Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Quality Measuring of Multicast Communication in Secure MAODV Protocol under MANET

Ankita Singh
Department of CSE
LNCT
Bhopal, India

Tripti Saxena
Asst. Prof., Department of CSE
LNCT
Bhopal, India

Vineet Richhariya
HOD, Department of CSE
LNCT
Bhopal, India

Abstract- The absence of centralized authority is the reason of attack that easily affects the routing performance in MANET. MANETs are vulnerable to various attacks at all layers, including in particular the network layer, because the design of most MANET routing protocols assumes that there is no malicious intruder node in the network.MANET faces various challenges like security issue, quality of service issue and routing decision as well as group communication. Before that various work done to resolve the entire problem with the help of number of technique so here we design secure group communication with the help of MAODV routing and node behaviour analysis base prevention mechanism that work improve the quality of service as well as provide reliable communication to the network and maintain group communication. The proposed prevention scheme in this paper provides the secure communication among the neighbours in presence of attacker. The performance is measured through performance metrics like PDR, Routing load and data dropping.

Keywords- MAODV MANET, Multicast, PDR, Attack

I. INTRODUCTION

The future military communication networks are envisioned to support a diverse range of applications such as voice, data, video, broadcast, imagery, and multicast services for users.

The networks will consist of both wired and wireless connections. The wireless connections can either be mobile or stationary. In general, mobile wireless connections have limited capacity, have constantly changing topology, and are subject to significant transmission delays.

Many existing and forthcoming applications in MANETs require the collaboration of groups of mobile users. Communications in battlefield and disaster relief scenarios, video conferencing and multi-party gaming in conference room or classroom settings, and emergency warnings in vehicular networks are example applications. As a consequence, multicast in MANETs becomes a hot research topic in recent years. Multicast is a communication scheme for sending the same messages from a source to a group of destinations. MANETs are inherently ready for multicast communications due to their broadcast nature. However, limited bandwidth between mobile nodes and highly dynamic topology due to unpredictable node mobility make the design of scalable and QoS-aware multicast routing protocols much more complicated than that in the traditional networks [3].Most of the multicast protocol proposed for ad hoc networks assume a trusted, non-adversely environment and do not take security issues into account in their design.

But in real time a MANET is vulnerable to attacks than a wired or infrastructure wireless network. Here we investigates the security of Multicast Ad-hoc on demand distance vector protocol (MAODV), a well known multicast routing protocol in MANET by identifying the impact of routing mis-activity nodes on it. Though there exists many security extensions on MAODV, the abnormal behaviour of nodes have not been explored extensively. Thus, a security extension to address the mis-activity node attack in multicast routing has been proposed in this title [4]

Security issues of MANETs in group (multicast) communications are even more challenging because of the involvement of multiple senders and multiple receivers as well as group membership leaving and joining information storing are complex so here we design architecture to solve problem of security and group management under MANET, in this paper we also measure the quality with different parameters in different environment namely as normal routing, attacker and prevention case [2].

II. RELATED WORK

This section provides a general overview on multicasting trends and previous frameworks introduced in research community. Several multicast routing protocols with unique features have been proposed for MANETs in the literature.

This section provides a general overview on multicasting trends and previous frameworks introduced in research community. Several multicast routing protocols with unique features have been proposed for MANETs in the literature.

K. Chen, K. Nahrstedt, [5] "Effective location-guided tree construction algorithms for small group multicast in MANET," In, the Small Group Multicast (SGM) protocol based on packet encapsulation is proposed. This protocol builds an overlay multicast packet distribution tree on top of the underlying unicast routing protocol. Different from the DSM protocol that computes the multicast tree at each sender, this protocol constructs the tree in a distributed way: each

node only constructs its out-going branches to the next-level sub trees and forwards the packet to the roots of the sub trees. This process repeats until all the destinations have been reached. This protocol is more scalable than the DSM protocol because the nodes in a group need not to know the global network topology. Instead, they are only aware of each other in terms of the group membership and the location information of the group nodes. However, this protocol does not specify a method for dynamic joins and leaves in terms of location update among the group nodes. Therefore, this protocol is more suitable for the groups in which the group membership is static.

