ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Performance Analysis of Secure Routing Protocols in MANET

K. Thamizhmaran[1], R. Santosh Kumar Mahto[2], V. Sanjesh Kumar Tripathi[3]

Asst Professor / ECE, Dept of Electrical Engg, Annamalai University, Annamalai nagar, Tamilnadu, India [1]

ECE (Final Yr) / Dept of Electrical Engg, Annamalai University, Annamalai nagar, Tamilnadu, India[2, 3]

ABSTRACT: Mobile Ad-Hoc Networks (MANET) is the infrastructure less network that can be constructed without any base station, re-transmission switches and routers. Mobile adhoc network nodes share the data and service. In MANET, a node can get compromised during the route discovery process. Attackers from inside or outside can easily exploit the network. Several secure routing protocols are proposed for MANETs. Security in MANETs is critical when deployed in real-world scenarios, such as battlefield, and event coverage, etc. In this paper we evaluate the performance comparison of three s routing protocols such as SEAD, AODV and DSR. Across the models with respect to considered metrics for comparison, SEAD outperformed others followed by AODV and DSR.

Keywords: MANET, Routing protocols, Ad-hoc networks, secure routing, evaluation.

I. INTRODUCTION

MANET stands for mobile ad hoc networks. It is a decentralized autonomous wireless system which consists of free nodes. MANET sometimes called mobile mesh networks. It is a self configurable wireless network. MANET is a spontaneous network. It is when dealing with wireless devices in which some of the devices are part of the network only for the duration of a communication session. The MANET Working Group (WG) within the Internet Engineering Task Force (IETF) works specifically on developing IP routing protocols topologies. To improve mobile routing and interface definition standards for use within the internet protocol suite. After huge research work on MANET, still it does not have a complete from of internet based standards.

Efficient Broadcasting in Mobile ad hoc networks using groups of Dynamic Routing Protocols. They are,

- Proactive MANET Protocol (PMP).
- Reactive MANET Protocol (RMP).
- Hybrid MANET Protocol (HMP).

Whereas the third one is derived from both of these and called as hybrid MANET Protocol (HMP).

The **Proactive MANET** Protocol is generally called table driven protocol and it detects the network layout periodically. It tries to maintain the routing table at every node which is used to detect a most feasible route to the destination from the source with less delay. Proactive MANET Protocols provide good reliability and low latency for deciding a route.

The **Reactive MANET** Protocol is called on-demand routing protocol and finds the route when a source node requests to communicate with the other. On-demand approach is suitable for the nodes with high mobility and nodes that transmit data rarely.

The **Hybrid MANET** Protocol integrates the merits of Proactive and Reactive Protocol. Zone Routing Protocol (ZRP) and Two Zone Routing Protocols (TZRP) are the examples of Hybrid of MANET Protocol.

Benefits of routing Algorithms: dependent on processing time of algorithms, dependent on amount of information required from other nodes, implementation specific, both coverage under static topology and costs, coverage to same solution, if link cost change, algorithm will attempt

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

to catch up and if cost depend on traffic, which depends on routes chosen, then feedback may result in instability.

II. ROUTING PROTOCOLS

SEAD: (*Secure and Efficient Ad hoc Distance vector routing protocol)* is based upon the *DSDV-SQ* routing protocol, a modified version of *DSDV*. It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. For authenticating a particular sequence number and metric, the node generates a random initial value x Є {0,1}ρ where ρ is the length in bits of the output of the hash function, and computes the list of values *h0,h1,h2,h3,…,hn*, where *h0=x* , and *hi* = H(*hi-1*) for 0< $i \leq n$, for some *n*. As an example, given an authenticated *hi* value, a node can authenticate *hi-3* by computing H(H(H(*hi-3*))) and verifying that the resulting value equals *hi*.

Each node uses one authentic element of the hash chain in each routing update it sends about itself. This enables the authentication for the lower bound of the metric in other routing updates for that node. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained, and compares it with the hash value in the routing update message. The update message is authentic if both values match. The source must be authenticated using some kind of broadcast authentication mechanism. Apart from the hash functions used, SEAD does not use average settling time for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes. SEAD prevents several types of DOS attacks. It also prevents formation of routing loops. However, it does not prevent the *wormhole attack*, which results in tunneling of packets via a virtual cut in the network.

