IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 47-50

Performance Analysis of ABR and AASR-ABR Malicious Node Revocation using Cluster based Mechanism (AASR) in MANET

S. Mohan, K. Thamizhmaran
Assistant Professor in ECE Dept. of ECE, FEAT, Annamalai University, Annamalainagar – 608002
mohann85@yahoo.co.in
Assistant Professor in ECE, NSS & RRC PO Dept. of ECE, FEAT, Annamalai University, Annamalainagar – 608002 tamil10_happy@rediff.com

Abstract: *A Mobile ad-hoc network (MANET) is a wireless dynamic self-configurable network, which has no fixed infrastructure. Reduction of routing overhead is a main disquiet when a MANET routing protocol is residential.In AASR(Authenticated Anonymous Secure Routing), the request packets are authenticated by the group signature and to prevent the inferring of neighbouring nodes to the destination by the onion routing.In this paper,we propose the maliciousnode revocation scheme to secure the network communications, to detect the attackermisbehaviour node and to isolate it by the revocation process.The cluster based mechanism used in MANETS and compared it against the various performances through simulations.The results demonstrated positive performances against malicious nodes in the network.*

Keywords: *MANETS, Security, Cluster based revocation scheme, ABR, AASR.*

I. INTRODUCTION

The MANET is a self-configuring network of mobile nodes connected by wireless link, which is full of electromagnetic and with no fixed infrastructures or central organization. MANET which is designed momentarily for instant communication without any fixed infrastructure. The network is decentralized, where all network motion including realizing the topology and delivering messages must be accomplish by the nodes. Each node acts as a router and host, it moves in a capricious manner. Many applications like rescue operation, military operations, business meetings etc. If the node has no power,then it should not takepart in the network path.The factors affecting the MANET are Scalability,power, Latency,Data rates,security,Coverage. The features of the mobile ad-hoc network includes: Dynamic topologies. Bandwidth Constrained links, Limited Physical Security. Energy Constrained Operation. It increases the overhead of routing protocols which reduces the packet delivery ratio and also increases the end-to-end delay. Thus, reducing therouting overhead in route discovery is an essential problem. The conventional on demand routing protocols use flooding to discover a route. MANETS canbe used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such application. They broadcast a Route Request(RREQ) packet to the networks and the broad casting induces excessive redundant retransmissions of RREQ packet.An important issue in MANETs is the Time-varying network topology,Mobility, Limited Battery Power, Limited Bandwidth, Wireless Transmitter Range, Route discovery required frequently.The reduction of routing overhead is a main concern when a MANET routing protocol is developed.

II. SECURITY ISSUES IN MANET

A MANET that consists of hundreds or thousands of mobile nodes in the self-configuring network, Security network mainly used to handle such a large network. Security in MANET can affect the entire network.To secure the ad-hoc networking the following factors such as availability, confidentiality, integrity,authentication, non-repudiation to be considered.In the wireless ad-hoc network there are two types of attacks they are, Active attacks Passive attacks. The nodes in which the energy can be loss to perform the various dangerous operation .The energy lost occurred due to the misbehaving of the node is termed as active attacks.The active attacks can be classified in to dropping,fabrication, modification and timing attacks.The passive attacks,nodes detect the information about the network.The examples of passive attacks are eaves dropping and traffic analysis.It is mainly watch the networks action and used to save the energy.The malicious nodes can be detected with the aim of damaging other nodes by causing network outage It can be considered as a selfish because saves the battery life for their own communications.Therefore these selfish nodes can severely degrade the performance of network.There are mainly two protocols used in MANET's link layer protocol and network layer protocol. The wormhole attack and the black hole attack are the other types of attacks.In the wormhole attack,attacker used to forward packets through the tunnel.The various steps to avoid the attacks in

the MANET's are:Secure Multicasting. Secure routing. Privacy-aware and Position based Routing.The network layer is the one where routing takes place. A router's main function is to get packets from one network to another on the network topography. The third layers protocols and technical methods allow for network-on to-network communications as needs. The corresponding third layer switch is simply a Layer 2 device that also does routing (a Layer3 function). Another key to the aspect of routers is to the each one of the interface on a router has its own IP address, because each of those interfaces is on different networks.

