A Secure Intrusion Detection on Clustered Heterogeneous MANET

Ashik E[1] Dr. P. Vijayalakshmi[2] M.E., Ph.D.

P.G Scholar[1], Assistant professor[2] ,Department of ECE.,
Hindusthan College of Engg. & Tech.,
Coimbatore, Tamil Nadu, India

***Abstract*—**Mobile Ad hoc NETwork (MANET) have been now seen as the advancement of network models. It involves mobility and hierarchy of network elements on it positive side. The two different parameters of prime importance in MANET are energy efficiency and security. This paper proposes the idea of combining these two factors. It involves a novel idea of dynamic re-clustering to address energy efficiency. Security have been incorporated in data transmission stage by a secure intrusion detection algorithm. Compared to conventional approaches the combination of these two ideas have improved the performance parameters without affecting network performance.

Keywords*—MANET;Security;Energy efficiency; Re-clustering; Clustering Algorithm*

INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception.

In IEEE 802.11 based MANET, it includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments, and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

RELATED WORK

A. Inter node Commnunication in MANET.

Wireless communication has improved the span of communication in every sense. This have seen further advancement with the introduction of MANET . But the problem with the MANET comes when there is packet loss, collision and energy loss. So we have introduced the idea of clustering. Clustering basically defines the process of grouping the nodes based on some parameters. It may be energy, geographical deployment, proximities or may be a random selection. We will be selecting some of the nodes as cluster heads. After that we will be defining some dependent nodes for the cluster heads.

Once we have done that the dependent nodes (General nodes) will be communicating with their respective cluster heads and cluster heads will be communicating with the server. This will reduce the packet loss as it have some sort of definition for the network. Despite of its advantages the major problem that occurs will be , performance of a set of General nodes will solely depend on the state of the cluster head. If there is some kind of misbehavior from any of the cluster head ,it will affect the entire network.

So to address that issue we have introduced the concept of re-clustering. We can take any of the network parameter as a base for network re-clustering. This process will further improve the network attributing to the malicious behavior. After that by including the further stages of intrusion detection will further make network strong to attack. Dynamic rerouting mechanism are also introduced in to make secure packet transfer

B. Clustering and Routing

Even though the idea of clustering is there long ago. Many of them were theoretical proposals, some of them involved additional network nodes , many had a pre defined hierarchical structure and some of them where mathematical analysis. All these had some vast differences between proposed performances and the obtained performance metric, it was very hard to achieve improvement. It had a problem that it never addressed any other issues like packet loss and performance of the cluster head.

We found that energy and distance between the server node can be taken as the most two reliable parameters for the purpose of cluster head selection. Basically with these kind of clustering we found that DSR or Dynamic source routing is the best method. In DSR routing is done at source node itself .This will make the process as we are earlier aware about cluster head and server node.

SECURE HETEROGENEOUS MANET

There are two things defined here .First one is the defining the network model on to which we can implement the research, the second will be the algorithm which is proposed algorithm which implements the re-clustering and securing the network.

C. Network Model

Network elements consists of heterogeneous elements ranging from cellular phone to big servers which rely on same mode of packet transfer .In other sense it must follow same MAC protocol. The version of MAC protocol that have been incorporated here is IEEE 802.11 which includes over the air modulation standard. It generally deals with a set of specification in both MAC and PHY layer for over the air modulation in wireless networks. The latest of which is IEEE 802.11 ac which uses OFDM modulation techniques which is being supported in almost all bands

D. Algorithm

The proposed algorithm deals with step by step implementation ranging from study of network topology to re-clustering.

- Step 1 : Initial topology discovery of the network elements and noting down its geographical deployment energy level and distance factor between them.
- Step 2 : Selecting (N) cluster head based on the energy and distance between the server node and general nodes.
- Step 3 : Sending a advertisement message from cluster head to dependent nodes.
- Step 4 : Sending discovery packets to make sure all nodes have been classified under some cluster head.
- Step 5:Packet transmission phase starts .initially the dependant nodes to respective cluster heads after that cluster heads to server nodes.
- Step 6 : Securing network with detecting malicious behavior.
- Step 7: If time reaches a particular value (T1) Cluster head re election occurs based on the distance and energy parameters.
- Step 8 : Steps 2 to Step 7 are repeated for infinite number of times.

ANALYSIS

E. Network analysis

1) Topology Discovery: It basically deals with identifying the initial geographical co-ordinates of the network node element. The density,inter node distance etc are the factors that require prime importance while deciding the number of cluster heads.

