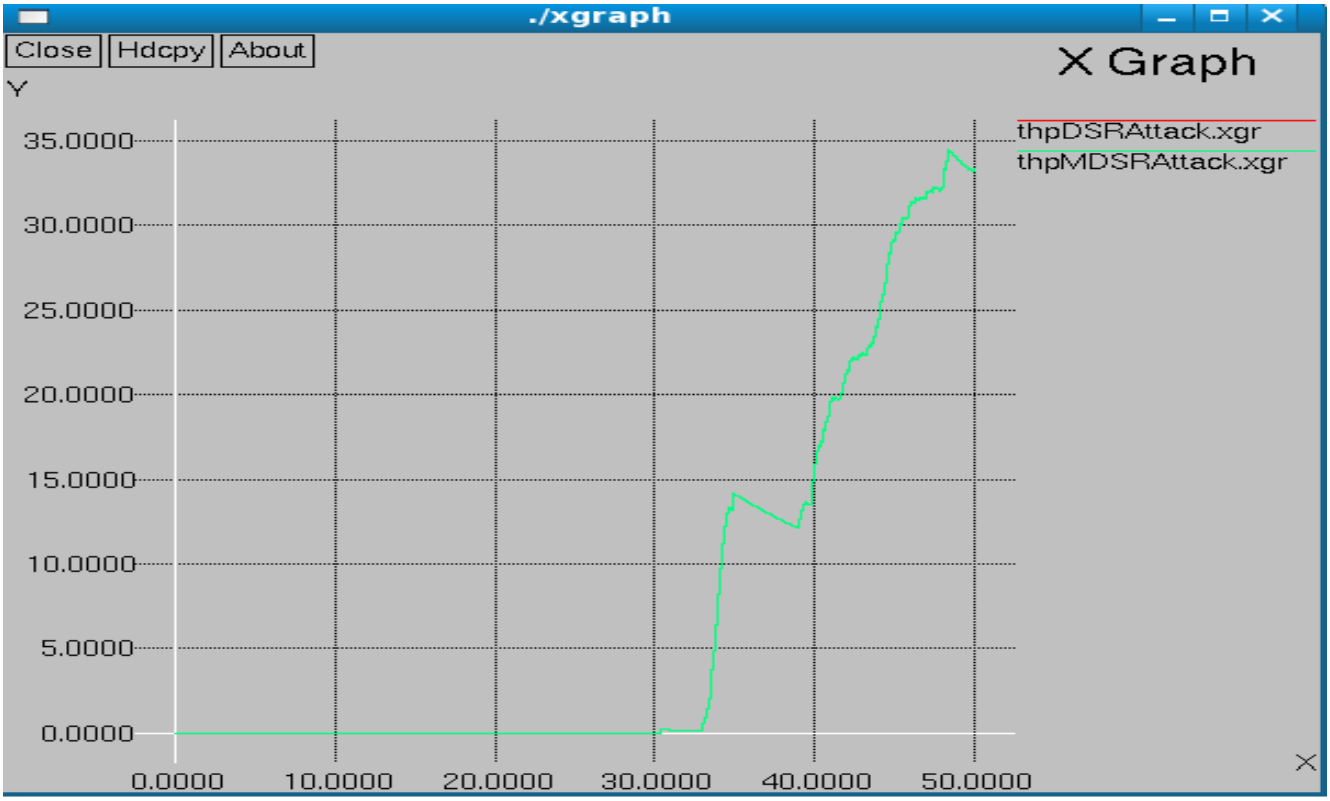
B. Mobility Metrics:

We have selected the transmission of packets in UDP transmission and in TCP, Packet Delivery Ratio and Routing Overhead as a metrics during the simulation in order to evaluate the performance of the different protocols:

- *Packet Delivery Ratio*: This is the number of packets sent from the source to the number of received at the destination.
- *Routing Overhead:* This is the ratio of the number of protocol control packets transmitted to the number of data packets received.
- *Packet Lost***:** It is the measure of the number of packets dropped by the routers due to various reasons.


./xgraph
Close
Hdcpy
About
X Graph
Y
eedDSRAttack.xgr
eemMDSRattack.xgr
150.0000
140.0000
130.0000
120.0000
110.0000
100.0000
90.0000
80.0000
70.0000
60.0000
50.0000
40.0000
30.0000
20.0000
10.0000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
X


./xgraph
Close
Hdcpy
About
X Graph
Y
pdfDSRattack.xgr
pdfMDSRattack.xgr
1.0000
0.9000
0.8000
0.7000
0.6000
0.5000
0.4000
0.3000
0.2000
0.1000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
X


./xgraph
Close
Hdcpy
About
X Graph
Y
thpDSRAttack.xgr
thpMDSRAttack.xgr
35.0000
30.0000
25.0000
20.0000
15.0000
10.0000
5.0000
0.0000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
X

Conclusion and Future work :

In Mobile Ad-hoc Networks, nodes use the air to communicate, so a lot of nodes might hear what a node transmits and there are messages that are lost due to collisions. In a network where everybody is anonymous, identity and trust need to be redefined. In addition, if the security protocols that are used in these kind of networks are based in mechanisms that require asymmetric cryptography, the task of having secure routing protocols for such kind of networks will not be completed without an specific key management scheme. In future we will implement asymmetric cryptography with Manet so that it can make more secure.

References :

[1] Kamarudin Shafinah and Mohammad Mohd Ikram, "File Security based on Pretty Good Rrivacy (PGP) Concept",www.ccsenet.org/cis, Computer and Information Science, Volume 04, July 2011.

[2] Nilesh P Bobade and Nitiket N Mhala, " Performance Evaluation of Ad hoc On Demand Distance Vector in Manet's with varying Network size using NS-2 Simulation", International Journal on Computer Science and Engineering (IJCSE) Volume 02 , August, 2010.

[3] Manali J Dubal, Mahesh T R and Pinaki A Ghosh, "Design of New Security Algorithm, Using Hybrid Cryptography Architecture", IEEE 2011.

[4] Hou Liping and Shi Lei, "Research on Trust Model of PKI", 4th International Conference on Intelligent Computation Technology and Automation, IEEE 2011.

[5] Jiang Haowei and Tan Yubo, "Research in P2P-PKI Trust Model", IEEE 2010

[6] Dongxia Li and Xinana Fu, "A Revised AODV Routing Protocol based on the Relative Mobility of Nodes".

[7] JuCheng Yang, "Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System", International Conference on Management of e-Commerce and e-Government, IEEE 2010.

[8] Byoungcheon Lee, "Unified Public Key Infrastructure Supporting Both Certificate Based and ID-Based Cryptography", International Conference on Availability, Reliability and Security, IEEE 2010.

[9] WU Xing-hui and MING Xiu-jun, " Research of the Database Encryption Technique Based on Hybrid Cryptography", International Symposium on Computational Intelligence Design, IEEE 2010.

[10] Antonio Vincenzo Taddeo, Alberto Ferrante, "A Security Service Protocol for MANETs", IEEE 2009.