Identification of the Suspicious Node using Unsupervised learning Technique in MANET

Developed by:

Sakeena Javaid

696-FBAS/MSCS/F12

Supervised by:

Dr. Muhammad Sher

Professor and Dean FBAS, IIUI

&&

Dr. Faraz Ahsan

Assistant Professor, HITEC, Taxila

Department of Computer Science

Faculty of Basic and Applied Sciences

International Islamic University Islamabad 2015

1. Machine learning
2. Computer algorithms

International Islamic University Islamabad

Date: 01-09-2015

Final Approval

This is to certify that we have read the thesis submitted by **Sakeena Javaid, 696-FBAS/MSCS/F12** It is our judgment that this thesis is of sufficient standard to warrant its acceptance by International Islamic University, Islamabad for the degree of **MS in Computer science.**

Committee·

External Examiner

Dr Muazzam A. Khan Khattak
Assistant Professor
CE&ME
National University of Sciences and Technology (NUST)
College of EME Peshawar Road, Rawalpindi

Internal Examiner

Ummara Zahid
14/9/15

Madam Ummara Zahid
Lecturer
Department of Computer Science & Software Engineering,
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad

Supervisor:

Dr Mohammad Sher
Dean, FBAS
Department of Computer Science & Software Engineering,
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad.

Co-Supervisor:

Dr. Faraz Ahsan
Assistant Professor
Department of Computer Science & Software Engineering,
HITEC, Taxila

"DEDICATED TO MY PARENTS,
INSTRUCTORS,
SIBLINGS,
COLLEAGUES,
FRIENDS AND
ALL OTHER MEMBERS,
WHO HELPED ME THROUGHOUT MY RESEARCH"

Sakeena Javaid
696\MSCS\FBAS\F-12

A dissertation Submitted To

Department of Computer Science,

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

As a Partial Fulfillment of the Requirement for the Award of the

Degree of MSCS in Computer Science.

Declaration

We hereby declare that this Thesis ***"Identification of a Suspicious Node using Unsupervised Learning Technique in MANET"*** neither as a whole nor as a part has been copied out from any source It is further declared that I have done this research with the accompanied report entirely on the basis of our personal efforts, under the proficient guidance of our teachers especially our supervisor *Dr Muhammad Sher and Dr Faraz Ahsan and Madam Humaira Ashraf* If any part of the system is proved to be copied out from any source or found to be reproduction of any project from any of the training institute or educational institutions, we shall stand by the consequences

Sakeena Javaid
696-FBAS/MSCS/F12

Acknowledgements

First of all we are obliged to Allah Almighty the Merciful, the Beneficent and the source of all Knowledge, for granting us the courage and knowledge to complete this Project

My deepest acknowledgments to Honorable Dr Muhammad Sher Dr Faraz Ahsan, and Madam Humaira Ashraf for their support and guidance through fulfillment of my thesis

Sakeena Javaid
696-FBAS/MSCS/F12

Project In Brief

Project Title:	Identification of the suspicious Node using Unsupervised Learning Technique in MANET
Undertaken By:	Sakeena Javaid 696\FBAS\MSCS\F-12
Supervisor:	Prof. Dr. Muhammad Sher Professor and Dean, Department of Computer Science & Software Engineering, Faculty of Basic and Applied Sciences, International Islamic University, Islamabad
Co-Supervisor:	Dr. Faraz Ahsan Assistant Professor, Department of Computer Science and Engineering, University of Engineering, Taxila
Start Date:	May-2014
Completion Date:	May-2015
Tools & Technologies	OMNeT++\OMNeT++ 3.3, Visual Studio 2008, MS-Excel 2007 or Above
Documentation Tools	MS-Office 2007 and 2013, MS-Visio
Operating System:	Windows XP Professional, Windows 7
System Used:	Intel(R) Core(TM) i5, 2450 M CPU-2.50 GHz
Installed Memory	Ram-6.00 GB, 64-bit O\S

Abstract

Mobile Adhoc Networks (MANETs) are the wireless networks in which all devices rely on the mutual trust relationships They have dynamic topology and due to this reason they are vulnerable to various attacks such as gray hole, blackhole and wormhole attacks etc There are three routing protocols used namely reactive proactive and hybrid for communication and route establishment procedures This scheme is based on grayhole attack detection and identification for the prevention of attacker nodes in the network The protocol used in this approach is AODV In this research an algorithm has been developed to identify the Grayhole attacker node using context-sensitive Hidden Markov Model This technique also introduces a new dynamic threshold property for the grayhole attacks

This Algorithm has been used for learning and evaluation of grayhole node based on the packet drop rate throughout the environment Simulation of the proposed approach has done in OMNeT++ for its verification and validation

Table of Contents

List of Figures

List Of Tables

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

Wireless Adhoc networks [25] are always preferred due to their spontaneous mobility and scalability This technology has gained too much popularity because of its reduced cost and infrastructureless topology over wired network in last few decades Mobile Adhoc network (MANET) is a collection of mobile nodes including transmitter and receiver communicating with each other by directional links directly or indirectly These networks are becoming very famous in industrial and remote access control now a days It allows data communication between multiple parties and also maintains mobility between them This is the benefit of the wireless MANET Although this type of communication is limited to the range of transmitters and receivers But MANET solves this problem as if two nodes are beyond the range of their communication environment, they can communicate each other by using their intermediate nodes to transfer data among them MANET has been divided in single hop and Multi-hop networks In single-hop network each node communicates to other nodes directly with in same radio range In multi-hop network, each node communicates to other nodes by relying on their intermediate nodes if destination point is out of the radio range of them

1.2 MANET ARCHITECHTURE

MANET [25] is decentralized infrastructure network It does not need any fixed or wired infrastructure All node are free and they can enter or leave the network anytime All nodes have the ability of the self-configuration and self-maintenance without the need of any central infrastructures It is often unreasonable in critical mission applications such as military or emergency recovery By making minimum configurations. MANET can be used in emergency scenarios like natural induced disasters, military conflicts and medical emergency cases where infrastructure is unavailable Considering these applications MANET security is very important as it has dynamic topology and remote distributions so it is vulnerable to different kind of attacks

1.3 VULNERABILITIES IN MANET

In MANET [26], any node can be made vulnerable as it does not verify the user identity before giving the users access rights Manet's weaknesses are given below

1.3.1 DEFICIENCY IN CENTRALIZED ARCHITECHTURE

As MANET [26] has no central monitor, so it is difficult to detect attacks at each node individually Transmission in adhoc network is highly dynamic and for large network it is not very easy to locate suspicious activities

1.3.2 AVAILABILITY OF RESOURCES

The common problem in MANET is the availability of required resources Providing security to all threats requires various methods and architectures [26]

1 3.3 SCALABILITY

Scalability factor varies all the time in MANET [26] due to the mobile nature of the network So there should be proper protection methodologies able to cope with huge networks as well as small segments

1.3.4 CO-OPERATIVENESS

Since routing protocol methodologies always based on the mutual trust based relationships in the network Due to this the malicious nodes [26] becomes part of the network and destroys the normal communication violating the standard protocol features

1.3.5 DYNAMIC TOPOLOGY

Mobile nodes [26] and its routing protocols characteristics can destroy their mutual co-operation relationship between them in the network Declaration of nodes as misbehaving could lead to destroy mutual co-ordination between them This approach of the network can be made secured by applying the distributed and enhanced methodologies

1.4 MANET PROTOCOLS

There are three routing protocols in MANET [27] such as proactive, reactive and hybrid as shown in figure below

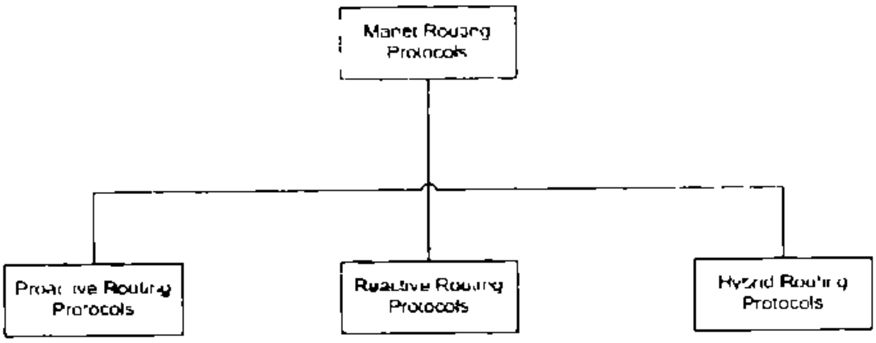

Figure 1.1 Roting Protocols[27]

1.4.1 PROACTIVE ROUTING PROTOCOLS

Proactive Routing Protocols [27] maintain routing tables to store addresses of other nodes in network. They are also known as Table Driven protocols. Due to the dynamic layout of the network, each time when node enters or leaves, changes are made in its routing table at each node. One of the examples is DSDV (Destination Sequenced Distance Vector). This reduces delay and make fast changes if any node enters or leaves the network.

