

# An Energy Efficient Intrusion Detection System in MANET.

Namrata<sup>1</sup>, Dr.Sukhvir Singh<sup>2</sup>

1. M.Tech, Department of C.S.E, N.C College Of Engineering, Israna , Panipat.

2. Associate Professor Department of C.S.E, N.C College Of Engineering, Israna , Panipat.

## Abstract

Mobile Ad-hoc Networks (MANETs) are wireless networks consisting entirely of mobile nodes (without base stations) that communicate with each other. In Ad-hoc networks, since there is no fixed infrastructure, therefore there are no separate network elements called routers and hence the mobile nodes themselves act as the routers. Recent advances in MANETs have led to many new protocols specifically designed for ad-hoc networks where energy awareness and security are major consideration. To increase the network lifetime, we propose an energy efficient routing protocol and in order to secure the network, we propose zone intrusion detection system for MANETs for randomly deployed mobile nodes. To achieve the better results, a maximum lifetime data aggregation algorithm which finds data gathering schedule provided location of nodes and base-station, data packet size, and energy of each node. An energy efficient and secure pattern based data aggregation protocol which is designed for clustered environment. In this protocol multi hop communication is used within cluster and cluster head to base station. MATLAB is used for simulation.

**Keywords:** MANET, Intrusion Detection System, Routing Protocols, Energy Efficiency, Data Aggregation, MATLAB.

## 1. Introduction

The entire life-cycle of MANETs can be classified as: First Generation, Second Generation, and Third Generation. The first generation MANETs were known as Packet Radio Networks (PRNET), developed during 1970's (1972). PRNET used a kind of distance-vector routing, which was a combination of Aerial Locations of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) approaches. The Defense Advanced Research Project Agency (DARPA) initiated research on packet-switched radio communication networks to provide reliable communication between computers and PRNET. DARPA was established in 1958 for establishing the technological superiority of the U.S military.

In 1980's, the second generation of MANETs came into existence by further improvement in ad-hoc networks and were implemented as a part of the Survivable Adaptive Radio Networks (SURAN) which proved to be beneficial in the improvement of the radios performance by reducing their size and making them cheaper. During those days, the suggestion of a collection of mobile nodes was proposed at some research meetings/conferences. The research community had started looking into the prospect of

deploying ad-hoc networks in other areas of applications. After adoption of the term ad-hoc networks by the IEEE 802.11 subcommittee, some of the outcomes of these efforts were Global Mobile Information Systems (GloMo) and the Near-term Digital Radio (NTDR). GloMo provided an office environment, with Ethernet-type multimedia connectivity, with anytime and anywhere capability introduced in handheld devices. NTDR was self-organized, two-tier network and used clustering and link-state routing. A functional group for MANET was created, which worked for routing protocols for MANET and gave rise to the development of various mobile devices like PDA's, laptops, notebooks etc. Some other standards were also developed that provided benefits to the MANET like HIPERLAN and Bluetooth. Present mobile ad-hoc networks are considered as third generation MANET [1].

## 1.1 Intrusion Detection System

An Intrusion Detection System is defined as "A system that dynamically monitors the events taking place on a system and decides whether these events are symptoms of an attack or constitute a legitimate use of the system". The major task of IDS is to monitor networks and systems to detect eventual intrusions in the network, alert users after specific intrusions have been detected and finally, if possible reconfigure the network and mark the root of the problem as malicious. An IDS protects data integrity and manages system availability during an intrusion. This system should be able to detect intrusion by monitoring unusual activities in the system and comparing them to a user's profile and evolving trends. The objective of the modeling is to identify the intrusion while reducing the number of false positives [2].

- a) To perform the statistical analysis on communication parameters to identify the effective communicating node in MANET.
- b) To increase the MANET network lifetime
- c) To achieve the better results, a maximum lifetime data aggregation algorithm
- d) To reduce the node battery life loss.
- e) To implement the work in MATLAB environment.
- f) To compare the results of applying and without applying Intrusion Detection System to WSNs.

### 1.2 Advantages of MANET

- a) Independence from central network administration.
- b) Self-configuring, nodes are also routers.
- c) Self-healing through continuous re-configuration.
- d) Scalable: accommodates the addition of more nodes.
- e) Flexible: similar to being able to access the Internet from many different locations.

### 1.3 Limitations of MANET

- a) Each node must have full performance.
- b) Throughput is affected by system loading.
- c) Reliability requires a sufficient number of available nodes. Sparse networks can have problems.
- d) Large networks can have excessive latency.

