Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Improved Location Aided Cluster Based Routing Protocol in MANETs

Yogita Wankhade*, Pankaj Vidhate, Vidya Dhamdhere

University of Pune,

India

Abstract— MANET is a network of mobile nodes that interconnect, interact with and collaborate with each other. Security is the main challenge for MANETs. Many attempts were made to secure a cluster based routing protocol, but due to lack of fixed infrastructure and central management, the security solution is challenging research. Intrusion detection System is one of the key technique and best solution to protecting an Improved Location Aided Cluster Based Routing Protocol - ILCRP on mobile ad hoc network. The unique features of ILCRP are the important factors of our success to achieve our goal for propose enhancement based on characteristics and measure of efficiency of intrusion detection system in terms of packet delivery ratio.

Keywords— MANET, IDS, Packet delivery ratio, ILCRP, Cluster Head.

I. INTRODUCTION

Mobile Ad Hoc Networks are created on the fly. In MANETs, there is no fixed infrastructure for the configuration of the network, nodes in the network are expected to assist in the routing of packets, and all hosts are allowed to move more freely through the network. Successful routing protocols provide means to deliver packet to destination given these dynamic topologies. We found different types of position based routing protocols during literature survey. In the Position based routing protocols, the mobile nodes uses a GPS system. They calculate their position using the distance formula as follows $d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$.

Security is the major issue in MANET. One of the promising ways to provide security is by means of IDS. The Architecture of IDS that best suits MANET is distributed cluster based. Position based routing protocols provides the following advantages. They provide better scalability and performance by using geographical position to improve routing decisions & efficiency. Cluster based routing protocols offers some advantages over other position based routing protocols. First, it uses multiple channels effectively and improves system capability. Second, it strengthens node management reduces the exchange overhead of control messages. Third, it provides Quality of Service for multimedia services efficiently. Finally, this supports the mobile ad hoc networks with a huge number of mobile nodes. The ILCRP protocol is a clustering protocol which is applicable for highly mobile ad-hoc networks was proposed earlier, where all the nodes are GPS enabled to increase the packet delivery ratio, reduce the control overhead and decrease end to end delay [1]. An intrusion-detection system (IDS) can be described as tools and methods to help identify, report unauthorized network activity. Intrusion detection is the one of the method to identify actions that attempts to compromise the integrity and confidentiality of a resource [11], [12]. It is technique to detect intrusion into network by observation of activities or audit data [2]. Hence in the mobile ad-hoc networks, we need to identify malicious nodes in the network trying to behaving malicious.

In section II, we discuss the related work. The proposed scheme has described in section III. Algorithms has described in section IV. A test result has been shown in section V and finally section VI has concluded the work.

II. RELATED WORK

Here is the summary of the some research papers that give an idea of the kind of work done in location aided routing protocol location aided cluster based routing protocol and performance metrics are delivery ratio, end to end delay and control overhead. An extensive literature survey was done before making any assumption in our work. MFR- (Most Forward within R) is a greedy position based routing protocol which tries to minimize the number of nodes by selecting the farthest node from its neighbours [3], [9], [10]. By using Greedy approach MFR do not maintain paths from source node to destination node. MFR has the shortcomings that it does not guaranteeing to find the path to the destination or a path which is longer. Due to the distance between the nodes, MFR is noted as packet dropping rate increases, especially in large network. LAR- Location Aided Routing uses restricted directional flooding for enhancing route discovery. Using GPS for location information LAR limits the searching for a new route to the smaller “Request Zone” [4], [5], [9], [10]. If the discovered route breaks for any reason and failure of single Node might result in packet loss, so the route discovery process must start again.

GRID- It includes geographic area that is partitioned into number of squares. A set is dominating of all the nodes and one mobile host closest to the centre as the leader of the grid. GRID saves network energy and route discovery,

maintenance as well as packet relay are more efficient. Failure of single node, results in packet loss and setting up of a new route [9], [10].

TERMINODES- This protocol is a hierarchical routing protocol. Terminodes presents two levels called TLR- Terminode local routing and TRR- Terminode remote routing [5], [9], [10]. If the destination closes to the source, then TLR is used and for long distance routing (TRR) is used. It enhances the packet delivery ratio. Failure of any node may result the packet loss and low overhead due to small packets. PNR- position and neighbourhood based routing the protocol uses "Need to know" concept to update the routing table [6], [9], [10]. The network is divided into quadrants and only maintains summarized information through GPS technology. When a node receives a flood message from another node, it will maintain the position information about nodes. This protocol reduces the packet transmission to only the nodes in need of knowing new position.

