IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Survey on TS-AOMDV Routing Protocol in MANET

Poornima S[1], D Khasim Vali[2]

PG Scholar, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[1]

Associate Professor, Department of CSE, Vidya Vardhaka College of Engineering, Mysuru, India[2]

Abstract: MANET (A Mobile Ad-hoc Network) is a network where nodes are not connected that is it is a wireless network where nodes are configured dynamically. Wireless network means there will be issues with network security that is an intruder get into the network and does flooding attack, black hole attack and a gray hole attack. To provide network security a better approach called TS-AOMDV-Trust-based Secured Ad-hoc On-demand Multipath Distance Vector is used than Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing protocol. TS-AOMDV uses Intrusion detection system and a trust-based routing factor so this provides a better security and a routing performance.

Keywords: Mobile Ad-hoc Network, TS-AOMDV, AOMDV, Intrusion detection system.

I. INTRODUCTION

Now a days, we are using a wireless communication over a wired communication as there are so many advantage over a wired connections there are some disadvantages too, in those security is the main in which we have to concentrate and to provide a better service. MANET is the new wireless communication technology used. MANET operates as a self centralized network, it dynamically finds a route between the source and destination that is, it is a multi-hop distributed communication network comprising of a collection of mobile nodes [1][2].
Due to the random mobility of nodes the network changes dynamically because there is no access point or a pre-defined network. The routing protocol should be designed to find a suitable path from source to destination. Neighbors are the next node from the node which to transmit the data within a transmission range [5]. In TS-AOMDV we will get a multiple path the first optimal path is chosen to forward the packet based on trust factors the nodes forward the packet [2]. The routing should takes place in a dynamic network conditions, varying mobility of the nodes, with less energy, with its own architecture, and with less resources. The data is forwarded either with a single or a multi-hop communication due to limited transmission range [3][4]. As there is no proper infrastructure it's a challenging task to provide security in MANET. The factors like availability, reliability, resiliency and self-healing are to be included in security. To utilize the potential of MANET the routing protocol has to overcome above security pitfalls.

II. HOW TS-AOMDV ARCHITECTURE WORKS?

The architecture aims at identifying and isolating the attacks such as flooding attack, black hole attack and gray hole attack[9]. Flooding attack is an attack where the intruder enters into the transmission range and fills the server or host memory with unwanted data for example simply asking to forward a packet to some destination IP where that destination IP address is not existing or simply sending many packets to the destination IP.
Black hole attack also called as packet drop attack is an attack where the node discards the packet instead of sending the packet to the destination IP. Gray hole attack is an attack where the node selectively drops and forwards the packet after advertising itself as having a shortest path from source to destination IP [8].
The TS-AOMDV architecture works with the help of Intrusion Detection System and a trust based routing [11]. Intrusion Detection System acts as a sniffer and monitors every neighbor node and runs on each node that is to note the routing activities of the node in the network layer [11]. An ID monitors every node and identifies the behavior of every node that is to check whether that node is an attacker by looking at the packet generation rate and by looking at the sent and received packets of nodes. Trust based routing means we maintain a source trust and a router trust that is it maintains a certain threshold value for the source node and for the router if the source node is less than the threshold value then that node is marked as malicious node and that node will be blocked hence that node cannot send the packets to other nodes. If the router trust is less than the threshold value then there will be a chance of black hole and gray hole attack that is the number of sent packets will be not equal to the received packets[2][6][7]

The architecture can be divided into five modules:

1. One Hop Neighbor Identification Module:

- In this module each node identifies its 1 hop neighbors using HELLO Exchange (UDP)

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

- Each identified 1 hop neighbors are set with 2 variables/parameters that is "Source-Trust" & "Router-Trust" and initialized to its default values that is "1"