In our purposed methodology we have used combination of both technique for long life MANET. There are the best example of preset static infrastructure and planning through a centralized system. The whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The advantages and disadvantages of the cluster-based approaches is very much similar to tree-based approaches. In recent, proposed a maximum lifetime data aggregation algorithm which finds data gathering schedule provided location of sensors and base-station, data packet size, and energy of each sensor. A data gathering schedule specifies how data packet are collected from sensors and transmitted to base station for each round. An energy efficient and secure pattern based data aggregation protocol which is designed for clustered environment. In conventional method data is aggregated at cluster-head and cluster-head eliminate redundancy by As we discussed in previous chapter about Zone-Based Intrusion Detection System and Energy efficient routing algorithm. So in our purposed methodology we have used combination of both techniques for long life MANET. There are the best example of preset static infrastructure and planning through a centralized system. The whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The advantages and disadvantages of the cluster-based approaches is very much similar to tree-based approaches. In recent, proposed a maximum lifetime data aggregation

algorithm which finds data gathering schedule provided location of sensors and base-station, data packet size, and energy of each sensor. A data gathering schedule specifies how data packet are collected from sensors and transmitted to base station for each round. An energy efficient and secure pattern based data aggregation protocol which is designed for clustered environment. In conventional method data is aggregated at cluster-head and cluster-head eliminate redundancy by

## 2. Concept Of Data Aggregation

Data Aggregation is used to make our proposed work more efficient and accurate for selection of next node in Zone-Based Intrusion Detection System. In MANET, moving nodes are mostly resource-constrained. For example in battery power, memory, processing speed etc. Data Aggregation for any process in which information is collected and elaborated in a pattern for various decision making purposes such as statistical analysis. Thus, data aggregation at Zone-Based Intrusion Detection System is used to eliminate redundant data and enhances the synchronization MANET network.

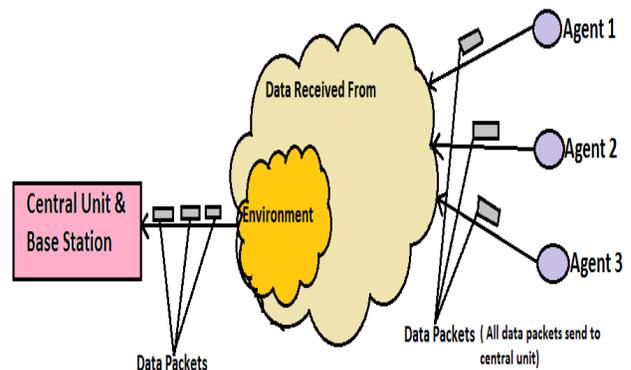


Fig.1 ( Non Aggregation Model)

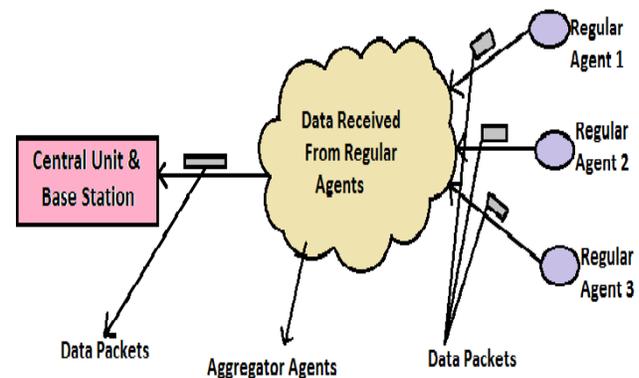


Fig. 2 (Data Aggregation Model)