1.4.2 REACTIVE ROUTING PROTOCOLS

These kinds of protocols do not maintain any routing table for establishing paths in network at the start of communication. These are also recognized as On-Demand routing protocols. They (nodes in AODV) discover routes by sending route-request and route-reply messages if some node wishes to communicate to others. Examples are AODV (Adhoc On-Demand Distance Vector) and DSR (Destination Source Routing) [27]

1.4.3 HYBRID ROUTING PROTOCOLS

These are mixture of proactive and reactive protocols. It uses the features of both proactive (table-driven) and reactive (On-demand) routing protocols. Zone Routing Protocol is hybrid and it works as making different segments of the network. It works in a hierarchy where every router in a network has to maintain some more layout configurations. The disadvantage of this is that it requires more space [27]

1.5 SECURITY CHALLENGES AND ISSUES

In MANET, all nodes works in a self-organizing way as performing networking functions like packet forwarding and receiving etc to others in a network So secured MANET is challenged due to these issues which are discussed as below [26]

1.5.1 AVAILABILITY

It means that resources (data and services) are available to all legal users when required even in presence of the denial of service attacks

1.5.2 CONFIDENTIALITY

It focuses on giving authority to use the resources only to network legal users and hide the important information from the unauthorized users in network It is also known as private or protected information handling approach

1.5.3 INTEGRITY

It means that resources can only be changed by the privileged users in an authenticated manner The changes are commonly as status modification, erasure and creation etc by the attackers while reaching the packet to the destination

1.5.4 AUTHENTICATION

This feature enables the authenticity of the node to its neighbor node during communication for proving its identification Basically, it checks that all nodes in transmission are valid and they are not using the false identities

1.5.5 NON-REPUDIATION

This feature enables that no one could deny for the sent or received packets after sending or receiving It can be used to distinguish that node is misbehaving or not.

1.6 MOTIVATION

All previous techniques are dealing with the prevention, detection and elimination of the suspicious nodes in MANET They are also based on supervised and re-enforcement learning techniques [4][8] but still there is a need of a more intelligent technique because they are all suffers from some shortcomings such as learning through unsupervised way. Some techniques are based on dynamic threshold detection where the specified threshold criteria was improperly defined and evaluated. That is why we want to address a new technique in this research that could be able to handle the grayhole attacks more efficiently.

1.7 RESEARCH DOMAIN

In recent era, MANET has been used at very large scale such as in military applications, emergency and disaster relief scenarios. MANET has been working very efficient and it is considered too much effective in these scenarios because it has no centralized administration and every node\working member makes its decisions very actively based on others mutual trust relationship. If a node claims it can reach another node by a certain path or distance, the claim is trusted/true. Similarly, if a node reports a link break, the link will no longer be used. While this assumption can fundamentally facilitate the design and implementation of routing protocols, it meanwhile introduces a vulnerability to several types of denial of service (DoS) attacks particularly packet dropping attack. To launch such attack, a malicious node can stealthily drop some or all data or routing packets passing through it. There are a lot of security attacks as blackhole attacks, wormhole attacks and grayhole attacks which cause malfunctioning in MANET. Detection and Prevention of the Grayhole attacks is an active area of the research in recent years because it attack the MANET's functionality in various ways as by packets dropping or unauthorized identity delegation.

MANET is badly attacked by the gray hole attacks. Gray hole attacks disturb the MANET's functionality by various ways such as illegal resource (battery, power or high computation) consumption or by packet dropping. Many of the devices has failed to forward packets due to high computation or large amount of the power required because attackers has used them illegally. In literature, grayhole attacks are prevented and eliminated by all approaches but they have used typical attach detection approaches or the techniques based on the supervised or reinforcement learning. There are two major problems in the previous techniques.

First is that Supervised learning creates a lot of overhead for the efficient attack detection of the grayhole attack Second is about unstable dynamic threshold specified which contributes to larger false negative rate that actually affects the MANET's functionality

1.7.1 PROPOSED METHODOLOGY

The approach is used for the identification of the grayhole node using unsupervised learning technique in MANET In this approach, Data communication is done by the sending data through intermediate nodes which makes possible the end to end delivery in network transmission with the help of the AODV routing protocol During communication, some of the nodes might be disastrous and want to destroy network resources For this we need some protection mechanism for their detection and identification

1.7.2 RESEARCH CONTRIBUTIONS

This technique has three major contributions as

- An Algorithm is developed using context-sensitive Hidden Markov Models to identify suspicious nodes
- Dynamic threshold is introduced
- Unsupervised Learning is used for the learning approach of the network

Threshold is initialized to twice of the round trip time of the packet and it will be adjusted to the network scenario after first iteration It prevents the suspicious nodes that occur in network and also minimize the network layer attacks

1.7.4 ASSUMPTIONS

We have taken the following assumptions in our proposed technique

- All nodes in the network are assumed to be well behaving except the specific criteria to malicious nodes
- Source and Destination nodes are assumed to non malicious

- The topology used here is static
- Nodes could be out of range due to limited transmission range or batter power
- All channels are supposed to be error free and packet loss rate would be tracked on nodes only
- Mac layer Protocol standard used here is IEEE 802 11b

1 7.5 PROPOSED ALGORITHMS

This research thesis is based on two dynamic programming algorithms using the context-sensitive Hidden Markov Model as given below

- Insider Algorithm
- Alignment Algorithm

Insider algorithm is used for evaluation of network in initial phase and Alignment is used for grayhole detection and identification but both of them have merged for achieving the required goal The complexity of this algorithm is O(n^2), including the set of nodes and its transitions(received packets) plus emissions(sent packets) of the nodes in network

1.8 THESIS ORGAINIZATION

This thesis is organized as follows Manet introductions, its architecture, applications vulnerabilities, security issues and the routing protocols used in MANET are presented in first chapter Chapter 2 describes the literature review in depth with its shortcomings related to our problem domain area Chapter 3 discusses our problem and its requirements with analysis in greater depth Chapter 4 explains the proposed solution and its methodology with detailed information according to the problem Chapter 5 presents the simulation scenarios, tests results and its performance details Chapter 6 concludes the final results and describe its expected future work

CHAPTER 2
LITERATURE REVIEW

2.1 INTRODUCTION

Grayhole or Selective forwarding attacks affected the MANET environment in a very dangerous ways We have studied the existing techniques presented by previous researchers in the field of security of the mobile adhoc networks They discussed the various solutions along their pros and cons Some of the related strategies are given below with their drawbacks and we extended our problem and its solution on the basis of these limitations

2.2 LITERATURE REVIEW

In this phase, we studied the existing blackhole grayhole or selective forwarding attacks and their detection and prevention strategies Some of them discussed below with their limitations

2.2.1 AI BASED BLACK HOLE TECHNIQUES

Monita et al [1] discussed an approach for detecting intrusion in MANET using fuzzy logic Their research was based on three attacks as blackhole, grayhole towards the source and grayhole towards the destination They first took some threshold value for determining packet dropping rate and then they detected attacks based on that value Secondly, they used fuzzy method, in which they assumed symptoms set as S= {s1 s2 s3} attack set A= {a1, a2, a3} and set of nodes as N= {1, 2, 3} They also considered four indications for successful attack detection scenario as occurrence indication conformability indication, non-occurrence and non-conformability indication Simulation results showed that when destination threshold grew larger, detecting the blackhole and grayhole ratio drop to be in minute amount The drawback of this approach was overhead in monitoring every action and degraded the network performance It improved the intrusion detection rate by using the fuzzy logic

Ahmed et al [2] described the detection of misbehaving nodes by Optimized Link State Routing protocol (OLSR) using Intrusion detection system (IDS) They discussed the suspicious node detection by validating the established routes In this paper, they were inclined towards the traffic relay attacks and discussed two attackers as blackhole and smart attacker (grayhole) They have used the periodic transmission of packets when valid connection of routes was established In simulations, it was shown that 12%

overhead was occurred in normal case but when attackers included due to Attacker Finder Messages (AFM), overhead was bit increased It lacked the false detection but improved the previous scheme by periodic monitoring

2.2.2 GENERAL AI-BASED APPROACHES

Shun-Zheng [3] explained the multiple tracking anomaly detection of the mobile nodes in adhoc networks They used the aggregate tracking and individual tracking approach for checking the behavior of the abnormal nodes and introduced the two states Hidden Semi-Markov Model (HSMM) to calculate the likelihood of the suspicious nodes by considering the parameters as RSS (received signal strength), claimed GPS positions media access control information and exchanged messages etc in network In the first step they took the initial estimates of the parameters whereas in second step they refined the normal nodes that were not suspicious The drawback of this model was, it did not store the most of the data as only few current results and also it lacked the implementation phase to validate the results