M. Mauve, H. Fubler, J. Widmer, T. Lang, [6] "Mobile Ad-Hoc Poster: Position-based multicast routing for mobile Ad-hoc networks," In, the Position-Based Multicast (PBM) protocol is proposed using only locally available location information about the destination nodes. This protocol provides a solution in order to approximate the optima for two potentially conflicting properties of the multicast distribution tree: (1) the length of the paths to the individual destinations should be minimal, and (2) the total number of hops needed to forward the packet to all the destinations should be as small as possible. If not properly handled, a greedy multicast forwarding may lead to a problem when a packet arrives at a node that does not have any neighbor providing progress for one or more destinations.

B. Karp, H.T. Kung,[7] "GPSR: Greedy Perimeter Stateless Routing for wireless networks," in this title to solve the problem in location-based unicast routing, such as using the right hand rule-based recovery strategy. This protocol extends the strategy to support the packet with multiple destinations. This protocol can deal with group members distributed in large-scale MANETs. However, it cannot scale well in terms of the number of group nodes due to the fact that the location and group membership information is required at each sender of the multicast group.

M. Transier, H. Fubler, J. Widmer, M. Mauve, W. Effelsberg,[8]"Scalable position-based multicast for mobile ad-hoc networks," In, the Scalable Position-Based Multicast (SPBM) protocol is proposed to extend PBM. SPBM uses a hierarchical aggregation of membership information: the further away a region is from an intermediate node, the higher the level of aggregation should be for this region. This hierarchical scheme improves scalability. However, because all the nodes in the network are involved in the membership update, it still cannot scale well in large-scale MANETs. In this paper, we solve this problem by summarizing the group membership information in a novel way and disseminating this information to only a portion of nodes in the network. Therefore, our scheme can potentially scale well in terms of both the number of groups and the number of group nodes in each group in large-scale MANETs.

Hu and Evans developed a protocol using directional antennas to prevent wormhole attacks [9]. Directional antennas are able to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from west and the other at east). This protocol fails only if the attacker strategically placed wormholes residing between two directional antennas.

Rouba El Kaissi et.al [10] obstacles impede the successful deployment of sensor networks. In addition to the limited resources issue, security is a major concern especially for applications such as home security monitoring, military, and battle field applications. This paper presents a defense mechanism against wormhole attacks in wireless sensor networks.

Y. C. Hu et.al. [11] have considered packet leashes – geographic and temporal. In geographic leashes, node location information is used to bound the distance a packet can traverse. Since wormhole attacks can affect localization, the location information must be obtained via an out-of-band mechanism such as GPS. Further, the "legal" distance a packet can traverse is not always easy to determine. In temporal leashes, extremely accurate globally synchronized clocks are used to bound the propagation time of packets that could be hard to obtain particularly in low-cost sensor hardware. Even when available, such timing analysis may not be able to detect cut-through or physical layer wormhole attacks.

Shalini Jain, Dr.Satbir Jain [12]"Detection and prevention of wormhole attack in mobile ad-hoc networks" This title we present a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, we demonstrate that our scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.

Ankita Singh, TriptiSaxena,VineetRichhriya[1] "Secure and Effective Group Communication using MAODV Routing in MANET". Here we design a secure group communication with the help of MAODV routing and node behaviour analysis base prevention mechanism that works to improve the quality of service as well as provides reliable communication to the network**.**Further, we detect attacker node and protect our system using prevention mechanism.

III. PROPOSED WORK

Multicast communication in MANET environment is very challenging issue because node move freely anywhere with independent nature, so big task to form group as well as group coordinator selection and joining and leaving information of receiver node's, for that situation handling we apply multicast ad-hoc on-demand distance vector routing for coordinate selection, and route establishment between sender to group membership communication, but various types of attacks are present in MANETs like black hole attack, wormhole attack, rushing attack, jellyfish attack, neighbor attacks, grayhole attacks, and flooding attacks, Repeater attacker. All previous studies have considered only unicast networks in which there is only single sender and single receiver in a communication session and solutions for some of these attacks have been addressed. even though many researchers have addressed security issues for unicast, but researchers still very early stage to work multicast security in MANETs due to several challenges specific to multicast operations such as group key management, mobility handling, Encryption, member access control, and secure routing. Here we design secure architecture in multicast ad-hoc communication using multicast intrusion detection system and provide best quality of service to the user. Initially we define mobile node in the network and apply multicast routing,

and form group, for that group formation we identify coordinator using group election method and after that generate output file, that file useful for analyze purpose and identify normal and abnormal activity of the network and detect mis-activity from the network, after getting the information of mis-activity type and mis-activity node we protect the communication using MAODV-IDS base, IDS watch the all neighbour node behaviour and if they identifies any mis-activity happen in the network so positively send blocking message to mis-activity spreader node and also send information about mis-activity node to the sender, so that the sender change the new route and send safely data to group members and protect them.