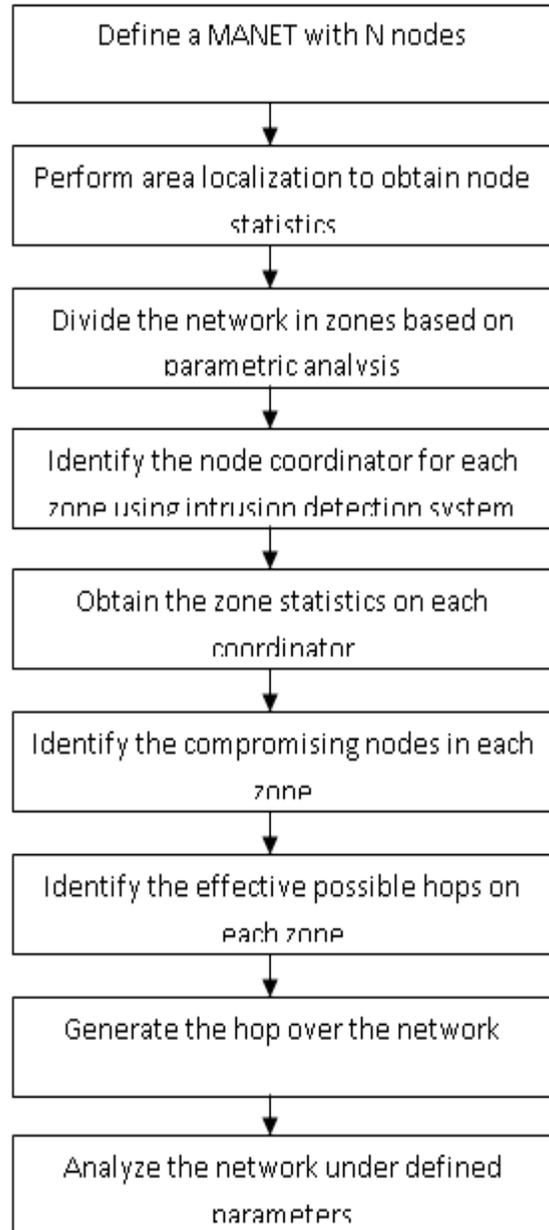
## 2.1 Flow Of Work

The presented work is about to improve the dynamic routing in network by using the concept of Zone based Intrusion Detection node coordinator approach. According to this approach, the node localization will be optimized. The work is here defined to divide the network scenario in smaller zones and identify the node coordinator over the zone. This coordinator will contain the communication statistics of zone nodes. As the routing will be performed, the effective hop selection will be done by the node coordinator.

## 2.2 Steps in purposed algorithm

1. Define the strength limits to identify the reliable coordinator node to optimize the network communication for synchronization.
2. Perform the communication for Fix Number of Communication Rounds.
3. Process all network nodes.
4. Check for Speed Level validity on node.
5. Check for the node coordinator acceptability respective to the area level density over the zone.
6. Identify the critical nodes in the area depends on remaining energy level.
7. Set the node as coordinator node.
8. Define the node as a coordinator to provide the adaptive communication in range.
9. Perform the communication via coordinator node.
10. Check for the critical node depends on remaining energy level.
11. Perform Communication without coordinator node for comparison.
12. Repeat all the steps over each iteration.

### FLOW CHART

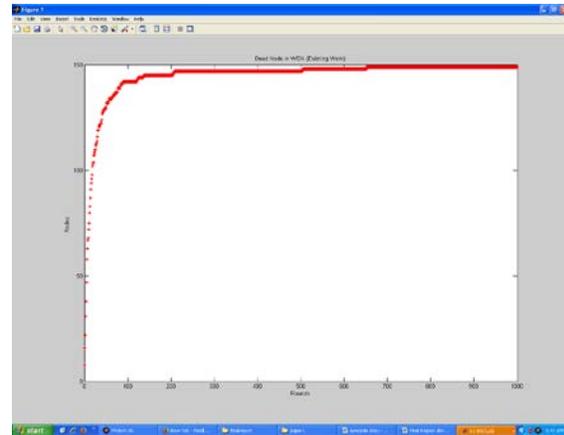


### 2.3 Simulation Scenario

The simulation scenario parameters of presented work are listed here under:-

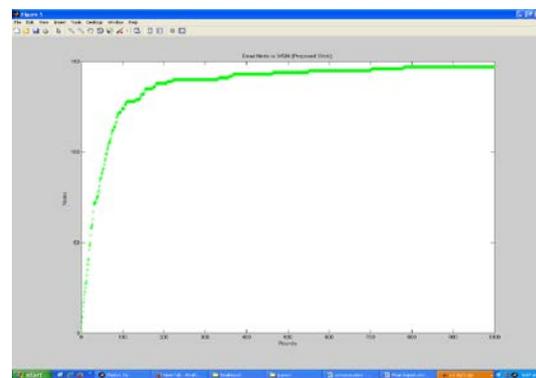
Table.1 Simulation parameters

Parameter	Value
Area	300x300
Number of Nodes	150
Number of Rounds	1000
Initial Energy	Random
Transmission Loss	50 nJ
Receiving Loss	50 nJ
Forwarding Loss	10 nJ
Topology	Random
Packet Drop Ratio	Random
Routing Protocol	MTPR



**Fig.4 Dead Nodes Analysis (Existing Approach)**

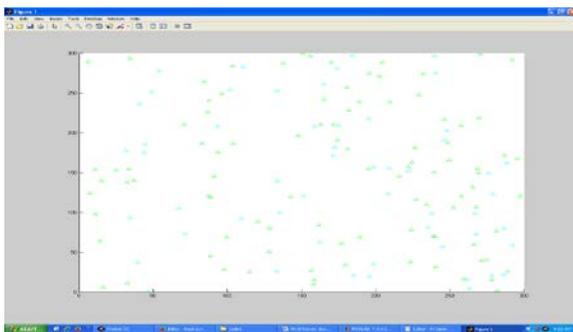
According to existing approach, the zone adaptive communication is performed but the node coordinator is not selected based on the energy criticality.