Basically we will be dividing a region based on the factor density of node in a particular area. We will be defining a square geographical area of L meter length and B meter breadth. We will be also consider a factor of limiting N1 number of nodes in each clusters.

*2) Cluster head re-election:*Once residual energy is considered we will be going for the distance between the cluster heads as the second factor of distance between the cluster heads and the server node ie Base station.

3) Securing the network: Securing the networks are basically implemented at data transmission stages. It have the phase of detecting malicious node by detecting some parameter by packet drop counter. Once we have done that there requires a re-routing of packet once in a while to avoid the malicious node from in between.When we implement these two things, we can assure that network will be secure.

F. Data transmission analysis

We can take any of the available performance metric for data transmission analysis. We will consider the below mentioned parameters.

1) Packet size: Packets are the fixed-size chunks of data that transfer requests and results between clients and servers. The default packet size set by SQL Server is 4,096 bytes. If an application does bulk copy operations, or sends or receives large amounts of text or image data, a packet size larger than the default may improve efficiency because it results in fewer network read and write operations. If an application sends and receives small amounts of information, the packet size can be set to 512 bytes, which is sufficient for most data transfers.
We will doing comparative study of 128 bytes ,256 and 512 bytes of data.

2) Packet Delivery Ratio:Packet delivery ratio is the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

This is the most important one because this defines about the loss of data packets. Secure a reliable data transmission has a factor of PDR as its performance metric. We will be taking no of packets dropped to get the instance at

which such a loss has occurred by monitoring in order to address the issue at a particular instant.

3) Residual Energy: This can be defined as the remaining energy generally attributed to remaining battery power. This is a factor of work load of each node.This have direct dependency towards work done. Considering the case when a cluster nodes have huge number of packet transfer, the respective cluster head will drain.This can in turn lead to loss of data packets which has been routed through the cluster head. This makes it an important factor to monitor energy at regular intervels.

EVALUATION

G. Simulation Environment.

Simulation environment is as shown in Table I. Basically we will be using NS-2 as simulation software as it have 80 % similarity when it is implemented in real time.NS2 is an open source software which can support the conditions attributed in the given project.

H. Simulation Configuration

We will be doing a simulation for about 45 seconds for the data packet sizes of 128bytes,256 bytes and 512 bytes. We will be doing performance metric analysis of all these things. Each of the parameters have been plotted separately as shown in the adjacent figures. The performance parameter are denoted below as the figure names. A study on this figures will be the inference from the simulation

TABLE I SIMULATION ENVIRONMENT

SIMULATION PARAMETER	VALUE
Channel type	Channel/Wireless channel
Radio propagation model	Propagation/Two ray ground
Network interface type	Phy/Wireless phy
MAC Type	MAC 802_11
Interface Queue Type	CMUPriqueue
Link Layer Type	LL
Antenna Model	Antenna/Omni Antenna
Maximum Packet in Queue	300
Routing Protocol	DSR
X-Co-ordinate	450
Y-Co-ordinate	450
Number of Nodes	37
Number of Source nodes	30
No of Destination node	1
Initial Energy	100

Fig. 1. Packet Drop for 128 bytes.

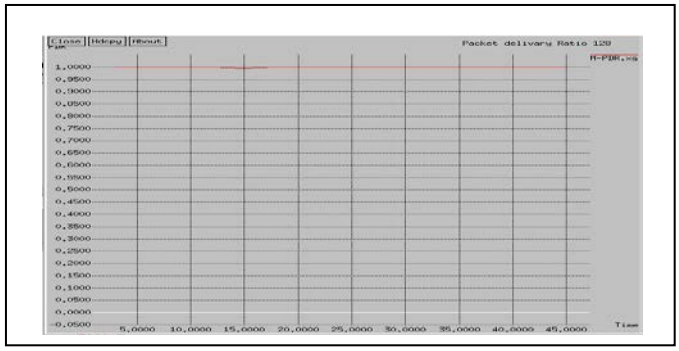


Fig. 2. Packet Delivery Ratio for 128 bytes.

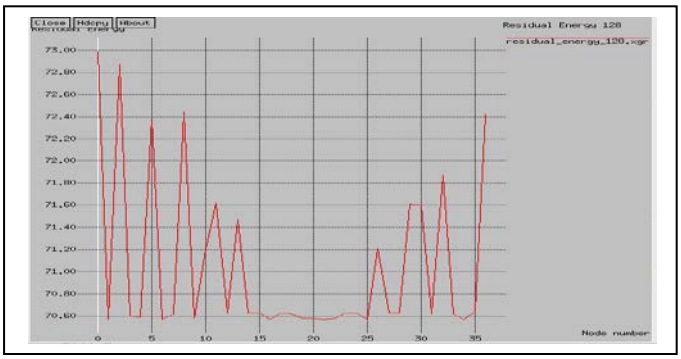


Fig. 3. Residual Energy for 128 bytes.