LACBER- Location aided cluster based energy efficient routing protocol. It proposed for GPS scarce mobile ad-hoc networks. The LACBER protocol requires one GPS enabled or antenna equipped node in every cluster [1], [7], [8], [9], [10].Comparing with cluster based routing protocols the formation of cluster in LACBER results high control overhead. Due to the absence of GPS, the exact location of nodes is difficult to determine. ILCRP- This is Improved Location Aided Cluster Based Routing Protocol proposed to improve packet delivery ratio. All the nodes in ILCRP are GPS enabled compared with few nodes in LACBER protocol [1], [8], [9], and [10]. ILCRP performs better as compared to GPS free and GPS scarce MANET.

III. PROPOSED SCHEME

The Proposed scheme ILCRP-IDS uses Distributed Cluster based IDS with GPS enabled nodes and it overcomes the problems associated with passive and active attacks and energy consumption by introducing the Intrusion Detection System (IDS). In ILCRP-IDS ,due to energy constraint the cluster head selects node with a second highest Node Value as in ILCRP as the Monitoring Node of the cluster .It is in the Monitoring node that the IDS is located .This node monitors and captures live packet traffic on the network. The proposed intrusion detection model includes five major components that is, Monitoring Node (MN), Cluster Head (CH), Gateway Intrusion Detection (GN), Local Sensor Node (LN),global cooperative decision module(CM).

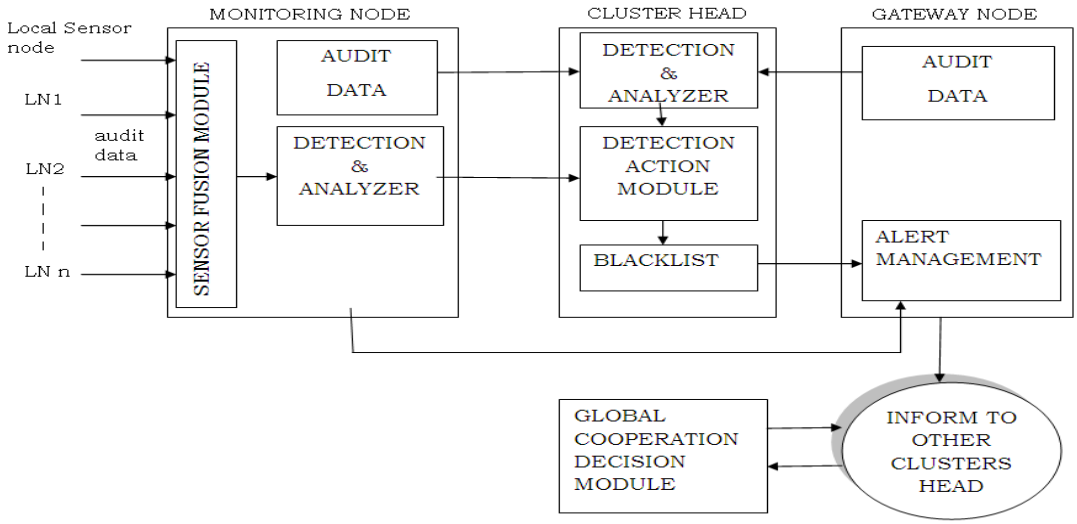

Fig. 1 IDS with ILCRP

In this new architecture, every mobile node runs a LN locally to perform local data collection and obtain data and forward it to DA (Detection and Analyzer) of the monitoring node which initiates local response to Action module, and only a subset of the nodes will run GN and these nodes are organized into multiple layers. The monitoring nodes Data collection module as shown in Fig.1 combines all the audit data of all the nodes in the cluster to analyze each transmission that occurred in the cluster. Analyzing the audit data, the monitoring node detects any malicious activity in the path of the nodes between the source and destination node using Detection and Analyzer (DA).Then detection action will be taken and forward to the blacklist.