Slavisa et al[4] discussed the misbehavior detection by Artificial Immune System with secondary response system in MANET The Destination sequenced vector routing protocol was used for the network communication and they modified this protocol for their use The detection and classification had done by negative selection and colonel selection This technique has four stages first stage is learning and second is classification and detection and third had no misbehavior nodes where the misbehaving nodes from the second phase are still there In forth stage again detection and classification had done but here the initial set of the detectors were changed so its second stage implemented primary supervised learning and third stage implemented reinforcement learning They traced out the misbehaving nodes through the traces of the datasets for some intervals of the activity When the detector was matched to an antigen it was eliminated by the negative selection When the same node detected by the detectors at multiple intervals it was finally classified as misbehaving by colonal selection They had used some default values for the detection and classification of the nodes as classification error α = 0 0001 and threshold 0 06 for the successful detection and classification of the nodes This technique reduced the false accusations and improved the

true positive rate It was needed a huge amount of time while classifying the misbehavior nodes in network Simulation results showed that detection accuracy and effectiveness of colonal selection was good by giving secondary response to the AIS
Guorui et al [5] introduced a novel approach as group-based intrusion detection scheme for the wireless sensor networks They used the scheduling algorithm for the intrusion detection, in which sensor network was divided into different sub-groups Secondly, they used the monitoring algorithm to monitor the suspicious activities in each sub-group All nodes in network have the same capability to sense and judge They used Mahalanobis distance measurements for achieving dependencies to achieve accurate results It had generated less false alarm ratio, gaves good results and had less energy utilization The drawback of this scheme was continuous monitoring

2.2.3 TYPICAL TECHNIQUES

Qiang et al [6] presented an approach for detecting collaborative grayhole attacks in wireless mesh networks (WMNs) It comprised of forwarding assessment and two hop acknowledgement for detecting attacks successfully It first obtained attack information detection and reaction Every router had kept two packet counters for received packets and two hop acknowledgement When the attack was detected then source took the action based on reply packet, either it was positive negative or above the maxTry limit of "k", where k is the threshold value for challenge packets Challenge packet were used for attack information collection process The final visual outcomes by the simulated environment approved it that it was better scheme than the previous schemes while detecting the false positive and false negatives but when the threshold value was too small, false negative will increase whereas false positive will decrease The weekness of this approach was, it increased the computations when allocating alternative channels to the suspicious routes but made it efficient by adopting the Ad-Hash Algorithm

Devu et al [7] explained the reduction of selective forwarding attacks by a new methodology known as Channel-Aware Approach in wireless mesh networks They introduced an algorithm as Channel-Aware-Detection (CAD) that differentiates the selective forwarding attacks from the usual packet loss The transmission monitoring and estimation of channel was used for successful attack detection This approach reduced the false alarms and missed detection errors but when the attacks were generated then noisy channels could avoids sensing mechanisms that results to invalid threshold

Gul et al [8] proposed the hybrid approach for detection of selective forwarding attacks in MANET The attack detection of the selective forwarding attacks was by the global and local monitoring approach by considering the threshold 6 % for global and 12% for local identification based on the packet dropping ratio The considered error rate was initially the 3% for testing the scenarios Once the attack had detected globally then they checked its local position for attack identification They considered the network environment as normal or congestion with attack This approach was the best suited for periodic monitoring

Soufiene et al [9] presented the survey of reducing packet dropping problems in MANET They discussed three defense lines for securing the blackhole attacks along with their characteristics and risks First defense line dealt with the prevention of the attackers nodes where as second had used to establish the cooperation among routers via economic model Third defense line was used to detect misbehavior node detection and exclusion from the network The drawback was that these approaches were relying on few assumptions and they were not valid in MANET due to dynamic nature

Wei et al [10] proposed the injected traffic attacks (Injecting Data Packet Attacks (IDPA) and query flooding attacks) launched by the insider attackers in mobile Adhoc Networks (MANET) The proposed schemes were two defending schemes as fully distributed and centralized with decentralized implementation These techniques could cope with the advance transmission techniques as directional antennas or beam forming to avoid being detected The shortcomings of the fully distributed approach was to require extra space for the source, destination (SD) pairs while the centralized suffered from becoming the central detector as the attacker's target The final results represented that when no defense schemes were applied even the simple route IDPA could destroy the network performance but when the defending strategies were applied attackers could not obtain the more gain to destroy network parameters performance Experimental and theoretical results also agrees to these outcomes

Semih et al. [11] proposed performance analysis of ad-hoc networks under black hole attacks. They developed a new protocol called blackhole AODV. This scheme considered the second highest route reply for the data transmission from the destination node by discarding the first route reply from the nodes in the network path. This technique had suffered from the delays in transmission performance, non-encryption based mechanisms. Simulations outcomes pointed that it improved the performance of the network by 19% to the previous schemes.

Sonja et al. [12] investigated the CONFIDANT protocol to eliminate the misbehavior nodes from the network. Four components were used for detection and isolation of suspects. These components were monitoring, trust manager, reputation system and path manager. Monitor used neighborhood watch mechanism to identify deviations in the next hop nodes. When it had detected and then it transferred its report to trust manager to evaluate the reported behaviors trustworthiness through trust tables. After their verification, these were further passed to the reputation system in which nodes checked them through rating function. Its rating was done by using their own experience, experience from the neighbour nodes and their reported behaviors. Path manger was used to isolate the reported node from the network and warn them not to send or receive any data or control packets from them. The weaknesses of this protocol is that it is not scalable to large networks but only to medium and small networks. It could work efficiently even if the 60% of the network was suspicious. It also kept the false positive and false negative low.

G. et al [13] proposed the impact of grayhole attacks in Adhoc network. An analytical method was described for the detection of the grayhole attacks by probability distribution function. They also introduced the algorithmatic framework for the generation of the grayhole attack using Adhoc on-demand Distance Vector Routing Protocol (AODV). For simulating the experiments on 60 wireless nodes by introducing the 0% to 40% misbehaving nodes, the parameters as Packet Delivery Fraction (PDF), Normalized Routing Load (NRL), Total Dropped Packets and overhead were considered for checking the network performance. Concluded outcomes proved that presence of grayhole node increased overhead and decreased network performance.

Kirk et al [14] had developed the protocol named as WATCHERS to detect the disruptive routers using distributive network monitoring scheme It detected the suspicious routers that either drops or misroutes the packets It has four conditions for achieving successful functionality They were link-state condition, good neighbor condition, good path condition and majority good condition It had used validation and conservation of flow for detecting the misbehaving routers Conservation of flow was the total number of incoming bytes in any routers should be equal to the total number of the outgoing bytes otherwise the router was suspicious Each router had maintained seven counters, six for keeping the source $S_{x,y}$, destination $D_{x,y}$ and intermediate $I_{x,y}$ routers counter values and one for suspicious router counter values Some advantages of technique as it had network monitoring tools (traceroute program, SNMP (Simple Network Management Protocol)) It could also detect the suspicious routers that partially dropped packets This was based on dynamic threshold property to check the routers in worst case or ideal scenarios The disadvantage in this scheme was that it has no encryption mechanism for maintaining the packets integrity

Sergio et al [15] explained the approach as mitigating routing misbehavior in mobile ad hoc networks (MANET) by using the watchdog (WD) and pathrater (PR) Watchdog detected the suspicious nodes by promiscuous monitoring whereas pathrater ignored them in further routing by rating them The bad effects in watchdog is ambiguous collisions receiver collisions, limited transmission power, false misbehavior, collusion and partial dropping The advantage was that it can find the bad node at forwarding level along with the link level The results shows that it enhances the network performance from 9% to 17% in moderate cases and 12% to 24% in worst/extreme mobility scenarios

Peng et al [16] proposed the Detection method of gray-hole node known as Gateway Based Gray Hole Detection (GBGHD) in wireless mesh networks Gateway Based Gray Hole Detection algorithm monitored the gateway information and all the information sent or received by all the nodes in the network This Algorithm used the piggybacking technology to reduce the overhead of the packets in network Simulating the outcomes they considered the two-step architecture known as wired-cum-wireless network architecture This architecture could be used to simulate the wired and wireless network at the same time. They had used two parameters Packet dropping Fraction (PDF) and Normalized Routing load (NRL). By comparing it with the AODV+ technique in the simulation setup, it performed 10% better than the AODV+ technique. But still, it sufferred from the small number of packet loss ratio and delays in transmission because of its malicious nodes advertisement.

Hizbullah et al [17] discussed the security mechanism of avoiding the single and cooperative blackhole and grayhole attacks in AODV using optimal path routing and hashing technique. They considered the second optimal\highest RREP (route reply) message while ignoring the first route reply from the destination node in the network. They further proposed the Hash function SHA$_{128}$ (Simple Hashing Algorithm) for the prevention of multiple gray\blackhole attackers and also for maintaining the integrity of the packets for comparing the DPE (Data Packet Errors) in the network. SHA is less expensive so it can be easily applied. This technique improved the prevention of the malicious nodes as well as data integrity in the network but suffers from long time delays while waiting for the reply message or data packet error message and also for computation of hash function values at the destination.