III. MOTIVATION

As per explained in issues troubled with the MANET are security, mobility, open medium, dynamic shifting topology, lack central monitoring and organization. These factors are dependable for misery attacks in mobile ad-hoc network. An ease of use of network services, confidentiality and integrity of data can be achieved by using routing protocols. With this weakness an intrusion detection system provides solutions is to detect and prevents against different types of attacks in various layers**.** With the help of routing protocol and using MARS4 algorithms to develop the security provides high efficiency of securing the data over the wireless network.

IV. PROBLEM IDENTIFICATION

Network wide routing in MANETs is a vital task of transferring data from a source to destination. The dynamic nature of MANETs requires the routing protocols to refresh the routing tables frequently that suffer from transmission contention and congestion that are the results of the broadcasting nature of radio transmission since a node in a MANET cannot directly communicate with the nodes outside its communication range, a packet may have to be routed through intermediate nodes to reach the destination. So it also becomes essential to monitor the constraints in intermediate nodes. Consequently, an efficient routing approach may generate route failures. The simplest scheme routing in MANET is the one to find a route without malicious nodes. This paper aims to provide an unbreakable route for secured transmission. We propose the malicious node revocation scheme to secure the network communications. This AASR- ABR provides better performance compared to the existing reactive routing protocols and also reduces routing overhead without any misbehaviour at intermediate nodes from source to destination.

V. CLUSTERING BASED CERTIFICATE

The formation of cluster is depends on the behaviour of the nodes within the Network. Every node in the network may be classified as: Legitimate Node, Malicious Node, Attacker Node,A legitimate node for secure communications in MANETs. It is used to detect attacks from the malicious attacker node. In the malicious node,it will not execute the protocols exactly. Attacker Node is a special malicious node.The heavy packet loss can be occurred in the node and it totallydisrupts the secure communications.The group of the nodes basically forms the Cluster.Each cluster consists of Cluster Head with many cluster Members.The Cluster head transmits HELLO packets to neighboring nodes.The nodes within the transmission range of the cluster head can accept the packets and sent reply RP packets and to form the clusters.The certification Authority can be formed in aclusterand it control the entire actions in the network.The certification authority consists of two lists, WarnList BlackList The list that contains the nodes information.The Warn list is used to hold the accused nodes in the cluster and black list contains the malicious node or an attacker node.

VI. SIMULATION

To facilitate the comparison of the simulation results with other research works, the default scenario setting in NS 2.34 has been adopted. The maximum hops allowed in this configuration setting are four. Both the physical layer and the 802.11 MAC layer are included in the non-wired extension of NS2, where the total bits transmitted is calculated using application layer data packets only and total energy.

Table 1 Simulation parameter

Parameter	Values
Examined protocol	AASR-ABR
Application traffic	CBR
Transmission range	900m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	800s
Number of nodes	150
Area	680 x 680m

VII.RESELTS & DISCUSSION

In this paper discuss AASR performance of different sets of nodes with follow above simulation parameters.

Table 2 Results of Packet Delivery Ratio

Packet delivery ratio					
Protocol/NN	**30**	**60**	**90**	**120**	**150**
ABR	**0.83**	**0.77**	**0.71**	**0.56**	**0.59**
AASR-ABR	**0.91**	**0.85**	**0.79**	**0.73**	**0.67**

From Table 2, it is clear that secure proposed scheme AASR-ABR surpasses ABR performance by above 70% when there are 30 and 150 nodes in the network.

Table 3 Results of Routing Overhead

Routing Overhead					
Protocol/NN	**30**	**60**	**90**	**120**	**150**
ABR	**0.17**	**0.23**	**0.29**	**0.35**	**0.41**
AASR-ABR	**0.14**	**0.20**	**0.26**	**0.32**	**0.38**

Simulation results of routing overhead Table 3. It is clear that AASR-ABR has the lowest overhead of about 30 to 150 number of nodes.

