International Journal of Research in Advent Technology, Vol.3, No.1, January 2015
E-ISSN: 2321-9637

Survey on Intrusion Detection Technique in MANET

Bharti Wankar
M-Tech IV SEM (Digital Communiction)
Truba Institute Of Engineering & Information Technology, Bhopal,India
wankarbharti@gmail.com

Neelesh Gupta
A.P. in Electronics &Communication Engg.
Truba Institute Of Engineering & Information Technology, Bhopal,India
neelesh.gupta@trubainstitute.ac.in

Abstract- A Mobile Ad-hoc Network (MANET) is a self-created, self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. MANET is a collection of mobile nodes equipped with both a wireless-transmitter and receiver that communicate with each other via bi-directional wireless links either directly or indirectly. Security is important part to MANET. Due to its unique features such as limited power and limited bandwidth, open nature, lack of infrastructure and central management node mobility and change of dynamic topology, it is mainly use for many intelligent missions and life critical applications natural disasters. Security measures play an important role in all these applications .Hence it is necessary to include intrusion-detection system for MANETs. The existing techniques to find the malicious nodes in the presence of false misbehavior report using the three parts of EAACK schemes namely ACK, S-ACK, and MRA. These are all acknowledgement based schemes. The cryptography used in EAACK schemes are DSA and RSA for authentication process. But DSA and RSA increases network overhead.
The main aim of this work to provide secure data transmission between source and destination therefore cryptography algorithm called Advanced Encryption Standard (AES) is used for encryption and decryption of data. In proposed mechanism will authenticate the node and ensure the security of important routing information by Ad-hoc On Demand Routing Protocol (AODV).Performance of the system is increased in terms of packet delivery ratio and end to end delay.

Keywords: MANET, Intrusion Detection, AES, AODV, EAACK

1. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infra-structure.[1] [2].Ad-hoc networks decreased dependence in infrastructure and increased deployement.Since nodes are not bound to any centralized control they are free to move and hence topology changes. Mobile ad hoc network is a self-organized network of mobile nodes, without base station support. In this the mobile nodes communicate with each other with the help of a shared wireless channel. The most significant characters of MANET are mobility. This means that nodes can join or leave the network in MANET dynamically [3].This leads to rapid change in topology. In order to keep the routing information available, all the nodes need to know the topological changes occurring anywhere in the network.

2. LITERATURE REVIEW

P.Gupta et.al [4] security is major issue during communication. To overcome these problems system is developed which support to detect intruder attacks and to detect the type of attack in MANET. To apply the intrusion detection technique this paper introduced a priory known approach known as acknowledgement based approach which is used to detect intrusion in MANET. Intrusion detection technique like matching algorithm is developed.

J.Abraham et.al [5] described EAACK to tackle three of the six weaknesses of Watchdog scheme, namely false misbehavior, limited transmission power and receiver collision. In these scheme digital signature to prevent the attacker from forging acknowledgement packets. EAACK is consisted of three major parts, namely: ACKnowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehavior Report Authentication (MRA).

Z.Yan, et.al [6] proposed a trust evaluation based security solution for the ad hoc networks. It is proposed to provide effective security decision on data protection, secure routing and other network activities. Logical and computational trust analysis and evaluation are deployed among network nodes. Each node's evaluation of trust on other nodes should be based on serious study from such trust factors as experience statistics, data value, intrusion detection result, and references of other nodes, as well as node owner's preference and policy. In order to prove the applicability of the proposed solution, further

present a routing protocol and analyze its security over several active attacks.

P.Anusha, et.al [7] developed to prevent MANET from passive and active attack. It is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Paper proposed and implemented an intrusion-detection system named Improved Intrusion Detection System (IIDS) for MANETs. Compared to contemporary approaches, IIDS demonstrates higher malicious-behavior-detection rates under certain circumstances while not greatly affecting the network performances.

R.S.Singamsetty [8] proposed on quantitative method for detecting malicious nodes in the Mobile ad-hoc network is proposed. The proposed method is a behavior anomaly based system which makes it scalable, robust, configurable, and dynamic. Voting process is used in this proposed method to confirm whether a node is malicious or not. The proposed method is verified by running simulations with mobile nodes using the Ad-hoc on-demand distance vector (AODV) routing.

A.Sagar et.al [9] studied that in MANET open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. After becoming part of active path, these nodes start refusing to forward or drop data packets thereby degrades the performance of network. So a new reputation based approach is proposed that deals with such routing misbehavior and consists of detection and isolation of misbehaving nodes. Proposed approach can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path.

S.Kahate et.al [10], discussed to provide secure data transmission between the source and destination. The proposed mechanism will authenticate the node and ensure the security of important routing information in AODV protocol. Module Implementation is based on Performance Analysis of AODV, AES Implementation Module and RSA & MD5 Implementation Module.

3. PROBLEM STATEMENT

A MANET is an infrastructure-less network consisting of self-configuring mobile nodes associated by wireless links. Every single node works both as a transmitter and a receiver. Nodes correspond directly with each other when they are both within the same communication range. If not, they rely on their neighbors to relay messages.. Therefore efficient intrusion detection must be develop to secure network from malicious nodes. The proposed paper is based on intrusion detection by using AES cryptography with AODV routing protocol.