Meenakshi et al. [18] extended the defense strategies of malicious attack in MANET by "A Behavioral Approach". They introduced the hybrid approach that was using the SVM (Support Vector Machine) classifier to classify the normal or abnormal behavior of the nodes. This classifier was using the three matrices to differentiate the behavior of the nodes as PDER (Packet Delivery Ratio), PMOR (Packet Modification Ratio) and PMIR (Packet Misroute Ratio). It collected the behaviors of all nodes and then compared it to certain threshold value to validate the actions either they were suspicious or not. SVM was accurate and effective in classification and hence improved it, but lacked the protection mechanisms as it was non encryption based. It had delays in performance while computing matrices values.

Faraz et al. [19] described the conservation of flow (CoF) with lossy channel in wireless mesh networks. They conducted the experiments for ideal cases and the scenarios with the lossy channel by using the parameters as transition matrix, sender and receiver matrices, delay, channel error rate, number of nodes and AODV protocol. The thresholds

0 01% for ideal case and 20% for the worst cases were used in this technique The experiments were using 8 and 12 wireless nodes Final results represented that in ideal case only 2% and in attacked environment it is 3% - 5% packets are dropped In worst cases packet dropping rate increases for the total number of the packets transmitted in particular time interval

Alper et al[20] discussed to detect the routers with incorrect packet forwarding behaviors They described the solution by dividing this issue in to three sub problems as characterizing the traffic for detecting assails, synchronizing all the routers and generation of response after getting detection of attacks They also developed the protocol as Π_{k+2} to detect the attacks and it is less costly at implementation

Taha et al [21] described the falsified data injection attack in multiple access relay Networks For detecting the misbehaving nodes and removal of their false injections, they appended the tracing bits at the source ends but for the correction of the results they had used the parity bits The relationship explained by them was between the tracing bits and parity bit for reducing the decoding errors and maximizing the performance of the network under the falsified data injection attacks and its final simulation results agrees to this fact

Rajendra et al [22] discussed the quantitative analysis of false positive and its effect on monitoring based intrusion detections for mobile adhoc networks They verified the experimental outcomes of the increased number of the false positives by Markov and probabilistic models But these results could not be simulated by any of the adhoc network simulators as NS-2, OPNET and Glomosim etc For this, they had implemented the GEV noise generator model in Glomosim that correctly visualized the false positive effects on network It sufferred from the overhead and the degradation of the network throughput

Elhadi et al [23] proposed a new Intrusion Detection System (IDS) named as Enhanced Adaptive Acknowledgement (EAACK) for the protection of the mobile adhoc network EAACK comprised of three components as acknowledgement (ACK), secure-acknowledgement (S-ACK) and misbehavior report authentication (MRA) This was acknowledgement based scheme but it was incorporated with digital signatures to exclude assailers from forging acknowledgement packets in network Through Simulations it was proved that it could be good for detecting the packet dropping attacks but it has the overhead in network while computation of the DSA and RSA signatures values for verification

Issa et al [24] developed a protocol as stealthy attacks and their detection and countermeasures (SADEC) in mobile adhoc network They defined that Stealthy attacks was the group of power control, packet misrouting, identity delegation and colluding collision They had used two strategies as first for reducing stealthy packet dropping by considering some guard nodes and second for detection of the power control. Identity delegation and colluding collision attacks by using additional neighbour nodes It showed that it was better than its previous methodology as Baseline Local Monitoring (BLM) but it was lacking by some of its facts as its guard nodes might be replaced by a misbehaving nodes by strong attackers groups

In [35] authors presented a scheme "A Vector Model of Trust for developing Trustworthy system" This Model was concerned with various degrees of trust and distrust using the parameters experience, knowledge and recommendations They had also investigated and compared dynamic nature of trust In [36], this Model was extended to detect the suspicious nodes in MANETs

Jiang-Ming et al[40] investigated the Cooperation Bait Detection Scheme(CBDS) to detect collaborative attacks In this scheme they used three phases for attracting the attackers First phase introduced the bait RREQ' packet to gain attraction of the malicious nodes by sending the first response to source RREQ packet While second phase was concerned with the reverse tracing program by using the trust set and doubtful information set of the node in any active path for the accurate detection of the suspicious route in network Third phase consisted of the dynamic threshold that was initially set to 90% and varies between 85% to 95% First two phases uses the proactive defense while the last phase uses the reactive defense This scheme is further compared to 2ACK BFTR and simple DSR and it had better performance ratio in terms of the throughput and packet delivery ratio matrices

2.2.4 COMPARISON MATRIX

Table 2 1 summarizes the limitations of all the techniques addressed previously

Reference No.	Approach Category	Threshold Type	Algorithms Developed\Techniques	Drawbacks
Ahmed et al [2]	AI based grayhole detection techniques	Static	AFM and PVM algorithms	low detection rate
Slavisa et al[4]			Learning and Adaptation Algorithms	Overhead in classification
Jian-Ming et al[40]		Hybrid	CDBS Scheme	Routing Overhead and Average end to end delay
Devu et al [7]			Channel Aware Detection Algorithm	Avoids sensing mechanisms in attacked environment
Patel et al[23]			Behavioral approach for Grayhole using SVM	Low detection
Meenakshi et al [18]		Dynamic	SVM classification Algorithm	Low performance
Sujatha et al[39]		Dynamic	Genetic Algorithm based IDS	Computationally intensive
Chaoli et al[38]			BANBAD	

Monita et al[1]			IDS using Fuzzy logic	
Devu et al [7]	Typical Detection Techniques	Static	Channel Aware Detection Algorithm	Avoids sensing mechanisms in attacked environment
Peng et al [16]		Static	GBGHD	Delays due to advertisement info
Hizbullah et al [17]			AODV with optimal path routing and Hash algorithm	• Computation overhead • Delays due to ACK
Qiang et al [6]		Dynamic	Algorithms for Attack information collection and Detection	Increased cost(time and alternative channels)
Devu et al [7]			Channel Aware Detection Algorithm	Avoids sensing mechanisms in attacked environment
G et al [13]			Algorithm Grayhole	Increases routing overhead
Basit et al[37]			Aggregation Algorithm	Congregation Threshold complexity
Elhadi et al[23]			RSA and DSA algorithms	Overhead in computation

Table 2 1 Algorithms\Techniques and their drawbacks

2.3 SUMMARY

After the detail discussion of the literature review, it shows that a lot of work has already done for the detection of black hole and gray hole attack in wireless sensor network and also there are some on MANETs We concluded that AI based Grayhole detection approaches are intelligent attack detection techniques because they had focused on the degree of attack instead of the specific static or dynamic threshold Black hole detection was more easy as compared to gray hole detection and its identification procedure because it is a smart attacker as compared to black hole Now We were requiring a new and fully featured scheme as for dealing and handling with the smart attacker and we already knew that it was dropping packets selectively It was staying in the network for long time and very complex to detect and identify than the other attacks Many techniques proposed in literature, were not sufficient to handle this kind of attack

CHAPTER 3
REQUIREMENT ANALYSIS

3.1 INTRODUCTION

MANET is a wireless network and it is combination of moving devices [15] It performs a variety of functions like packet sending, routing, deploying network and its services and transmission between moving devices Many proactive and reactive routing protocols as Dynamic Source Routing (DSR), Destination Sequenced Distance Vector (DSDV), Ad-hoc on Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) protocols are used for route discovery and data transmission in network[1][17] Each intermediate node in the network forwards the data and control packets to other nodes but most ad hoc routing protocols are not secure against malicious attacks as they are relying on implicit trust neighbors' relationships Some Techniques [18] are needed to protect MNAET from the Attackers for their prevention, detection and proper response These methods are availability of network, integrity of packets, and its confidentiality and users authentication [18] Multiple solutions are presented by the researcher to protect MANET but they are not sufficient and it is needed to develop a new secure strategy for its safety measures

In this chapter, we will discuss the requirement analysis of our work Here, we will describe common network attacks in section 3 2 In section 3 3 we will explain problem Definition, focus of research would be discussed in 3 4 and in section 3 5 we will conclude the whole in summary

3.1.1 MANET Attacks

MANETs [12][29] are suffered from a lot of attacks that are difficult to detect as compared to infrastructure networks MANETs attacks falls into two broad categories They are based on source of attack as internal and external attacker and also known as active and passive attacker as shown in figure 3 1 Passive attacks are behavioral attacks that do not disturb normal communication of the network as it always secretly overhears to the network traffic where as active attack disrupt all the active performance of the network