Table 4 Results of Throughput

Throughput					
Protocol/NN	**30**	**60**	**90**	**120**	**150**
ABR	**0.13**	**0.25**	**0.38**	**0.51**	**0.55**
AASR-ABR	**0.22**	**0.34**	**0.47**	**0.60**	**0.64**

Table 2 proves that the proposed AASR-ABR provides better performance of the throughput when there are 10 to 100 of nodes compared to ABR routing protocol

From the above table, it is clear that the comparison of the AASR-ABR illustrate that the proposed algorithm outperforms the ABR by providing lowest end-to-end delay, packet drop and routing overhead with increase in the number of nodes.

VIII. CONCLUSION AND FUTURE WORK

Packet-dropping and loss attack have always been a major threat to the security in MANETs. In this research paper, a novel approach named AASR-ABR protocol specially designed for MANETs is proposed in comparison with other popular techniques in different scenarios through simulations. The results demonstrated positive performance of the remaining energy in AASR-ABR than, the research was extended to incorporate elliptical curve cryptography in this proposed scheme. Although it generates more end-to-end delay in some cases, as demonstrated in this research, it can vastly improve the network's PDR to more than 1.8% compared to the existing ABR routing protocol and improve remaining energy by 6% compared to the existing ABR routing protocol when the attackers are smart enough to forge acknowledgment packets. AASR cryptography schemes were implemented in the simulation. Eventually, it is arrived to the conclusion that the AASR-ABR scheme is more suitable to be implemented in MANETs. To increase the merits of this research work, there is a plan to investigate the following issues in our future research.

- The same concept can be applied in satellite to reduce more congestion in the route and also to save more energy.
- The possibilities of adopting the shortest path algorithm to eliminate the requirement of redistributed end to end delay can be examined.
- The performance of AASR-ABR can be tested in real time network environment instead of software simulation.

REFERENCES

[1]. A.Rajaram, Dr. S. Palaniswami, "Malicious Node Detection System for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies, Vol. 1,NO. 2, 2010, 77-85.

[2]. H. Shen and L. Zhao, "ALERT: An Anonymous Locationbased Efficient Routing Protocol in MANETs," IEEE Transaction on Mobile Computing, Vol. 12, No. 6, pp. 1079– 1093, 2013.

[3]. J. Kong and X. Hong, "ANODR: ANonymous On-Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.

[4]. J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad-hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.
[5]. K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Transaction on Mobile Computing, Vol. 10, No. 9, pp. 1345– 1358, Sept. 201.
[6]. M. Yu, M. C. Zhou, and W. Su, "A secure routing protocol against Byzantine attacks for MANETs in adversarial environment," IEEE Transaction on Vehicular Tech., Vol. 58,No. 1, pp. 449–460, 2009.
[7]. RadhikaSaini, ManjuKhari, "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network", International Journal of Computer Applications, Vol. 20, No. 4, 2011.
[8]. RamandeepKaur, Jaswinder Singh, " Towards Security asgainst Malicious Node Attack in Mobile Ad-Hoc International Journal", Vol. 3, No. 7, 2013.
[9]. R. Song and L. Korba, "A robust anonymous ad hoc ondemand routing," in Proc. IEEE MILCOM'09, Oct. 2009.
[10]. S. Seys and B. Preneel, "ARM: Anonymous Routing protocol for mobile ad hoc networks," Int. Journal of Wireless and Mobile Computing, Vol. 3, No. 3, pp. 145– 155, 2009.
[11]. Wei Liu, Hiroki ninshiyama and Neikato, "cluster-based certificate revocation with vindication capability for mobile ad hoc networks," IEEE transactions on parallel and distributed systems,2013.
[12]. Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for MANET," IEEE Transaction on Wireless Communication, Vol. 11, No. 5, pp. 1922–1932, 2012.

BIOGRAPHY:

S. MOHAN received his BE and ME from Annamalai University, Tamilnadu, India in 2007 and 2012, respectively. He is currently working as an Assistant Professor of ECE in the Department of Electronics and Communication Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu, India. His research interest includes wireless communication, networking.

K. Thamizhmaran received his BE and ME from Annamalai University, Tamilnadu, India in 2008 and 2012, respectively. He is currently working as an Assistant Professor of ECE in the Department of Electronics and Communication Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu, India. His research interest includes networks security, ad-hoc networks, mobile communications, and digital signal processing. He has published more than 89 technical papers at various national / international conferences and in journals. He is a life member of IAENG and IACSIT.