International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

Enhancement of Node Authentication and Security in Mobile ADHOC Network

[1] Manohar B N, [2] Suchitra V
[1] Department of Digital Communication Engineering
[2] Department of Telecommunication Engineering
Siddaganga Institute of Technology (SIT) Tumkuru, India
[1] Manoharbn73 @gmail.com, [2] suchi8689@gmail.com

***Abstract*- The wireless networks play major rule in networking field. Routing and mobility are the major problems in mobile ADHOC networks. These problems can be avoided using clustering based authentication of approaches. In these paper describes The implementations of secured node verification scheme that authenticates the true nodes to access network and detects attacker nodes and Q–LEACH based clustering so that external and internal attacks also avoided. Every node in the network can act like self originating nodes to their neighbors. So every node is builds its own IP address. The wireless networks is used in military application. The mobile adhoc network vulnerable nature not secures. Assign the authentication key for every node to achieve the energy saving of the battery. Therefore it is necessary to adapted Intrusion Detection System mechanism to prevent and detected the Network from attackers. In the other hand Enhanced Adaptive Acknowledgement is proposed as an IDS. In this paper a both IP-trace back with End-to-End Adaptive Acknowledgment getting acknowledgments or information in both ends.**

Index Terms-. ADHOC Networks; Intrusion Detection System; clustering; malicious node; Authentication node

I. INTRODUCTION

A wireless mobile ad hoc network is a collection of mobile hosts which communicate with each other through wireless links directly on other nodes as routes.

The data packet is sending and receiving by the nodes and execute by either individually or collectively depending upon application and area of network. Wireless network is highly dynamic topologies with multi hop and no fixed infrastructure, very rapid movement of the nodes.
The above are the reasons for security critical tasks for mobile wireless networks.

In this paper end to end adaptive acknowledgment and IP- trace back mechanism to prevent and protect against the malicious attacker. Finding out malicious node location is the critical task in the network.End to end adaptive acknowledgment getting the information at both the ends. Traditional security mechanisms are not well suited for mobile adhoc network because they are centralized manner , static and they also require huge memory and high computational power and its may leads to processing overhead and bandwidth consumption is high. So in overcome the regarding issues, then propose trust in this context to ensure the authentication by the way security can be achieved and selfish nodes can be isolated from the network with less memory and high computational capabilities because our proposed algorithm does not involve complexity. In other hand, by making use of faith that means trust, clusters can be formed. Hence scalability major problem that can be solved using clustering also verify Mobile Ad Hoc Network for project over traditional network and its significance.

II. SYSTEM MODEL AND ANALYSIS

A. Related Work

Mobile adhoc network security has in recent years been the subject of various number of proposals.
In [1], propose a micro-payment scheme for multi-hop cellular networks that hope to cooperation in packet forwarding by letting users benefit from depending on others packets. At the same time as proposing mechanisms for detecting and gratifying collaboration, we introduce appropriate mechanisms for detecting and punishing various forms of Misuse and attackers. Then show that the resulting scheme – which is exceptionally lightweight makes cooperation rational and cheating undesirable. Acknowledgments to destination then destination notify the source about reception of data packets.

In [2] , propose a new routing service named best-effort fault-tolerant routing (BFTR). The design goal of BFTR is to provide packet routing service and achieve the high packet delivery ratio and low overhead in presence of malicious nodes. Judging whether a path is good or not, i.e., whether it contains any misbehaving node or selfish node, BFTR analysis the routing feasibility of a path by its end-to-end performance (e.g. packet delivery ratio and end to end

delay). By continuously observing the routing performance, BFTR dynamically routes packets through the almost all feasible path. BFTR provides an efficient and uniform solution for a large range of misbehavior nodes with some security presumption. The BFTR algorithm is evaluated via both analysis and simulations results. The results show that BFTR (best-effort fault-tolerant routing) enhance the ad hoc routing performance in the existence of misbehaving nodes in the network.

In [3] paper describes the routing misbehavior in MANETs (Mobile Ad Hoc Networks). There routing protocols for MANETs are designed based on the assumption that all nodes are completely Cooperative each other. However, due to the open medium and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that few selfish nodes will participate in the route discovery and route maintenance mechanism but refuse to forward data packets.