2. Flooding Attack Detection Module

- IDS service is deployed at each node to monitor the every neighboring node.
- In case of RREQ packet reception, IDS extracts Ip Address of the packet originating node and increments the RREQ count of the corresponding source
- Source-Trust Parameter is calculated by, Source-Trust = $(\text{RREQ Count})^{-1}$
- If the Source-Trust Parameter value is lesser than the threshold, then the RREQ packet from the corresponding source is dropped (instead of rebroadcasting) to block the flooding activity of the attacker

3. Route Discovery Module

- Uses DSR (AODV) Routing Protocol to find an optimal path between any source and destination nodes
- Avoid accepting RREP packets from those nodes whose Source-Trust & Router-Trust parameter are abnormal. Hence selects only optimal & secure path between any give source and destination node
- Compute Backup paths at each node for respective destination (Computed during RREPs received at each node)

4. Data Transmission Module

- Uses Multihop Data Transmission Protocol[10]
- Uses End 2 End Acknowledgement Scheme
- Uses time-out timer named ACK_REC_TOT (Acknowledgment Reception Time-Out-Timer) for Acknowledgement Reception

5. Black & Gray Hole Attack Detection Module

- IDS service is deployed at each node to monitor the neighboring node that is selected for data transmission
- IDS service computes Router-Trust Parameter of selected neighboring node using, Router-Trust = Received Packet Count / Forwarded Packet Count
- Prior to forwarding the data packet to the router, every node checks for the trust value of the router (indicates the reliability of the data delivery through it)
- If the Router-Trust Parameter value is lesser than the threshold, the current data transmission through the malicious router is blocked. Subsequently, the trusted router (Backup Path) from the routing table is accessed to resume data transmission

III. CONCLUSION

From this survey TS-AOMDV Trust-based Secured Ad hoc On-demand Multipath Distance Vector routing protocol provides better security in MANET. The proposed architecture is included with two main things that is Intrusion Detection System and Trust based factors so by using these we can overcome the attacks like flooding, black hole and gray hole.

REFERENCES

[1] Erciyes, K. "Distributed Graph Algorithms for Computer Networks", Computer Communications and Networkss , London: Springer, pp. 259-275, 2013.
[2] Abrar Omar Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET" IEEE 30th International Conference on Advanced Information Networking and Applications pp, 212-219,2016
[3] S. Abdel Hamid, H. Hassanein and G. Takahara, "Routing for Wireless Multi-Hop Networks: Unifying Features", SpringerBriefs in Computer Science, pp. 11-23, 2013.
[4] Hamid, S. A., Hassanein, H., & Takahara, G., "Routing for Wireless Multi Hop Networks–Unifying and Distinguishing Features", School of Comp.—Queen's University, Canada, report 583, 2011.
[5] Habib, S., Saleem, S., & Saqib, K. M., "Review on MANET routing protocols and challenges", IEEE Student Conference on Research and Development SCOReD , pp. 529-533 , 2013.
[6] A. Ahmed, K. Abu Bakar, M. Channa, K. Haseeb and A. Khan, "A survey on trust based detection and isolation of malicious nodes in adhoc and sensor networks", Frontiers of Computer Science, vol. 9, no. 2, pp. 280-296, 2015.
[7] I. Abdel-Halim, H. Fahmy and A. Bahaa-Eldin, "Agent-based trusted on-demand routing protocol for mobile ad-hoc networks", Wireless Netw, vol. 21, no. 2, pp. 467-483, 2015.
[8] Shanmuganathan, V., and T. Anand. "A Survey on Gray Hole Attack in MANET." IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), pp. 2250-3501, 2012.
[9] Tayal, S., & Gupta, V., "A Survey of Attacks on Manet Routing Protocols", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, No.6, pp. 2280-2285, 2013.
[10] Vaidya, Binod, et al. "Secure multipath routing scheme for mobile ad hoc network." Third IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 163-171, 2007
[11] Mitchell, R., & Chen, R, "A survey of intrusion detection in wireless network applications", Computer Communications, vol.42, pp. 1-23, 2014.