DSR: (*Dynamic Source Routing protocol)* is a reactive protocol which uses source routing, i.e., each routing packet has a complete list of nodes through which the packet must pass. Since every packet has the complete route, the intermediate nodes need not maintain up-to-date routing information. The protocol itself consists of two phases – route discovery and route maintenance. In the *route discovery* phase, a node S wanting to send a packet to another node D broadcasts a route request packet (RREQ) to neighboring nodes. D unicast a reply packet (RREP) back to S. During the *route maintenance* phase, a node S detects whether its link to a destination node D is no longer valid. If there is a broken link, S is notified via a Route Error packet (RERR).

AODV: (Ad-Hoc On-Demand Distance Vector) The AODV routing protocol is a pure on-demand routing protocol. The primary objectives of AODV are:

a) To perform path discovery process when necessary. AODV uses broadcast route discovery mechanism.
b) To distinguish between local connectivity management (neighbor detection) and general topology maintenance.
c) To broadcast information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information.

One of the distinguished features of AODV is its use of a destination sequence number of each route entry. The AODV algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. Several attacks can be launched against AODV routing protocol such as message tampering attack, message dropping attack and message replay attack. The path discovery process is initiated whenever a source node needs to communicate with another node and when the node does not contain the routing information in the routing table or the route entry has been expired. Each node maintains two separate counters a node sequence number and request broadcast ID. The source node then broadcasts a route request (RREQ) packet to its neighbors. Each RREQ is uniquely identified by <IP address, broadcast ID>. The value of broadcast ID is incremented every time a node issues a RREQ request. All nodes that received this RREQ packet will update their information for the source node. AODV uses 3 types of control messages to run the algorithm, RREQ, RREP and RERR messages. The sequence number and request broadcast ID uniquely identifies a RREQ. Each neighbor either satisfies the RREQ by sending a RREP back to the source, or re-broadcasts the RREQ to its own neighbors after increasing the HOP Count. A node may receive multiple copies of the same route broadcast packet from various neighbors. When an intermediate node receives a RREQ, if it has already received a RREQ with the same broadcast ID and source address, it drops the redundant RREQ and does not rebroadcast it. If the node cannot satisfy the RREQ, it keeps track of necessary routing information in order to implement the reverse path setup,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

as well as the forward path setup that will accompany the transmission of the eventual RREP. When RREQ arrives at a node that possesses the current to the destination, it determines whether it has a valid route entry for the desired destination by finding the freshness of the route by comparing sequence numbers. After ensuring that route is an updated route and valid one, the node unicast RREP message to the source using the reverse path that has been by the RREQ message. In each routing table entry, the address of active neighbors through which packets for the given destination are received is also maintained. A neighbor is considered active if it originates or relays one packet for that destination within the most recent active timeout period. This information is maintained so that all active source nodes can be notified when a link along a path to the destination breaks. A route entry is considered active if it is in use by any active neighbors. The path from a source to a destination, which is followed by packets along active route entries, is called an active path. A mobile node maintains a route table entry for each destination.

III. PERFORMANCE COMPARISON

The following are the metrics which we have used for the performance analysis.

***Packet Delivery Fraction (PDF)*:** This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

PDF = no of Received Packets / no of sent packets.

PDF estimates how successful the protocol is in delivering packets to the application layer. A high value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

***Normalized Routing Load (NRL)*:** This is calculated as the ratio of the number of routing packets transmitted to the number of data packets actually received.

NRL = no of routing packets sent / no of data packet received

NRL estimates how efficient a routing protocol is since the number of routing packets sent per data packet gives an idea of how well the protocol maintains the routing information updated. Higher NRL indicates higher routing overhead, and thus lower efficiency of the protocol.