In paper [4] The causing attack against Wireless mobile Networks is Node Replication attack, where clone attack due to identity theft or attacker. The Node replication attack can be extremely causing to many important functions such as routing, resource allocation, misbehavior detection, This investigation proposes a method called Randomized and Trust based witness finding scheme for replication attack detection mechanisms in wireless sensor networks (RTRADP) with faith that means trust factor. Resilient to malicious witness and increased detection rate by avoiding malicious attacker selection process. Performances are compared with the existing approaches and how the malicious attacker drops the claim without processing and how those malicious attackers are avoided.
Paper [5] Low-Energy Adaptive Clustering Hierarchy is a clustering-based routing protocol that now a days has attracted a more of attention in literature survey. However, this protocol is not prefect and has some deficit that other extensions of LEACH try to solve the many problems. Security is one of the major problems of LEACH and several security attacks can be launched against LEACH protocol. The need for security in LEACH protocol has inspired many researchers and scholars to design secure versions of this protocol and to avoid the internal and external attackers. In this paper, also discuss the current state-of-the- art secure LEACH approaches that are proposed in literature survey. This paper also describes the security features and highlights their objectives, advantages and disadvantages. In addition to classify secure the LEACH schemes into cryptographic-based and trust-based solutions and reviews the major development in these two categories. Then present a qualitative comparison on secure LEACH schemes based on various security issues.
In [6] deals there are a some of routing protocols designed for Wireless Sensor Networks. These routing protocols can be categorized in accordance with the network. But these protocols did not consider the following issues concurrently: mobility of the sensor nodes with base station, security of network layer and Energy. Low Energy Adaptive Clustering Hierarchy and LEACH-Centralize are the routing protocols are hierarchical manner. However the network is divided into clusters and all clusters hold an elected sensor node. On the other hand LEACH and LEACH-Centralize are not fit for large wireless sensor networks which cover whole geographic area because of direct communication between base station and cluster head takes place. They also do not take care of link or any other node failure. A new secure routing protocol is proposed for wireless sensor networks in which sensor nodes and the base station. The protocol attains security through symmetric key cryptography as well as threshold key cryptography are used. An study of the security strengths of the protocol is presented. Simulation results show the throughput of the proposed algorithm and a comparison of LEACH regarding its throughput.

Most recent year ad hoc network research has concentrated on providing routing services not in view of security issues with security injury against ad hoc routing protocols, especifically examining AODV and DSR protocols. In these threats and identify three different environments with distinct security requirements. Then propose a solution to one, the managed-open scenario where infrastructure fewer networks is pre-deployed, but a small amount of important security coordination is expected.

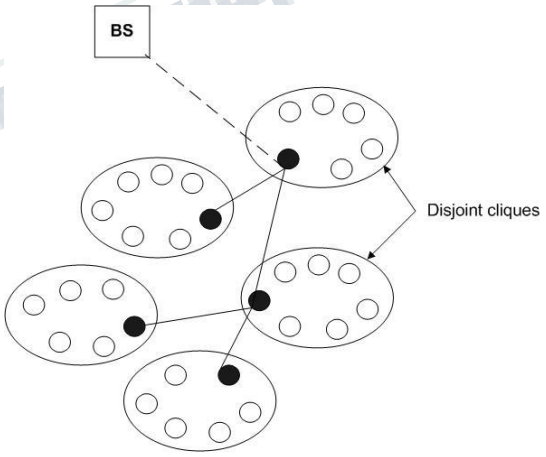

Fig1- Clustering based Mobile Adhoc network

C. Proposed Approach

Consider network area assumed several numbers of the nodes within the network and next clustering the
nodes clustering means is a grouping of the set of nodes in the network. The nodes clustering based on the category wise and take the random location[x, y] within region.

Assign the key or id number for each node. The proposed approach clustering the nodes in other hand each cluster can select the one node each category all the nodes in the network.

If any node in particular area of network communicate with other area of the node then matches the key pair otherwise its treated as malicious node and in real time system IP address blocked and malicious cannot access into particular web. The clustered node send the some message to the base station the key pair is valid then cluster node communicate with base station using the CH. CH analysis and gather the data to BS. The CH election process is applied to the overall network in the limited time. The above reasons energy saved and nodes are secure.