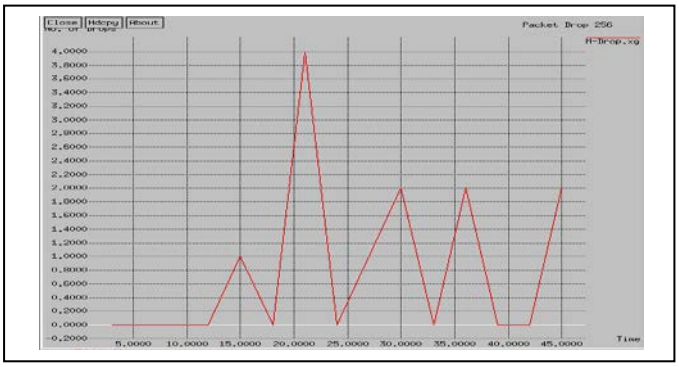
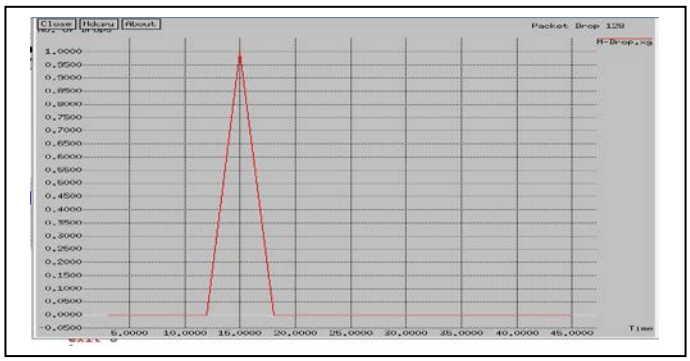
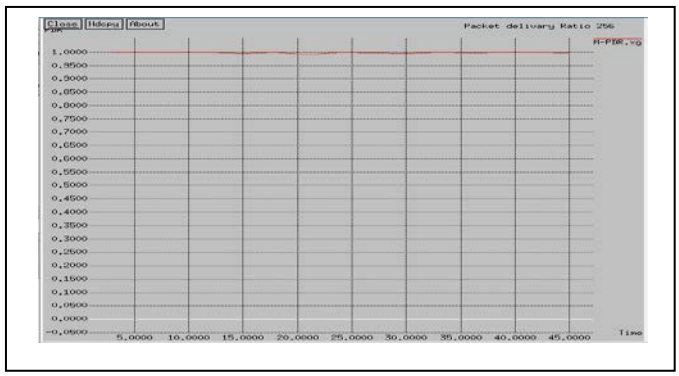


Fig. 4. Packets Drop for 256 bytes.





\\\

Fig. 5. Packet Delivery Ratio for 256 bytes.

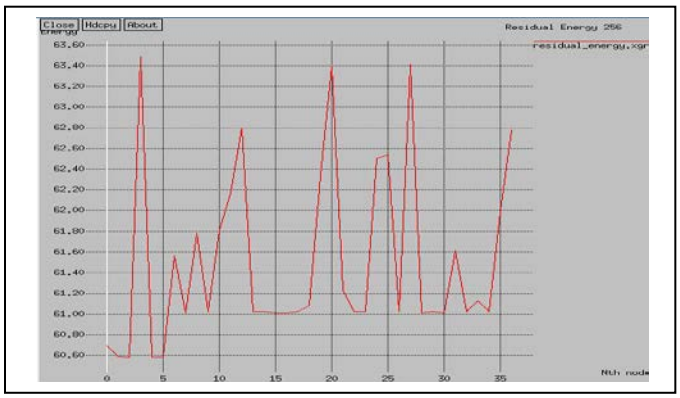


Fig. 6. Residual Energy for 256 bytes.