Local alarms indicate a security attack observed by local DA, and global alarm decisions made by GN. When a node detects an intrusion with right evidence, the node can inform an alarm message to the CH by sending. If any malicious activity is found on the node, the cluster head replaces with another node and moving the node to blacklist, which in turn triggers alert management. There may be a possibility that the monitoring node can become malicious node. In order to monitor the activity of the monitoring node, the cluster head detect and analyze the audit data obtained from the monitoring node. If any malicious activity is found on the node, the cluster head replaces with another node and moving the node to blacklist. Cluster head also monitors the activity on the gateway node. There may be another possibility of malicious activity on the cluster head itself whose activities are collectively monitored by all the nodes in the cluster. However, if a node moved from the first cluster to nearer cluster, the monitoring node informs Local Alert to the GN, which directly starts global cooperative intrusion detection procedure, and inform to other cluster.

To collect the strong evidence about the malicious node nearer cluster will be participate in the global cooperation decision module. At the same time, any cluster member does not have evidence should not participate in the global cooperation decision. Blacklist will maintain by every cluster head as a part of CAT (Cluster adjacency table), we can minimize energy consumption for detection purpose. The monitor node is the responsible node for detection process; due to this battery may get reduced faster than cluster members. Care should be taken to elects another cluster-head from time to time as battery power of node elapsed. There may be a possibility that the monitoring node can become malicious node. In order to monitor the activity of the monitoring node, the cluster head detect and analyze the audit data obtained from the monitoring node. If any malicious activity is found on the node, the cluster head replaces with another node and moving the node to blacklist. Cluster head also monitors the activity on the gateway node. There may be another possibility of malicious activity on the cluster head itself whose activities are collectively monitored by all the nodes in the cluster.

A black hole may falsely replies for any route requests for specified destination and drops some received packets. If few malicious nodes come together in a group then there will be serious damage. Due to continuous monitoring of the transmission and reception of metadata, a node functioning as the black hole can be easily identified and submitted to cluster head for further action. On receiving information from the monitoring node, the cluster head marks that node as the blacklisted node of the cluster and adds it to the blacklist. The cluster head broadcasts the blacklist to all the member nodes of the cluster. The gateway node informs the adjacent clusters about the malicious node. Since ILCRP uses the permanent identifier for all nodes which is the MAC address, the adjacent cluster heads adds the MAC address to their clusters blacklist. A wormhole attack is an attack on MANET where two attackers connected through high speed channel link, are intentionally placed at different tops of a network. They have the complete control of the link; in this, attackers may drop packets which are forwarded by this link. All packets can be dropped by an attacker which can be a small portion of packet or specified targeted packet. Since exact information of the nodes is known to all the nodes in ILCRP, the wormhole does not exist in the cluster. Node impersonation does not occur due to use of long and permanent identifier for each node.

IV. ALGORITHM

A. Cluster Head Election Procedure algorithm

1) Find the neighbours for every node present say v. This will give the degree of that node say dv.
2) Then calculate the dynamic average for the speeds for each node. This can be used for the measurement of mobility which can be represented with the help of Mv.
3) Calculate the sum of distances with $Pv = \sqrt{(x1 - x2)^2 + (y1 - y2)^2}$ for each node from all its neighboring nodes.
4) For each node v, find out the degree-difference Dv, in this dv is the degree of that node and Mv is mobility through which the nodes are moving in random direction. Dv is calculated with $Dv = dv - Mv$.....(1)
5) Calculate the duration, Tv, for the node v for which it works as a cluster head. Tv interprets the battery power consumption as we have assumed that the battery power consumption for the cluster head is more than that of the general node which is calculated in random.
6) Calculate a combined weight for each node v.
   $Iv = C_1.Dv + C_2.Pv + C_3.Mv + C_4.Tv$
   The coefficients C_1, C_2, C_3, C_4 are representing the factor for weighing which corresponds to system parameters.
7) Select the node which is having lowest value for Iv as a head for the cluster. The remaining neighbours of already opted cluster head will no longer take part in the election algorithm.
8) Repeat Steps from step 2 to step 7 for the remained nodes from the cluster. Fig. 2 shows the cluster formation depends on the weighted clustering algorithm in which node 6 has been elected as the cluster head.