III. FLOW CHART

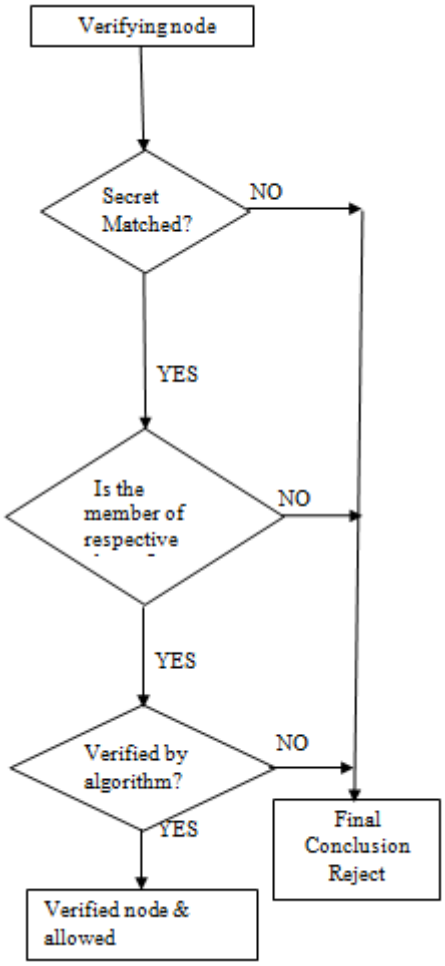

Fig -2 Flowchart for authentication scheme

In flowchart shows that verification of nodes in the network. In cluster-based mobile adhoc networks, nodes are logically divided into clusters and each cluster communicates with a based station via a interface node, called gateway node. Secret key assign to every node in the network. If secret key matches then communication between one node to other node in different cluster. If secret key does not matches to other area of the node and its treated as malicious node. the next stage is to verifies the node is member of respective cluster or not. if node member of respective cluster then move to next stage. Node is verified using algorithm. The verified nodes allowed access particular web. Then communication between the nodes takes place. The sink node establishes the communication patterns for data forwarding to the neighboring sensor nodes inside the clusters through the cluster heads . The cluster head node forwards the data from the neighbor nodes to gateway node. The Gateway node further forwards the data towards the Base Station. Fig 3 Show the flow chat for the data propagation for various nodes. If the Cluster Head does not receive packets from a node n during the expected time slot for two consecutive times then h informs the gateway node. It has the id of the missing node, time slots during which packets are not received and location of the cluster head.

III. SIMULATION SETTINGS

In this paper AODV protocol used .particular area is 500 x 500 MAC/802.11used and mobility taken random. In table shows parameter and taken values is given below

parameter	Value
X,Y	500,500
Routing protocol	AODV
PROB	Radio propagation
NN	25
MAC	MAC/802.11
Energy Model	Energy-Model-true
Mobility	Random
Moving speed	2 m/s
Traffic	CBR
Bandwidth link	2 Mbps
Propagation path loss model	Two ray ground Model

Table-I: Simulation parameter

There are 5 clusters belonging to every group containing the 10 nodes and every node to be part of one state, about 10 state available in network. Simulation tool used is NS-2.34(Networksimulator2),packagesnam-1.14,xgraph-12.1,programming language oTcl &TCL In this Section the simulation results of proposed system is compared with the existing system. In this paper, we make simulation using ns2 in the Linux (Ubuntu) environment. Nodes are randomly scattered around the network area. Two ray ground propagation model is used. The antenna used is Omni-directional antenna. The values of energy, throughput are extracted from the trace files. Traffic pattern consists of several CBR (Constant bit rate)/UDP (User defined protocol) connections between randomly chosen source-destination pairs. The performance metrics taken for evaluation is as follows. Average energy consumption is the average of the total energy expenditure in the network system over a period of time. Throughput is a ratio between the actual numbers of packet transmitted by the nodes in the system to the numbers of successfully delivered packets at the sink. Average end-to-end delay of data packets is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. Packet delivery ratio is the number of data packet delivered to multicast receivers over the number of data packets supposed to be delivered to multicast receivers.