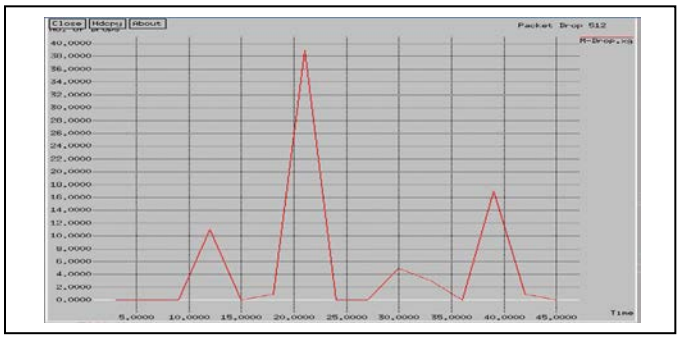
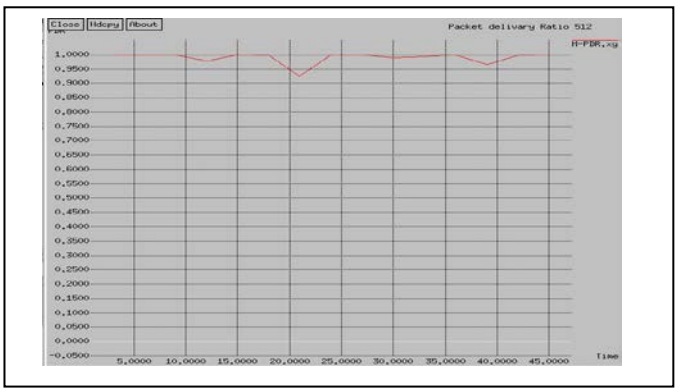


Fig. 7. Packets Drop for 512 bytes.



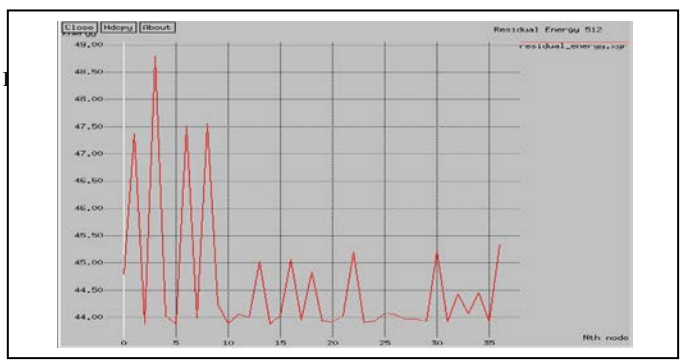


Fig. 9. Residual Energy for 512 bytes.

CONCLUSION AND FUTURE WORKS

As a future work we can aim at securing the network again with some hybrid cryptographic techniques and doing study on some evident attacks.

We have concluded that after the implementation of the algorithm there has been a uniformity in the energy drop which is evident from rsidual energy plot. PDR and Packets dropped has been decreased as the packet sizes increases from 128 bytes to 512 bytes.

REFERENCES

[1] Boukerche. A. “Algorithms and Protocols for Wireless. Mobile Ad Hoc Networks”. Hoboken. NJ: Wiley. Nov. 10. 2008

[2] Boukerche. A. “Performance evaluation of routing protocols for ad hoc wireless networks.” Mobile Netw. Appl. vol. 9. no. 4. pp. 333-342. Aug. 2004.

[3] Du X.Wu D. Liu W. and Fang Y. “Multiclass routing and medium access control for heterogeneous mobile ad hoc networks.” IEEE Trans.Veh. Technol. vol. 55. no. 1. pp. 270–277. Jan. 2006.

[4] Ghaderi J. Xie L. and Shen X. “Hierarchical cooperation in ad hoc networks: Optimal clustering and achievable throughput.” IEEE Trans.Inf. Theory. vol. 55. no. 8. pp. 3425–3436. Aug. 2009.

[5] Liu . C. Zhang. W. Yao G. and Fang Y. “ Delar: A device–energy–load aware relaying framework for heterogeneous mobile adhoc networks ” IEEE J. Sel. Areas Commun. vol. 29. no. 8. pp. 1572–1584. Sep. 2011.

[6] Priyanka Patil. Rizvi M.A. “Issues and Challenges in Energy Aware algorithms using clusters in MANET” IJCCN. Volume 2. No.2. April - June 2013.

[7] Shah V. Gelal. E. and Krishnamurthy P. “Handling asymmetry in powerheterogeneous ad hoc networks.” J. Comput. Netw.—Int. J. Comput.Telecommun.Netw. vol. 51. no. 10. pp. 2594–2615. Jul. 2007.

[8] Villasenor-Gonzalez L. Ge Y. and Lament L. “HOLSR: A hierarchical proactive routing mechanism for mobile ad hoc networks.” EE Commun.Mag. vol. 43. no. 7. pp. 118–125. Jul. 2005.

[9] Wu. J and Dai. F. “Virtual backbone construction in MANETs using adjustable transmission ranges.” IEEE Trans. Mobile Comput. vol.5. no. 9. pp. 1188–1200. Sep. 2006.