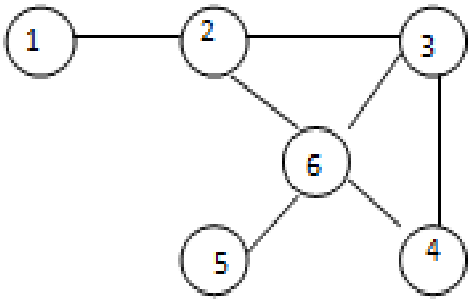

Fig.2 Cluster Head Election

B. Detection and Analyzer

Detection and Analyzer has 3 rules as follows:

1) Interval rule: Considering a pre-defined time frame, a failure is observed if the time passed between the receptions of two consecutive messages is larger or smaller than the allowed limits. Integrity rule: Any attack on modification of the transmitted packet within the transmission channel is subject to anomaly and will be detected based on this rule. A propagation failure due to the jammers interference in the network constitutes example of such rule and will be used as part of our detection process.

2) Transmission/retransmission rule: Monitoring by the monitor node pertaining to number of messages intended for any of its neighbours falls be- low expectancy as the nodes fails to forward the message to the next hop.
3) Delay rule: The transmission of a message by a monitor's neighbour must occur before a defined time out otherwise an attack will be detected.

V. PERFORMANCE EVALUATION AND RESULTS

In Fig. 3 we have shown Comparison for Packet Delivery Ratio between ILCRP and ILCRP-IDS. Packet Delivery ratio noted as the ratio of overall packets has reached the destination node to the overall packets originated from source node. Packet Delivery Ratio when number of clusters are increasing and the number of nodes remains unchanged with the value = 200.We can observe Fig. 3 with increasing number of clusters; packet delivery ratio improves in %.