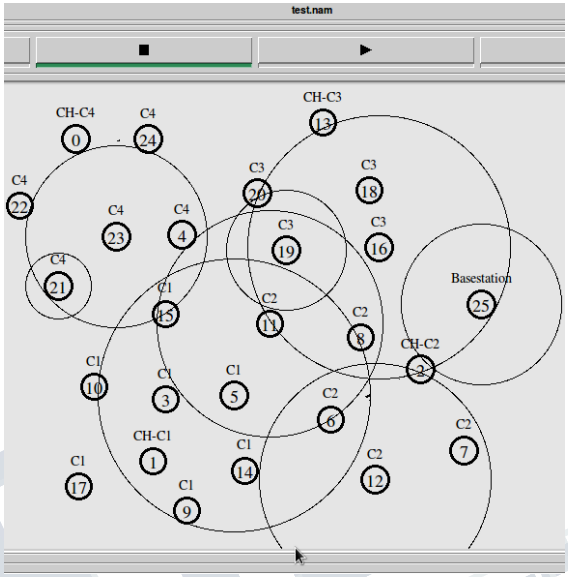

Fig-3 simulation setup

Q-LEACH implementation is based on the clustering and Deployment of nodes and base station.BS awaiting for RSSI then finally cluster formation takes place. Nodes 1,29,17,14,10,3,5 belonging to cluster1.Nodes 8,2,7,6,12,11belonging to cluster2.Nodes 21, 22, 23, 24, 0, 4 belonging to cluster3.Nodes 19, 16, 8, 13, 20 belonging to cluster4.then node24 sensing the data. Data transmission from node 24 to cluster head node 0.cluster head node 13sending data to base station via node 16.BS is discarding the redundant data. The energy level indication at node 13and energy depletion at the node 16 .Rerouting taking place via node19 and 8 to BS

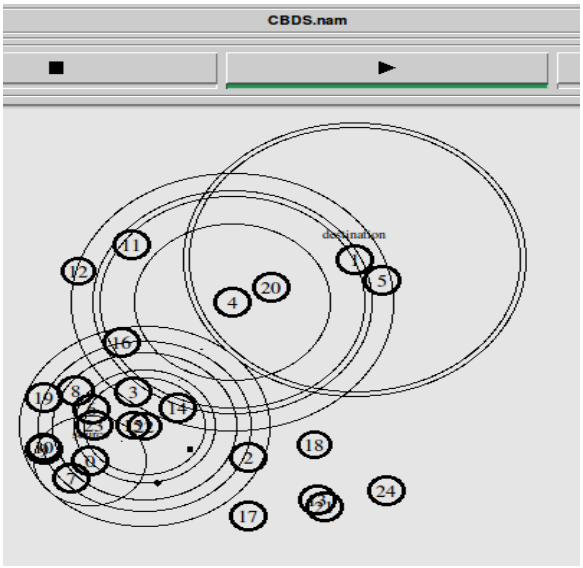

Fig-4simulation setup

A. Results & Discussion

The malicious node can be easily detected by the graph. By implementing the proposed approach in TCL with several numbers of nodes deployed in the network like 25, 50, 75 and 100 nodes. According to the nodes and simulation round the result is generated and given in graph form for analyzing the performance. While simulation the important factors of the network like end to end delay, malicious node packet delivery ratio and if threshold decreases then malicious activity takes place otherwise there is no malicious activity takes place. The following Figure-5 shows the number of malicious node detected in a given period of time by the proposed Approach as well as the existing approach.

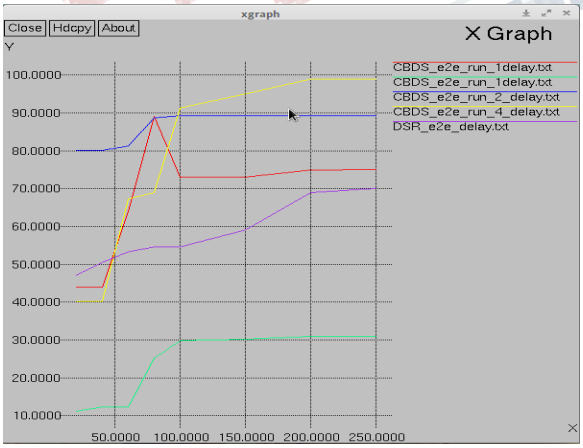

Fig-5 End to end delay obtained by proposed system vs. existing system.

The malicious activity takes place then thresholds suddenly decreses.In the same manner end to end delay decreases then malicious node activity takes place. The proposed approach retains the 69.03, 91.29, 95.090, 99.045, 99.0345.In all four rounds with 00,150,200,250nodes respectively where existing system retains some values 54.546, 54.54, 59.09, 69.0, 70.1 of the delay. Fig 5, 6and 7shows total dropped packets, packet delivery ratio and average end-to-end delay.