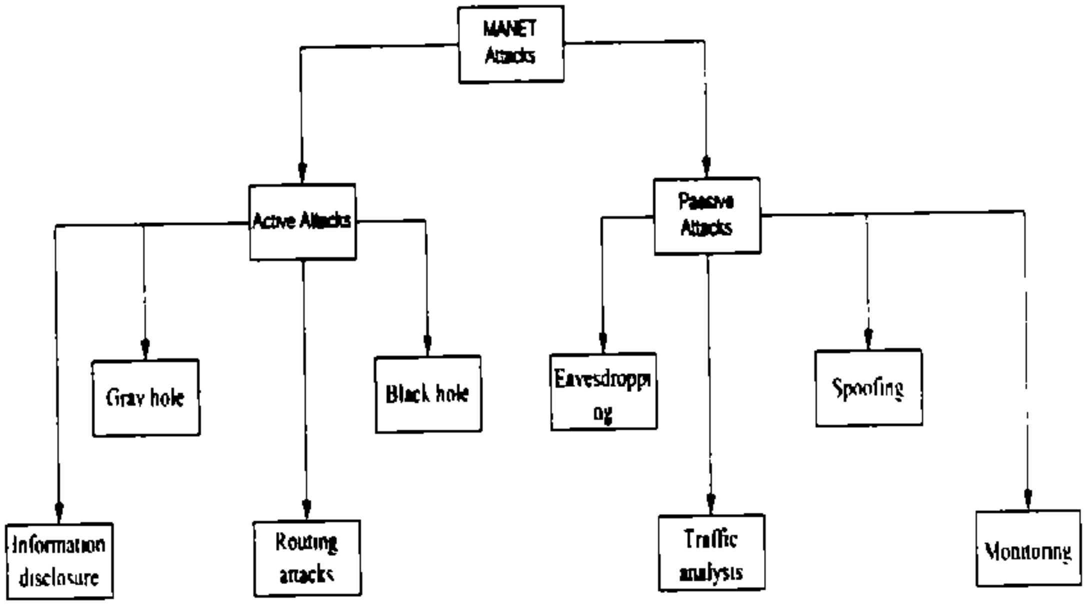

Figure 3 1 Manet Attacks[29]

These are some active and passive attacks that are taken from the literature which are explored in detail in this phase

3.1.1.1 ACTIVE ATTACKS

MANET active attacks are discussed below in detail as grayhole blackhole information disclosure and routing attacks

- **GRAYHOLE ATTACKS**

These attacks occur at the network layer as it is active in nature [29] It intentionally losses some or many packets to destroy the performance of network layer It works in two stages Firstly it pretends that it has the fresh route to the destination and violate the AODV routing protocol mechanism Secondly, when it gets success from the first step it begins to lose packets that it receives from the source node It drops packet at certain intervals due to its selective dropping nature it is difficult to locate It often behaves as a normal node but for some intervals of the time it changes its behavior to suspicious node It reduces the variety of the matrices in network as performance, packet delivery rate end-to-end delay and packet drop rate [29]

- **BLACKHOLE ATTACKS**

The Attacker node [7] gain access to network in this case by violating the standards followed by the routing protocols and drops both data and control packets For the participation in the network in case of the AODV routing protocol it initiates the route request mechanism to its destination through intermediate node with its specific sequence number If the intermediate nodes are not destinations they will broadcast it again to the other nodes until the destination is reached Now the destination will send the route reply to the source by using the route to the intermediate nodes by upgrading the source sequence number If during the RREQ time any intermediate node send the reply to the source by using the destination sequence number either equal or greater to show that it is destination The actual path between the source and destination could be lost where link error messages could be originated for the source node Intermediate node could be the suspicious and can destroy all of its packets as it is the black hole attacking node nature [7] Its mechanism is described in figure 3 2 Attacker node have minimum hop distance and it can cause to destroy packets

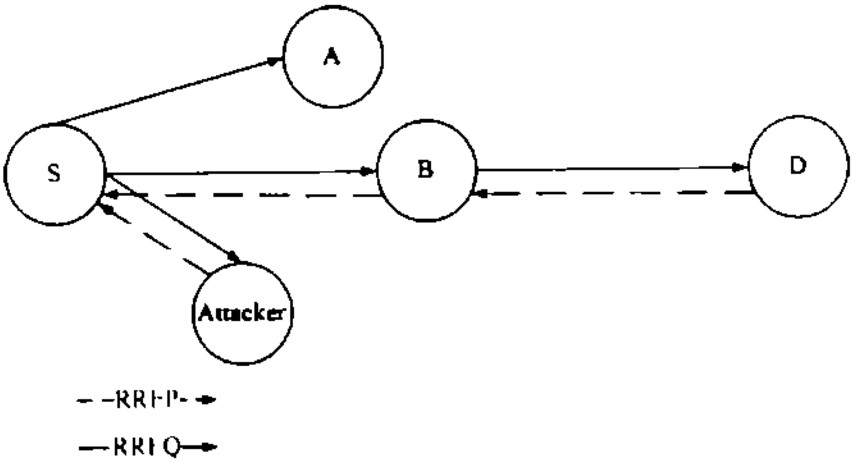

Figure 3 2 Black hole Attacker Representation[9]

- **INFORMATION DISCLOSURE ATTACKS**

Assailers try to gain participation in network to access secret and necessary data about its architecture layout, dispersed areas of nodes and its most updated routes to exploit them [31]

- **ROUTING ATTACKS**

These are network layer attacks Here nodes connect to other nodes in their environment and their connection is based on mutual trust to each other Various attacking parties, first breaks the protocols specified rules to participate in the network so they could be able to overhear the network transmission, add their own packets etc , for their purposes Mostly adversaries define routing loops, congestion in network and channel contention at certain places to make poor efficiency [30]

3.1.1.2 PASSIVE ATTACKS

- **EAVESDROPPING**

To overhear network communication is eavesdropping It is unauthorized access of the sender's packets and use them for illegal aims and objectives As the nodes in the network rely on infrastructureless medium So assailers could read their messages or send the bogus packets in their places to the transmission [32]

- **SPOOFING**

Attackers masquerade by having the IP of another node and gets all the packets inclined to the actual node This type of the misbehavior happened in the network to gather data and attacking node may introduce other severe assails using this This kind of the node may be a part of many route and cause a serious damage [32] Figure 3 3 shows the mechanism of the spoofed link

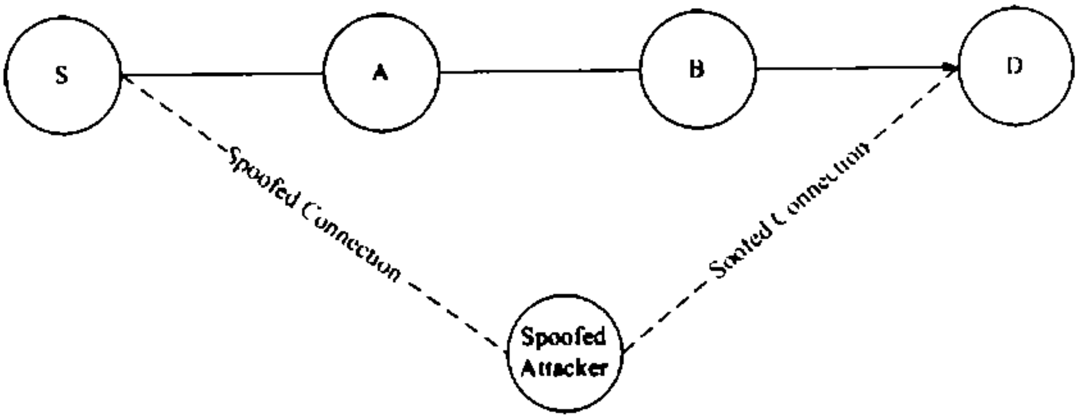

Figure 3 3 Spoofing Attacks and Connections[9]

- **TRAFFIC ANALYSIS**

To access the network information during transmission in a passive mode and their working and responsibilities is traffic analysis [32]

- **TRAFFIC MONITORING**

This is not specified to Mobile Adhoc Network, several networks are also suffered from this as cellular, satellite and wireless local area networks It is launched to access the network users and their duties related information to cause many other misbehaviors [32]

3.2 PROBLEM DEFINITION

Grayhole attacks are one of the most sophisticated and need complex mechanisms to detect They are basically the variation of the blackhole attacks in which attacker partially drops some packets [7] The attacker node always tries to behave as a normal node but for the very small interval it switches its normal behavior and drops the packets as the most valuable information of the network To prevent, detect and eliminate this attack various solutions are cited in the previous literature but they all have few shortcomings [6][4][8][12] Some of the techniques lacks the efficient detection strategies of the suspicious nodes in the network that's why, they fail to present the accurate solution While the rest of the strategies lack the unsupervised learning [8]

Now here, in this research work we have developed an algorithm using context sensitive HMM for Grayhole Identification with the help of unsupervised learning Although this is the latest and the most effective approach to all the existing solutions but it also suffers from some drawbacks First it suffers from dynamic memory allocation problem Secondly we are using the dynamic threshold property to determine the false detection ratio so the attackers might be tried to modify the threshold and could claimed to higher false detection rate The authors are not focusing on its solution at this time

3.3 PROBLEM STATEMENT

> "If there are N numbers of nodes in a network topology T and all are assumed to be well behaving except one that is Grayhole as M based on the some threshold parameter ¥, how can we adjust our threshold to the identification of that Grayhole Node "