IV. GROUP COMMUNICATION AND ELECTION ALGORITHM

A. Group Formation

Step 1: Set Mobile Node M = { V_1, V_2…… V_{i-2}, V_{i-1}, V_i, V_{i+1}, V_{i+2}……V_n} **//Set of mobile Node's**

Step 3: Select random nodeV_iє N for election message generation

Step4: Calculate S_i = $D/(t_2-t_1)$ // t_1 initial time , t_2 Broadcast Time, D distance travel

Step 5: Broadcast-Elct-msg(V_i,S_i)

// S_i is speed of i^{th} node

{

If (radio-range<=550 && neighbour == True)

{

Record time at t_n; **// t_n time in second's**

Get neighbour V_{i-1}, V_i, V_{i+1}, $V_{i+2,...}V_{i+n}$

Get info [Vj][S_j] **// $S_j$is speed ofj^{th} node**

Compare if ($V[s_i]$> $V[s_j]$)

{

Eliminate V_i from competition

Set new V_i = V_j;

New V_i generate election msg ;

Goto step 5:

}

Else { V_i as a coordinator;}

}

B. Sending of Data to Group

//Manage and broadcast group message through coordinator under MANET

Set mobile node = M ; // mobile node

Set group coordinator = V_i; // V_i € M, V_i select on the bases of energy and speed

Send group_join_msg (m_n , V_i, No) // group join message

{

if (range <=550 && V_i == "true")

{Join group member = {m1, m2…..m_n} // m_n€ V_i, if $m_n$is in radio zone}

Else {Out of range}

Set sender node = S;

Set routing = MAODV; //Routing Protocol

Broadcast _RREQ(S, V_i, rr)

{ if (rr<= 550 && neighbour>=1)

{forward RREQ and create Rtable

If (V_i =="true")

{accept route packet and send group info

}

Sender sends actual data to V_i node;

Call group-msg(S,m_n, type);

}

}

Else { node out of range or unreachable; }

Group-msg(S,m_n,type) // type contain packet info

{Search m_n nodes in radio range;

Broadcast actual data to all group member m_n;

}

C. Steps for Secure Group Communication

In this proposal we provide secure multicast communication and simulate our result using network simulator -2 and following step we do.

- Create Mobile node

- Identify coordinator node for group communication
- Generate output file
- Analyze behaviour
- Identify abnormal or attacker node
- Inbuilt security model into NS-2
- Block attacker node using MAODV-IDS protocol
- Analyze quality of service of entire network

V. SIMULATION SETUP

Network simulator 2 is the result of an on-going effort of research and development that is administrated by researchers at Berkeley. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols .The simulator is written in C++ and a script language called OTcl2. Ns use an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called is Simulation setup.

A. Simulation Parameter

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc.
According to below table 1 we simulate our network.

Table i simulation parameters

Number of nodes	50
Dimension of simulated area	800×600
Routing Protocol	MAODV
Simulation time (seconds)	100
Transport Layer	UDP
Traffic type	CBR
Packet size (bytes)	512
Number of Attacker Node	4
Maximum Speed (m/s)	Random
Prevention Mechanism	Message base
Detection	Node PDR base

B. Data Receiving Analysis

The data receiving analysis in a given simulation time of 100 seconds is illustrated in this graph in normal multicasting MAODV, Attack with MAODV and Prevention MAODV. The data receiving in due to routing misbehaviour of attacker drops the huge amount of data in network by that the only 3 packets are received in network but the prevention scheme provides the better performance and secure communication in presence of attacker.