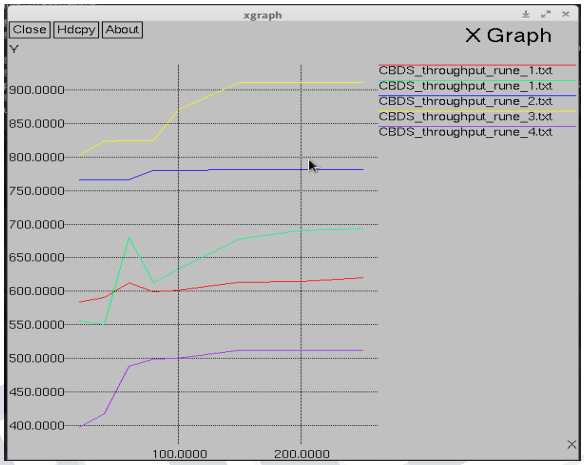

Fig-6Throughput obtained by proposed system vs existing system.

The throughput compare with CBDS(cooperative bait detection scheme) and DSR take the some values. The proposed approach transmitted 870,911.3 in rounds of 100,200.the existing system transmitted 500,512 packets. The thresholds suddenly decrease then malicious activity takes place. Fig 6 shows the graphical representation of Throughput with respect to number of nodes. Throughput is increasing when the network size is increased.

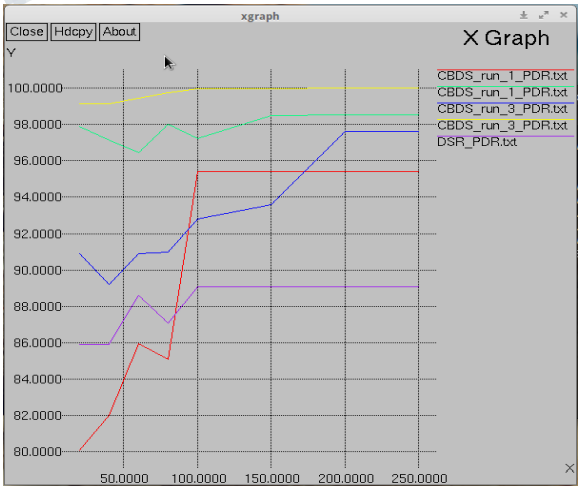

Fig-7 packet delivery ratio obtained by proposed system vs existing system

The packet delivery ratio increases then there is no malicious activity takes place. the proposed system

transmitted 99.7210,99.9465,99.9465,100,100packets in all rounds with 50,100,150,200,250 nodes respectively. In existing system transmitted87.0901,89.07,89.07,89.07,89.07.Takesomethres holds compare the CBDS and DSR to measure the packet delivery ratio. The dropped packet is less in proposed system and the packet delivery ratio is also high for proposed system

V. CONCLUSION

In the proposed approaches more efficient compared to the existing approaches in terms of packet delivery ratio, end to end delay, throughput and security for mobile ad hoc networks. Detect and prevent the malicious node in the network. Improve the network performance.

REFERENCES

[1] H. Miranda and L. Rodrigues, .Preventing selfishness in open mobile ad hoc networks,. inProc. of the Seventh CaberNetRadicals Workshop,October 2002.

[2] YUAN XUE and KLARA NAHRSTEDT, "ProvidingFault-Tolerant Adhoc RoutingService in AdversariaIEnvironments", journal=WirelessPersonal communications29,pages=367, year=2004, publisher=Kluwer AcademicPublishers

[3] S. D. Khatawkar, U. L. Kulkarni and K. K. Pandyaji, "Detection of Routing Misbehavior in MANETs", (201 1) IACSrT Press, Singapore

[4] V. Manjula and C. Chellappan," Trust Based Node Replication Attack Detection Protocol For Wireless Sensor Networks", Journal of Computer Science 2012, 8 (1 1), 1 880-1888, rSSN 1 549-3636

[5] Jianguo SHAN, Lei DONG, Xiaozhong LIAO, " Research on Improved LEACH Protocol of Wireless Sensor Networks", PRZEGLf\D ELEKTROTECHNTCZNY, ISSN 0033-2097, R. 89 NR I b/2013.

[6] Jianguo SHAN, Lei DONG, Xiaozhong LIAO, " Research on Improved LEACH Protocol of Wireless Sensor Networks", PRZEGLf\D ELEKTROTECHNTCZNY, ISSN 0033-2097, R. 89 NR I b/2013