- **RESEARCH OBJECTIVES**

After studying the literature and its deep analysis, we have formulated the problem as how to identify the suspicious Grayhole node in the MANET using unsupervised learning approach Here, we will focus on the smart attacker which drop the data on certain time intervals and we will discuss how to prevent it from the data loss MANETs uses multiple paths to send packets to destinations and suspicious hops drop packets secretly at certain intervals from any hop and there are a lot of difficulties to detect them Authentication and access control mechanism to network are lacking so network performance is badly affected Techniques using the supervised learning also requires more prior knowledge that decreases efficiency Recently, many security challenges and attacks occurred in MANET because all nodes are independent and can communicate with each other via neighbors or intermediate nodes Normally packet loss is due to due to collision or congestion The following major problems are found in our case

- ✓ Identification of the Grayhole node by using unsupervised learning
- ✓ Unstable dynamic threshold specified leads to low detection rate

3.4 SUMMARY

We have discussed the problem on a specific domain In past, there are a lot of methodologies used for describing detection, prevention and elimination of the malicious nodes as grayhole attacks MANETs performance was degraded and its QoS is also effected when legitimate node are trying to destroy its packet from inside the network So there is a need to develop an artificially intelligent a security solution that would be more active to overcome the existing and future MANET threats and reduce false negative rate of the network

CHAPTER 4

SYSTEM DESIGN

4.1 INTRODUCTION

We have discussed our problem already in detail in previous chapter Now we have designed our solution that will be more robust to overcome grayhole attacks in MANET It will identify the suspicious node easily based on its learning approach and certain threshold value It has been conducted to develop the efficient and more secured strategy in Mobile Adhoc Networks as they do not have fixed domain and are of varying nature There are a many security challenges that requires a lot of concentration for well functioning So, with the time, an intelligent and efficient technique is required for MANETs This chapter is focused on detailed description of the proposed methodology and its requirements for its good functionality

4.2 DESIGN REQUIREMENTS OF OUR SOLUTION

For construction of the its design it has required the following as below

- A network architecture for representing the safe and sound environment for its interpretation
- It also needs any form of learning for training as we have specified unsupervised learning because it has some advantages over supervised learning
- There is a need to set the effective dynamic threshold to minimize the false negative ratio and to improve the true positive ratio
- It requires training data either labeled or unlabelled we have used here is number of packets and number of nodes\states or collectively we could say the total amount of the data during its processing for maintaining each state.node probability

4.3 REFERENCE ARCHITECHTURE

The grayhole attacks partially drops the packets in certain time intervals that could degrade the performance of MANET For tracking the behavior the gray holes we have used cs-HMM[43] to model its architecture For Monitoring the packet drop rate we have used the context sensitive states\nodes that stores the information at each state to adjust their evaluation rates The context sensitive states\nodes have their own transition and emission probabilities at each node to evaluate their drop rate

4.5 PROPOSED APPROACH

The proposed approach is described as under by following steps

4.5.1 DESIGN

We have developed an HMM based Grayhole Identification Algorithm that will follow the design in the figure below and it starts with the initial state probability $\pi_i = 0$ and the set of its sent packets 'a_{ij}' and dropped packets 'b_{jk}' for calculating its state information The algorithm is described in the end of this chapter with its functional case study Our proposed technique design can be expressed as below

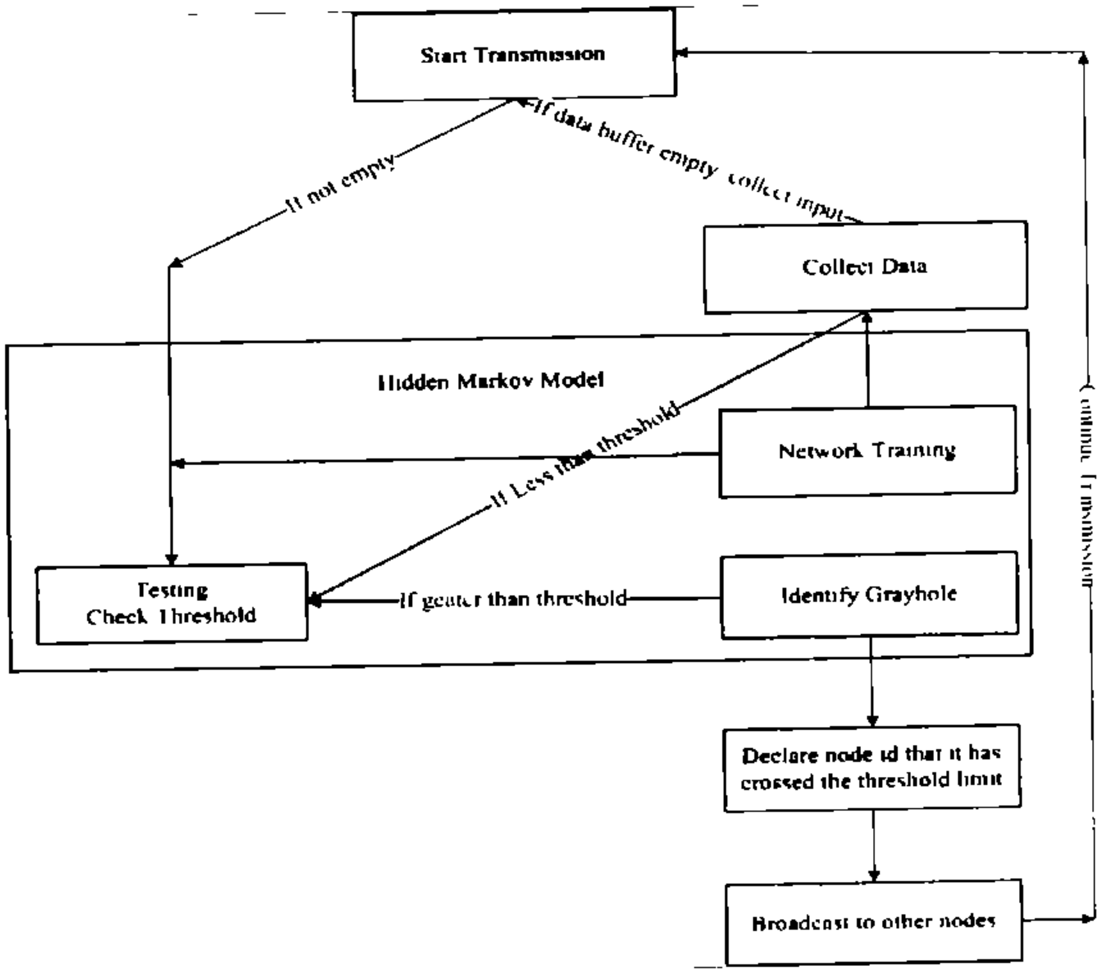

Figure 4 1 Design Of The Proposed Approach

It has started with the normal communication of the network. first the information of the network will be collected for few minutes and then evaluation of the network be done by the forward algorithm and it has used as the training data for the future observations The learning here is unsupervised and is done by algorithm The packet drop rate of each node have been determined from the first phase and then the comparison have made to detect the most suspicious node by the algorithm using dynamic threshold property The attacker have been identified accordingly

4.5.2 DESCRIPTION OF PROPOSED SCHEME

The proposed algorithm is described by the following fundamental steps in this scenario we have

i We have evaluated the each node\state in network by the algorithm under es-Hidden Markov Model Its observed information have been used as training data Training has based on the two parameters as states\nodes and Packet drop ratio

ii. We have assumed that source and destination are not suspicious because we are dealing with packet drop rate on each node and source has no data receiving packets and destination has no data packets sending to some nodes during communication along the path Source only receives control packets and destination has to send control packets only

iii. Each node will be based on three observations as sending packets, receiving packets and dropped packets respectively

iv. The most suspicious node detection done along the AODV protocol oriented path with the minimum hopcount by the Viterbi algorithm using the following terminology as mentioned below,

a) We have specified the timing for packet dropping ratio, it has been checked at the states processed at the session time and continues till the session ending We are using the periodic monitoring for the nodes here

b) If Packet drop rate is less than 2*RTT of the total sent packets it is considered as normal node

c) If the packet drop is greater than or equal to 2*RTT loss of the total sent packets, it is grayhole node

v. Once the node is specified as the grayhole, we have identified it as a grayhole by using its packet dropping ratio or average packet dropping ratio

4.5.3 THRESHOLD CALCULATION

If **'n'** is total originated packets for the destination and **'RTT'** is the round trip time of the packets, threshold will be adjusted dynamically as in its initial phase

Threshold= 2*RTT

and in its subsequent network transmission phases it will updated automatically according to the scenario If the packet drop occurs twice of the RTT then that node is considered as grayhole node of the network

4.5.4 MAPPING OF cs-HMM ELEMENTS TO NETWORK ARCHITECHTURE

The mapping of this model is given as below

cs-HMM --- Network Architecture

cs-Transition Variables --- Total packets sent\recieved

cs-Emission Variables --- Total dropped packets

cs-States --- Set of nodes

cs-Hidden States --- Source, Destination

cs-Observed States --- All intermediate States including Suspicious node

4 5.7 PROPOSED ALGORTIHM

Our proposed Algorithm is using cs-Hidden Markov Model that is used to detect the suspicious node from the MANET cs-HMM uses two states sets as hidden and observable set of the states which have been already described in previous topic In this technique we have initially specified two dynamic programming algorithms but while using we have merged them to a single algorithm for the evaluation and learning of the network and the Identification of the grayhole node from the network The algorithm is given as under but it will be explained with an example in the subsequent topic