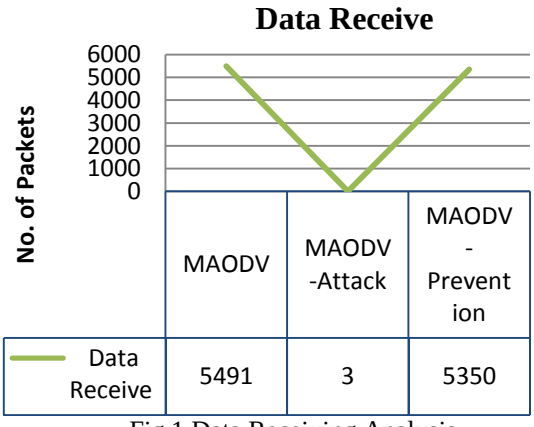

Fig.1 Data Receiving Analysis

C. Routing Load analysis

The less routing packets in network is always represents the better performance in network it implies that the attacker routing load in network is showing the better performance in network. In this case first to analyse the data receiving in network that is worst due to the dropping of attacker. It means for few packets about 930 routing packets are deliver in network. That is represents the malicious behaviour of attacker. But in prevention with respect to routing packets about 4 time more data packets are deliver in network.

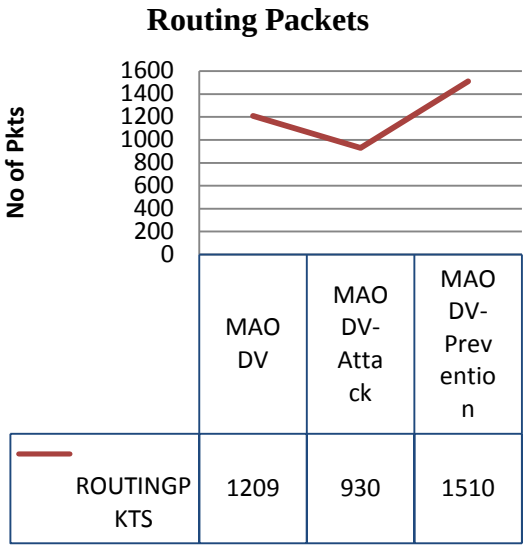

Fig.2Routing Packets Analysis

D. Normalized Routing Load Analysis

The routing load is measure here is the ratio of routing packets and data received packets. In this graph we clearly visualized the attacker routing misbehaviour in network. The routing load in network is always better if it is less than or equal to one. This only in case of normal MAODV and prevention in MAODV, that is showing better performance.

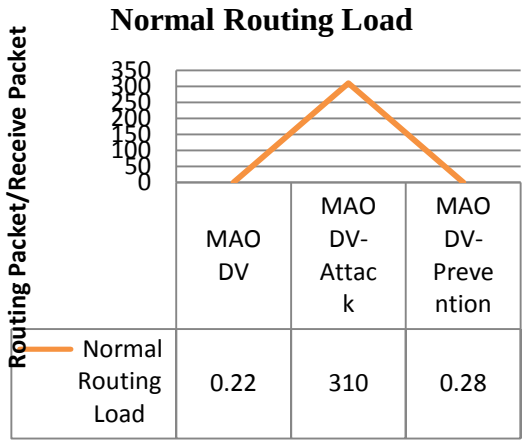

Fig.3 Routing Load Analysis

E. Packet Delivery Ratio Analysis

The PDR is the packet percentage receiving analysis in case of normal MAODV, Attack and Prevention scheme. The PDR performance in case of normal multicasting routing is about more than 99% but in attack the routing performance is almost nil. The proposed prevention scheme is showing the again secure network to provides the attacker free network that again obtain the PDR more than 97% i.e. much better performance.

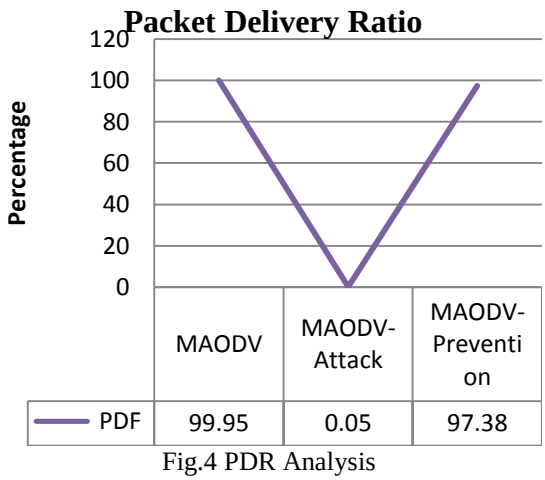

Fig.4 PDR Analysis

F. Packet Drop Analysis

The packet dropping in network has many reasons like congestion, collision destination unreachable and many more. The packets dropping reason in this research is routing misbehaviour of attacker in MANET. The packets dropping due to attacker is heavy, almost all packets are drop in network. The dropping in prevention and normal routing is showing the better network performance.