4. PROPOSED METHODOLOGY

In MANET data is transmitted in the form of packet. So before a packet is transmitted into the network, it is necessary to find secure route. AODV routing protocol is used to find secure route. Ad-hoc On Demand Distance Vector Routing (AODV) is designed specifically to address the routing problems in ad hoc wireless networks and provides communication between mobile nodes with minimal control overhead and minimal route. Ad-hoc On Demand Distance Vector Routing (AODV) being a reactive protocol does not require the maintenance of routes to destinations that are not in active communication, instead it allows the mobile nodes to obtain routes quickly to new destinations.AES technique encrypts the packet so that it is not accessible to any unwanted user. In proposed work, nodes first find out the secure route for data transmission by using AODV routing protocol. The sender sends a data to the destination through previously find secure route.

The source node sent data will be encrypted with AES encryption algorithm before its travelling to the destination node. Before receiving the data destination node will decrypted it with AES decryption algorithm. The destination node required to send an acknowledgement packet to the source. In the presence of malicious node, the destination node is not received the data from the source. Because the sender node cannot be identified the route to the destination. Flow chart of proposed paper is given below

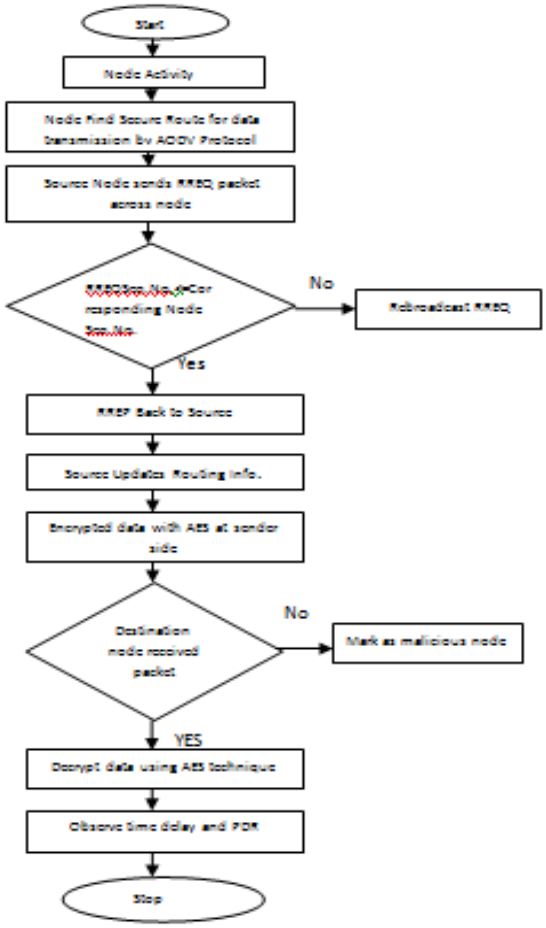

Fig.1.flow chart of proposed Methodology

5. EXCEPTED OUTCOMES

In proposed methodology packet delivery ratio is increased and malicious node detected. End to end delay is also less. No. of the received nodes increases at the receiver side so system performance is also increased.

6. CONCLUSION

MANET is a wireless communications technology whose development is in progress. In this technology data is transmitted and received by nodes with respective to the different security aspects. The technology is characterized by wide bandwidth, high spatial capacity, and increase packet delivery ration. Many researches have been done on the different aspects of MANET technology. There are many factors and parameters having a great influence on the performance analysis of the system. Proposed method improve the performance of the MANET by increasing packet delivery ration.AODV protocol is suitable for improvement of security issues So it can say that proposed approach is best for the homogenous MANET due to the higher efficiency of this routing protocol.

REFERENCES

[1] B.Patel, P.Shah, H.Jethva, N.Chavda, “Issues and Imperatives of Ad hoc Networks”, International Journal of Computer Applications Volume 62 – No.13, pp.0975 – 8887, January 2013.

[2] P. Rama Devi and D. Srinivasa Rao,” Congestion Adaptive Hybrid Multipath Routing Protocol for Load Balancing in Mobile Ad hoc Networks”, International Journal of Computer Science and Telecommunications ,Volume 3, No.12 pp.2345-4356, December 2012.

[3] N. Nasser and Y. Chen. Enhanced Intrusion Detection Systems For Discovering Malicious Nodes in Mobile Ad Hoc Network, In Proceedings of IEEE International Conference On Communication, Glasgow, Scotland, June 24 –28, 2007.

[4] P.Gupta, M.Kirkire “Intrusion Detection in MANET” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 2013.

[5] J.Abraham, V.Arun Prasath, G.Michael,” A Survey of Intrusion Detection for Ad-Hoc Network “, Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013.

[6] Yan Zheng, Zhang Peng, V.Teemupekka. “Trust Evaluation Based Security Solution in Ad Hoc Networks” Helsinki University of Technology, Finland, December 2003, pages 14

[7] K.Anusha “Secure Adaptive Acknowledgment Algorithm for Intrusion Detection System “International Journal of Emerging Research in Management &Technology ,Volume-2, ISSN: 2278-9359,March 2012.

[8] R.S.Singamsetty, "Detection of malicious nodes in mobile ad hoc networks".Theses and Dissertations. Paper 722, 2011.

[9] A.Sagar A.Ukey, M.Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010 ISSN 1694-0814 2002.

[10] S.Kahate, K.Hande “Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 5, ISSN: 2277 128X , May 2012.