***Average end to end delay (AED)*:** This is defined as the average delay in transmission of a packet between two nodes and is calculated as follows:

$AED = \sum_{i=0\ldots n}$ (*time Packet Receive* $_i$ *time Packet* Received$_i$) / total no of Packet Received

A higher value of AED means the network is congested and hence the routing protocol does not perform well. The upper bound of AED is application-dependent. For example multimedia traffic such as audio and video cannot tolerate very high values of end-to-end delay when compared to other types of traffic such as FTP.

IV. CONCLUSIONS

Performance comparisons of AODV, DSR and SEAD routing protocols in MANETs have been done in this research paper, based on the performance metrics rather than security metrics such as PDF, NRL and AED. The SEAD is high secure compare the other two. The routing protocols AODV, DSR and SEAD. Although prior studies have been conducted to evaluate these routing protocols, few of them have considered these protocols in real-life scenarios which may impose seemingly contradicting constraints including security, reliability, performance, and power conservation. In MANET security would be to evaluate the security protocols with regard to protocol performance which would help in the adoption of MANET security protocols that meet up routing demands as well as security requirements.

REFERENCES

[1] Charles E. Perkins, "Ad Hoc Networking." Addison-Wesley, 2001.

[2] Geetha Jayakumar, and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols – A Review," in Journal of Computer Science 3 (8): pp 574 582, 2007.

[3] J. Macker and M.S. Corson, "Mobile Ad Hoc Networking and the IETF," in ACM Mobile Computing and Communication Review 2(2), pp. 9-12, April 1998.

[4] Yogesh Chaba, Yudhvir Singh and Manish Joon, "Simulation based Performance Analysis of On-Demand Routing Protocols in MANETs," in 2010 Second International Conference on Computer Modelling and Simulation, 2010.

[5] S. R. Das, C. E. Perkins, and E. M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," in INFOCOM, March 2000.
[6] C. E. Perkins and E. M. Royer," Ad Hoc On Demand Distance Vector (AODV) Routing," Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999.
[7] D. B. Johnson and D. A. Maltz, Yih-Chun Hu," Dynamic Source Routing in Ad-Hoc Wireless Networks," IETF Internet Draft, draft-ietf-manet-dsr-09.txt, April 15, 2003.
[8] Elizabeth .M. Royer and C.K Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" in IEEE personal communications, 1999.
[9] Hongmei Deng, Wei Li, Dharma P. Agarwal,"Routing security in wireless Ad-Hoc networks", IEEE Communications Magazine, October 2002.
[10] Lidong Zhou, Zygmunt J.Haas,"Securing Ad-Hoc networks", IEEE Network, 1999.
[11] Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer,"A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols, 2002, pp. 1-10.
[12] C.E. Perkins, E. M. Belding-Royer, S. R. Das. "Ad-Hoc On-Demand Distance Vector Routing", IETF RFC 3561, July 2003.
[13] Junaid Arshad, Mohammad Ajmal Azad,"Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-Hoc Networks", 2006 IEEE.
[14] M. F. Juwad, H. S. Al-Raweshidy,"Experimental Performance Comparisons between SAODV & AODV", IEEE Second Asia International Conference on Modelling & Simulation, 2008.
[15] Yih-Chun Hu, David B. Johnson, Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp 3-13, 6/2002.
[16] P. Papadimitratos and Z. Haas. "Secure routing for mobile ad hoc networks" (SRP) SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27--31, 2002.

Biography

Prof. K. Thamizhmaran has received his B.E and M.E degree from Annamalai University, Chidambaram, Tamilnadu, India in the year of 2008 and 2012. He is currently working as an Assistant Professor in ECE / Department of Electrical Engg, FEAT, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu., India. His interested area includes Mobile Communications, Digital Signal Processing, Signals And System. He has published three papers at International journal. He is a member of IAENG, IACSIT.

R. Santosh Kumar Mahto has Doing Final Year ECE, Dept of Electrical Engineering in Annamalai University, Chidambaram, Tamilnadu, India. His interested area includes Mobile Communication, Digital Signal Processing.

V. Sanjesh Kumar Tripathi has Doing Final Year ECE, Dept of Electrical Engineering in Annamalai University, Chidambaram, Tamilnadu, India. His interested area includes Mobile Communication, Telecommunications.