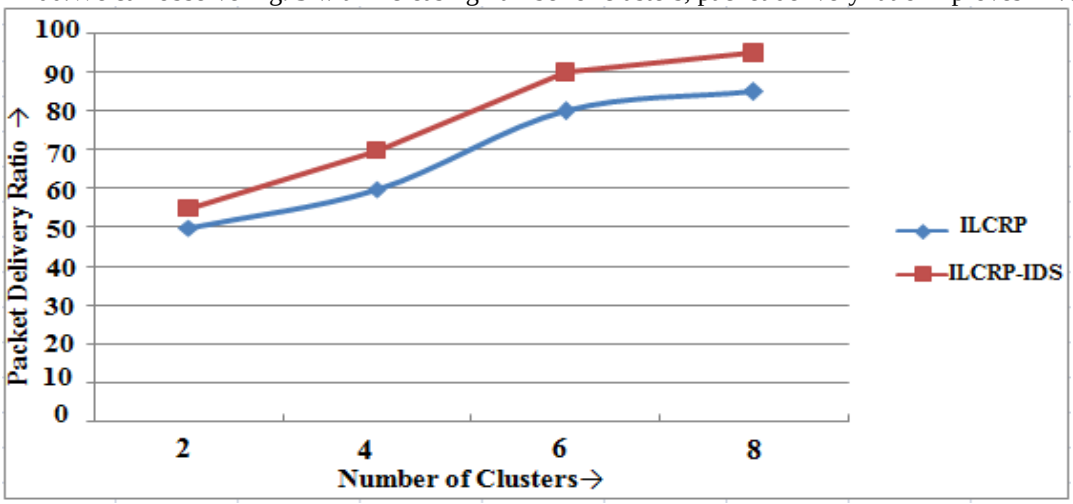

Fig. 3: Comparison for Packet Delivery Ratio and Number of clusters

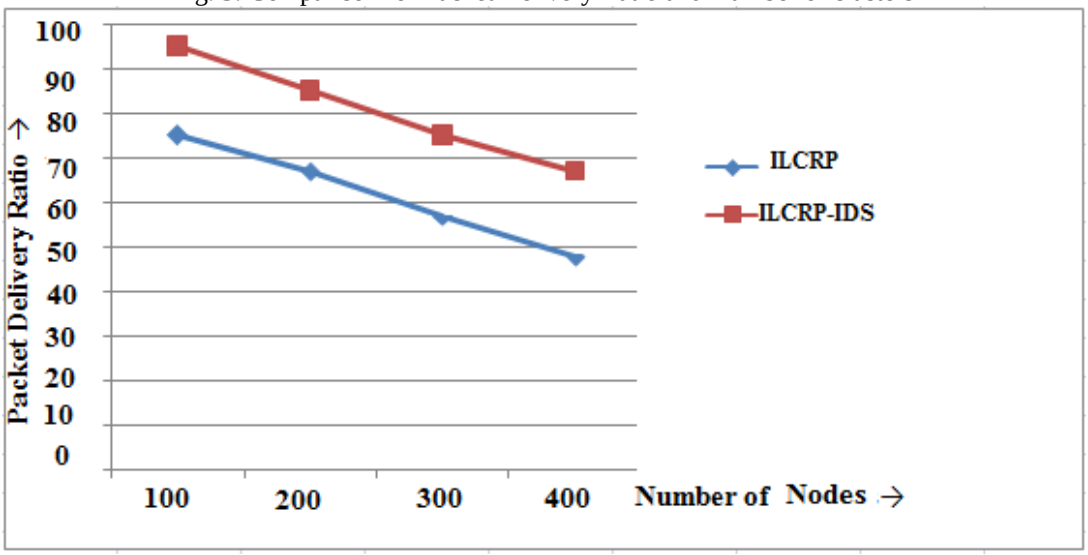

Fig. 4: Comparison for Packet Delivery Ratio and Number of Nodes

We can observe Fig. 4 with increasing number of nodes the % of ratio decreases, so there is need of cluster maintenance.

VI. CONCLUSIONS

In this paper, we presented our efforts to develop an IDS model for Improved Location Aided Cluster Based Routing Protocol. This proposal is centred on a malicious behaviour detection model for ILCRP. ILCRP-IDS have capability of preventing active and passive attacks. It performs better security due to the presence of IDS. Packet drops due to malicious nodes are reduced by IDS which results in higher ratio compared to ILCRP. In terms of performance, an intrusion detection system with ILCRP becomes more accurate as it detects more attacks and cluster head raises alarms. By considering all the aspects, ILCRP is better and secure.

ACKNOWLEDGMENT

I would like to acknowledge all the people who have been help and assisted me throughout my research work. I would like to thank my lovely parents and my friends for time to time support and encouragement and valuable suggestions at every stage of this research. The acknowledgement would be incomplete without mention of the blessing of the almighty, which helped me in keeping high moral during most difficult period.

REFERENCES

[1] SenthilVelmurugan Mangai and Angamuthu Tamilarasi, "A new approach to geographic routing for location aided cluster based MANETs", EURASIP Journal on Wireless Communications and Networking, 2011.
[2] Heng Wai, Yin Nwe Aye, Ng Hian James, "Intrusion Detection in Wireless Ad-Hoc Networks", 2009.
[3] Miss Laiha Mat Kiah,Liana Khamis Qabajeh, Mohammad Moustafa Qabajeh, "Unicast Position-based Routing Protocols for Mobile ad hoc networks", Vol. 7, No.5, 2010.
[4] Young-Bae Ko and Nitin H. Vaidya, "Location- Aided Routing (LAR) in Mobile Ad Hoc Networks," ACM/Baltzer WINET J./vol 6,no. 4,pp.307-21,2000.
[5] Neelesh Gupta, Roopam Gupta, "Estimated New Routing Scheme in MANETs," International Journal of Computer Applications (0975 – 8887), Volume 17– No.5, March 2011.
[6] Hossein Ashtiani, Shahpour Alirezaee, seyed mohsen mir hosseini, and HamidKhosravi , "PNR: New Position based Routing Algorithm for Mobile Ad Hoc Networks", WCE 2009, July 1 - 3, 2009, London, U.K.
[7] Dipankar Deb, Srijita Barman Roy, and Nabendu Chaki, "LACBER- A new location aided routing protocol for GPS scarce MANET", International journal of wireless and mobile Network (IJWMN), vol. 1, august 2009.
[8] SenthilVelmurugan Mangai and Angamuthu Tamilarasi," Evaluation of the Performance Metrics in Improved Location Aided Cluster based Routing Protocol for GPS Enabled MANETs", European Journal of Scientific Research, ISSN 1450-216X Vol.46 No.2, pp.296-308,2010.
[9] Martin Mauve and Jörg Widmer, Hannes Hartenstein," Survey on Position-Based Routing in Mobile Ad Hoc Networks", IEEE Network, November/December 2001.
[10] Liana Khamis Qabajeh, Dr. Miss Laiha Mat Kiah, Mohammad Moustafa Qabajeh, "A Qualitative Comparison of Position-Based Routing Protocols for Ad Hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.
[11] Tiranuch Anantvalee and Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, pp. 170-196, Springer 2006.
[12] Foong Heng Wai, Yin Nwe Aye, Ng Hian James, "Intrusion Detection in Wireless Ad-Hoc Networks", 2009.