➢ VARIABLES USED AND THEIR NOTATIONS

initial state probability = π_i

sent_packet = a_{ij}

recieved_Packets = b_{jk}

States = Sj, // counter for all states\nodes

Time t, // counter for time

Total time T

Threshold Th

• PSEUDOCODE

➢ Phase 1: Initialization phase

```
init network(),
init paths(),
currentSimTime = 0,
Th = 2*p(pktDropRate|$s_i$(t)),
Sj=0,
$a_{ij}$ = p($s_j$(t)|$s_i$(t-1))= 0,
$b_{jk}$ = p($v_k$(t)|$s_j$(t)) = 0,
```

➢ Phase 2. Evaluation and Learning

```
while(currentSimTime != simTimeTotal)
```

```
    if($S_j$ <= Sn && queue == empty())            // Sn -> for final state

            collect_data(),

    else

            calculate_ $p(v_k(t)|s_i(t))$,

            calculate_ $p(s_j(t)|s_i(t-1))$,

            $p(pktDropRate|s_j(t))$ =  $[(p(s_j(t)|s_i(t-1)) - p(v_k(t)|s_i(t)))/ p(s_j(t)|s_i(t-1))]$,

            $p(percentPktDropRate|s_i(t))$ = $[(p(s_j(t)|s_i(t-1)) - p(v_k(t)|s_j(t)))/ p(s_i(t)|s_i(t-1))]$
                    *(1/ 100),

            collect_ $p(pktDropRate|s_j(t))$,

            currentSimTime++,

            $S_i$++,

            until currentSimTime == simTimeTotal,


if($p(pktDropRate|s_j(t))$ < Th)

    train_the_network(),

    It is Normal Scenario,

else

    Attack Oriented Scenario,
```

- **Phase 3: Identification of Grayhole Node**

```
if ($p(pktDropRate|s_j(t))$ > Th){

    Monitor(Nodes)

    Locate $p(pktDropRate|s_j(t))$(SuspiciousNodes),
        detect_max(p(pktDropRate|$s_i(t)$))

        Identify_Grayhole(node).

}
```

➢ **Time Complexity**

The time complexity of this algorithm is $O(n^2)$, by considering its set of nodes in the network and its recieved plus sent packets

4.6 WORKING OF OUR PROPOSED ALGORITHM: CASE STUDY

Let us take an example of the network scenario consisting of the 10 nodes which have been arranged in a topology When the communication has started, protocol is initiated to communicate in the network Our proposed Protocol is AODV, it has started the RREQ mechanism from the randomly chosen source to the destination node for the discovery of the routes During communication each node have maintained a routing table for maintaining the destination address, next hop address, destination sequence number and the TTL(Time To Live) value The RREQ mechanism has broadcasted through the neighbour nodes in the network and when it has reached to destination and the RREP packet has reversed back to source node along the path having minimum hop count The path has be established between them and the source will start communication to the destination node

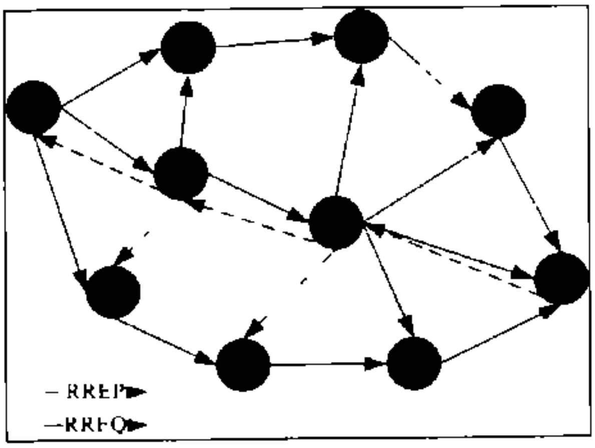

Figure 4 2 AODV Communication

Here, when communication has been established with the help of the AODV routing protocol, the network nodes have maintained the routing table with its initialized values after the communication setup Now the algorithm have been triggered, the initial path have been selected with the minimum hop distance along the first iteration values is as below, with the hidden and observed states as below

Hidden states = {S, 8, 4 D}

Observable states = {1, 2, 3, 5, 6, 7}

Now the algorithm has started and it will calculate the probabilities of all the values and it will update the values during each iteration till the normal communication stops for few minutes, its normal communication will store its data for training of the network and when the attack will be activated it will check all nodes packet drop probabilities and it will compare their drop ratio and average packet drop ratio

The first iteration is started as given below with the path

This is calculated from state\node S -> state\node 8

t=0,

Sj=0

πi=0,

recieved_Pkts = 1800,

Sent_Pkts =2000,

totalSent_Pkts =2000,

p(packetDropRate) = 0 1

path = {S,8,4,D}

Now the second iteration will be given as below

this is calculated from state\node 8 -> state\node 4 t=1,

Sj=1,

recieved_Pkts = 18000,

Sent_Pkts = 20000,

totalSent_Pkts = 20000,

p(packetDropRate) = 0 1,

path = {S,8,4,D}

Now the third iteration is given as below

this is calculated from state\node 4 -> state\node D

t=2

Sj=2,

recieved_Pkts =18000,

Sent_Pkts =14000,

totalSent_Pkts =18000,

p(packetDropRate) = 0 25

path = {S,8,4,D}

now loop has been terminated here

The final test matrix has calculated and is stored by the algorithm for the probability of packet dropped ratio along the specified path is given as below, the training matrices are not mentioned here

$$\begin{array}{c|cccc} & S & 8 & 4 & D \\ S & 0.1 & 0 & 0 & 0 \\ 8 & 0 & 0.1 & 0 & 0 \\ 4 & 0 & 0 & 0.25 & 0 \\ D & 0 & 0 & 0 & -0.99 \end{array}$$

The matrix and comparisons made by the Viterbi in matrix form is given as below

$$\begin{tikzcd}
 & S & 8 & 4 & D \\
S & 0.1 \arrow[dr, <->] & 0 & 0 & 0 \\
8 & 0 & 0.1 \arrow[dr, <->] & 0 & 0 \\
4 & 0 & 0 & 0.25 \arrow[dr, <->] & 0 \\
D & 0 & 0 & 0 & -0.99
\end{tikzcd}$$

Here, the execution has terminated successfully by the algorithm and it has detected the maximum packet drop by comparing all the dropped values of the nodes and the node 4 is suspicious because it has dropped above 2*RTT of the packet sent as shown in matrices above

We have checked its packet drop ratio at some intervals of time on the states while execution Any state having the max packet drop ratio is the suspicious state\node In this case let us say node 4, is suspicious and we will check its packet drop ratio, if at any interval of the time it is greater than 2*RTT or exactly 2*RTT of the sent packets then we could say it is suspicious it could be detected by the algorithm At the end, the algorithm will be terminated successfully This was our proposed Algorithm working

4.7 SUMMARY

In short, we could summarize the whole approach in just few words MANET is infrastructureless and open to many security attacks as DOS attacks Communication in MANET is always dependant on its intermediate nodes cooperation So there might be more chances to the existence of the attacker nodes Here, we have proposed an artificially intelligent solution in which detection and identification of the grayhole node is done by cs-HMM based Algorithm It is such a technique that checks the suspicious nodes packet drop probability at each state by using its sent, dropped and received packet observations on each node to determine the packet drop ratio Basically, grayhole node is a kind of the attacker node that selectively drop some packets at certain intervals without forwarding them to destination node So we have discussed how to eliminate this node and save network from the damage and loss of its resources We have used parameters to prove this research in a good working state

CHAPTER 5
IMPLEMENTATION

5.1 INTRODUCTION

In our research work we are trying to simulate the grayhole attacks in wireless adhoc network in OMNeT++ As there are many simulation tools used for designing the mobile adhoc networks (MANETs) i e , OPNET, GlomoSim and Network Simulator (NS-2) etc , but we have used the OMNeT++ version 3 3 for the simulation of our work and verifications of its results In this chapter we have discussed the testing environment data flow diagram and flow of our proposed scheme

5.2 OMNET++

It is a network simulator[33] used for the visualizations of discrete events normally for telecommunication transmissions, protocol and queuing networks simulation, for verification of the hardware topologies and their working etc It can be used anywhere where discrete events and object-oriented approach is reasonable Blocks of the codes are arranged in the hierarchy Communication between different modules is by sending packets to each other and packets structure of data could be complicated Each module forward packets to the receiver by already established route or the link through it Every module depends on different parameters for their customized actions or the layout of the network All functionality of the modules are coded in C plus plus

5.2.1 HIERARCHICAL MODULES STRUCTURE

The OMNeT++ programs are composed are multiple modules in a hierarchy Top level is the system block\module where as lowest one is the simple module in the order Mostly simple modules consists of some algorithms A module has more than one blocks is the composite module as shown in figure below