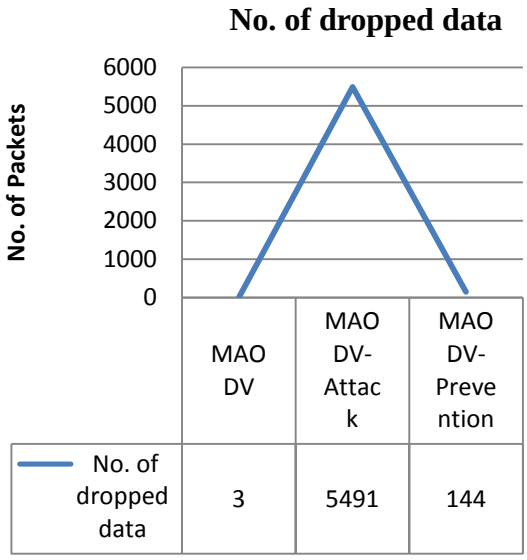

Fig.5 Data drop Analysis

VI. CONCLUSION AND FUTURE WORK

In MANET routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. Consequently, a malicious node can exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In this research we apply security scheme on MAODV (multicast ad-hoc on-demand distance vector routing) and deploy network after that provide group communication, in this paper we analyze the routing attack protection and provide reliable communication, initially we identifies data drop reason and detect attacker node after that we prevent through attack symptoms base message sending mechanism and get 100 percentage recovery through attack behaviour, and quality of service measure with the help of packet delivery ratio , result conclude that the proposed security scheme is much better and provides the secure communication in presence of attacker to block their misbehaviour.

In future we also apply ODMRP routing for energy efficient routing in network for utilized the battery life time in network. Also try to compare the congestion control scheme in multicasting and multipath routing in MANET.

REFERENCES

[1] A. Singh, T. Saxena and V. Richhriya, *Secure And Effective Group Communication using MAODV Routing in MANET*, International Conference on Computational Intelligence and Communication Networks (CICN-2014), Nov. 08-09,2014, India.

[2] N. Sreenath, A. Amuthan, and P. Selvigirija, *Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs*, 2012 International Conference on Computer Communication and Informatics (ICCCI -2012), Jan. 10-12, 2012, Coimbatore, INDIA

[3] M.Nagaratna et al., *Team Multicasting Routing Protocol In MANETs*, IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.6, June 2009

[4] P. Sankareswary et al., *Impact of Selfish Nodes in Multicast Ad Hoc On demand Distance Vector Protocol*, ICWCSC 2010X

[5] K. Chen and K. Nahrstedt, "*Effective location-guided tree construction algorithms for small group multicast in MANET*,"Proc. IEEE 21th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), Vol.3, pp. 1180-1189, Jun. 2002.

[6] M. Mauve, H. Fubler, J. Widmer and T. Lang, "*Mobile Ad-Hoc Poster: Position-based multicast routing for mobile Ad-hoc networks*," ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 7, No. 3, pp. 53-55, Jul. 2003.

[7] B. Karp and H.T. Kung, "*GPSR: Greedy Perimeter Stateless Routing for wireless networks*," Proc. 6th annual international conference on Mobile computing and networking (MobiCom 2000), pp. 243-254, Aug. 2000.

[8] M. Transier, H. Fubler, J. Widmer, M. Mauve and W. Effelsberg, "*Scalable position-based multicast for mobile ad-hoc networks," Proc. First International Workshop on Broadband Wireless Multimedia: Algorithms*, Architectures and Applications (BroadWim 2004), San Jose, CA, Oct. 2004.

[9] L. Hu and D. Evans, "*Using directional antennas to prevent wormhole attacks*," in Proceedings of the Network and Distributed System Security Symposium.

[10] R. E.Kaissi, A. Kayssi, A. Chehab and ZaherDawy, "*Dawsen: a defense mechanism against wormhole attacks in wireless sensor networks*", IN Second International Conference on Innovations in Information Technology (IIT'05).

[11] Y. C. Hu, A. Perrig, and D. Johnson, "*Packet leashes: a defense against wormhole attacks in wireless networks*," in INFOCOM, 2003.

[12] S. Jain andS. Jain "*Detection and prevention of wormhole attack in mobile adhoc networks*" International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