**Fig.5 Dead Node Analysis (Proposed Approach)**

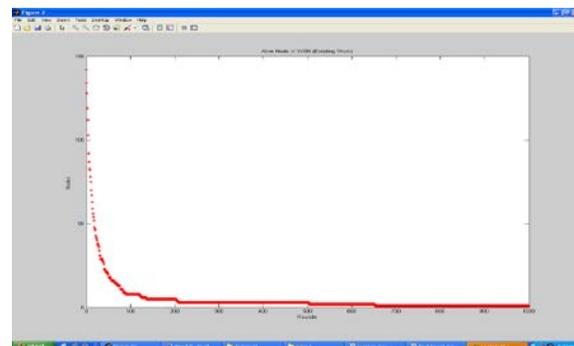
The work is here defined using the next coordinator selection model so that the improved communication is performed.

### 3. Implementation and Result Analysis



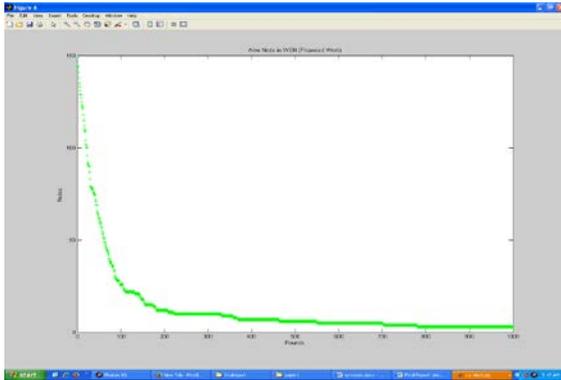
**Fig.3 (Network Architecture)**

The network is here defined in restricted area of 300x300. The network is having 150 nodes with random energy specification.



**Fig.6 Alive Node Analysis (Existing Approach)**

The communication is performed nodes start losing its energy.



**Fig7. Alive Node Analysis (Proposed Approach)**

Here, X axis represents the number of rounds and Y axis shows the number of alive node As we can see, initially all nodes are alive over the network.

#### 4. Conclusions

In our purposed technique, a scenario of network of 150 nodes has been created and some specific simulation parameters have been taken. Using these parameters and MTPR protocol, we analyzed the performance of MANET having random initial energy without applying and with applying intrusion detection system. The proposed algorithm (with energy algorithm) is compare with existing network (without energy algorithm) on the basis of different parameters like dead node analysis, alive node analysis, network communication analysis, and round based communication analysis. After analysis of result, we came to know that even after 1000 rounds still nodes have some energy and communication is being performed among nodes over the network. In the existing network, energy problem occurs, so network is failed. And intrusions are detected using implementation of zone-based intrusion detection system against attacks so that network services can be provided without any interruption in MANETs. So we can say that our network is more effective than previous work.

#### Reference

[1] E. Ahmed, K. Samad, and W. Mahmood, "Cluster-based intrusion detection (cbid) architecture for mobile ad hoc networks," in 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Proceeding, 2006.

[2] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in Wireless Network Security, pp. 159-180, Springer, 2007.

[3] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," Wireless Communications, IEEE, vol. 14, no. 5, pp. 56-63, 2007.

[4] Y. Li and J. Wei, "Guidelines on selecting intrusion detection methods in MANET," in The 21st annual conference for information systems educators (ISECON), Rhode Island, USA, pp.4-7, 2004.

[5] L. Bononi and C. Tacconi, "A wireless intrusion detection system for secure clustering and routing in ad hoc networks," in Information Security, pp. 398– 414, Springer, 2006.

[6] Z. Xing, L. Gruenwald, and K. Phang, "A robust clustering algorithm for mobile ad-hoc networks," Handbook of Research on Next Generation Mobile Networks and Ubiquitous Computing, pp. 187-200, 2008.

[7] L. Bononi and C. Tacconi, "A wireless intrusion detection system for secure clustering and routing in ad hoc networks," in Information Security, pp. 398– 414, Springer, 2006.

#### Namrata

I completed my bachelor's in Computer Science And Engineering from S.D.I.T.M to Kurukshetra University in 2014. Presently pursuing the M.Tech from N.C College of Engineering, Israna, Panipat and working as a Teaching Assistant. My research interest in Networking.

#### Dr. Sukhvir Singh

I completed my PHD in Computer Science And Engineering from M.D University, Rohtak and studied in National Polytechnic University of Armenia in (1996). I have 18 Yrs, experience in teaching. Presently am working in N.C. College of Engineering, Israna Panipat as a Associate Professor in Department Of Computer Science And Engineering.