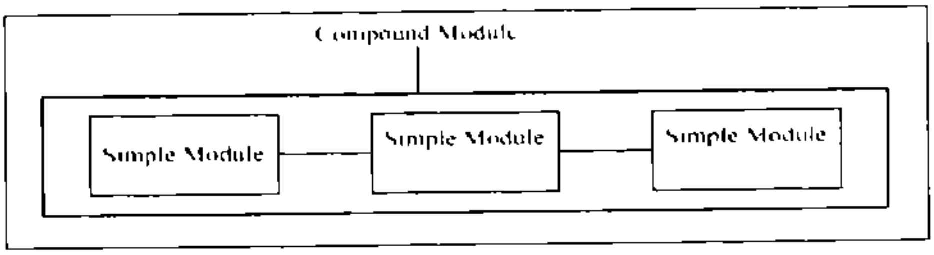

Figure 5 1 Modules Structure[33]

5.2.2 MODULE TYPES

The simple and compound modules are extended from the term module types When user discusses some framework or model, it explains module types that specifies the object or instances of the complicated modules The developer firstly specify the system module and all other simple modules that are referred to it as its submodules When users define that module type is the building block than simple or composite modules are considered at the same level Developers are permitted to divide simple module into further simple and composite to use them as a simple It will not disturbs the others peoples module types

5.2.3 LINKS, MESSAGES AND GATES

Links are used to connect a level of single modules arranged in hierarchical structure [33] They can be used to connect two submodules or they can be used for connection of one submodules to a composite module as shown in figure below Gates provides the interfaces for incoming and outgoing packets\messages between all the modules in a system Messages depict the packets and frames in the network communication All messages are travelled through a consecutive links called a route

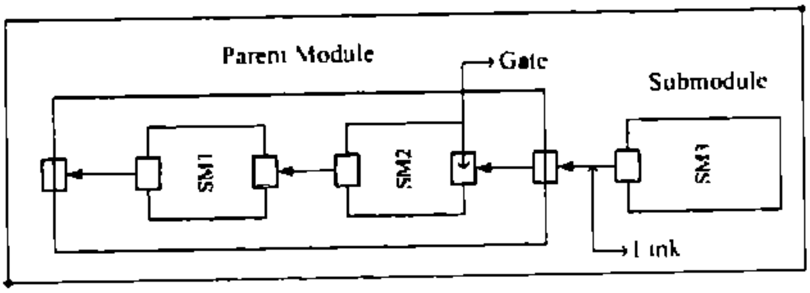

Figure 5 2 Links and gates representation[33]

5.2.4 PACKET TRANSMISSION MODELING

There are three variables used for packets travelling in network for helping the new developers Because they can be applicable to different designs and they are bit error rate propagation delay and data rate When the packets arrive through a link are delayed by certain limits of the time is propagation delay Bits are not travelled accurately due to bad link quality are known as bit error rate Transfer of packets from one location to another is data rate

5.3 THE ADHOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV) PROTOCOL

AODV [34] has not mentioned all the hop-by-hop paths during the initial setup They are only invoked when they are required for communication in network Paths are used only when they are needed except they are discarded from the network It starts route discovery procedure by RREQ (route request) and RREP (route reply) parameters Sender sends RREQ message using intermediate nodes RREQ message comprises of IP address of sender, current sequence number, destination IP Address, destination last sequence number and broadcast Id It uses ring search strategy in which in which host assigns a Time to Live value to its Route Request at some starting point The response of the route request is considered to come to sender host in that time period (as TTL assigned) otherwise the source starts another RREQ with incremented TTL If response is found in a TTL time limit then the path between sender and receiver will be oriented for a session They can communicate to each other for time specified earlier by them If sender host walks away during active session then there is a need to forward RREQ again by choosing another path in the network If some intermediate host along the path moves away from its original location then host from the upstream initiates the RERR (Route Error) message to its previous hosts to inform senders After receiving that Route Error source ends the transmission along that specific path and initiates the new route for Route Request Procedure for further communication [34] The data flow diagram of Route Request and Route Reply processing is shown in figure 5 3

5.3 1 DATA FLOW DIAGRAM

AODV data flow diagram is described by the figure 5 3

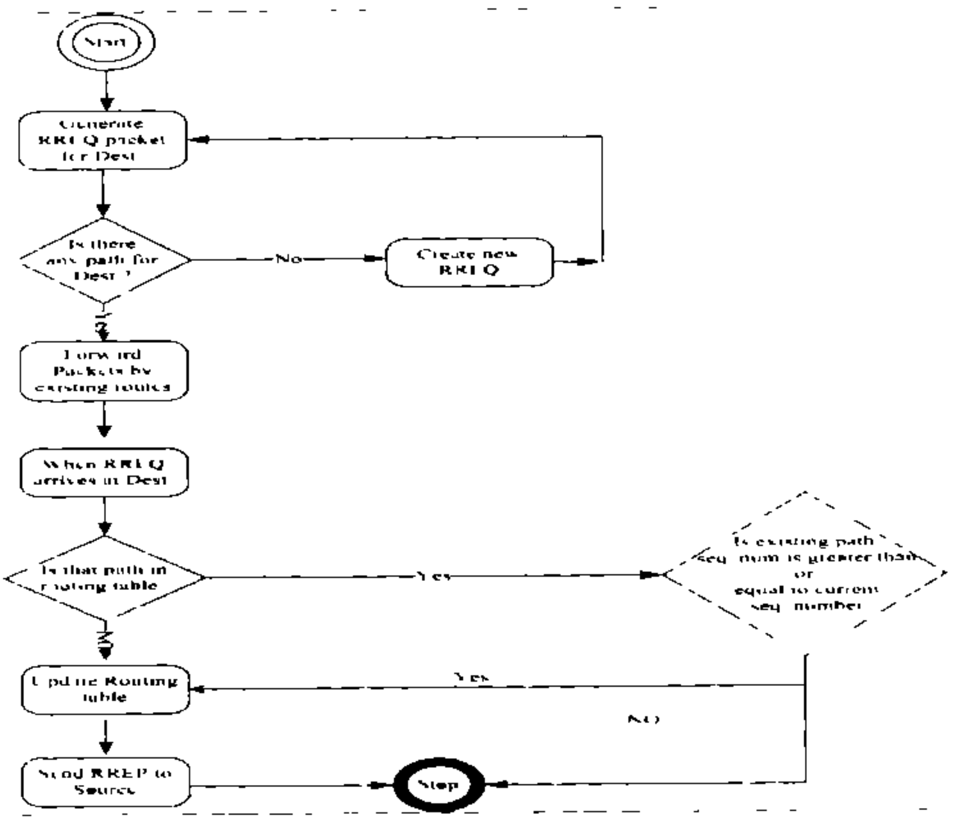
Start
Generate RREQ packet for Dest
Is there any path for Dest ?
No
Create new RREQ
Forward Packets by existing routes
When RREQ arrives in Dest
Is that path in routing table
Yes
Is existing path seq num is greater than or equal to current seq number
Yes
Update Routing table
NO
Send RREP to Source
Stop

Figure 5 3 AODV control mechanism for RRFQ and RRFP[34|

5.5 SUMMARY

In chapter we have discussed the OMNeT++, its features and other Graphical User Interface details The data flow diagram of our AODV protocol has been discussed with its parameters At the end, control of the proposed System is also discussed to show the functionality of the scheme with the AODV routing protocol In the next chapter we will show different test cases for the evaluation of this approach

CHAPTER 6:

TESTING AND PERFORMANCE EVALUATION

6.1 INTRODUCTION

In this chapter we have discussed the simulation scenarios of the presented approach We have specified the simulation parameters and its environment (hardware specifications and software both) on which it is tested Two test cases are presented with different simulation times to show their functionality under ideal and attack oriented situations At the end the comparison of the technique will be conducted to show achievements and benefits of this scheme

6.2 SIMULATION SCENARIOS AND TESTING ENVIRONMENT

It is described as below using different set of topologies

6.2 1 TEST SYSTEM

Processor: Intel(R) Core(TM) i5-2450M CPU @ 2 50 2 50 GHz

RAM: 6 0 GB

System type: 64-bit OS

6.2.2 OPERATING SYSTEM AND SIMULATION TOOLS

OS: Windows 7 Home Premium

Tools: Visual C++ 2008 and OMNeT++ 3 3

6.3 SIMULATION SCENARIOS

For the implementation of the Grayhole attacks in MANET we have used OMNeT++ version 3 3[33] simulator for the testing and validation of the simulation scenarios and their results either our developed Algorithm is working according to our requirements or not Testing our inputs, we have implemented simulations for two network topologies In first, we have used 8 and 12 nodes network and did not simulate any grayhole attack but in second we again use same topologies and initiate grayhole attacks and hence we concluded the final outcomes of the simulation scenarios Our research is based on these metrics as packet sent, received, packet drop rate and throughput for identification of grayhole node in the absence or existence of attack

6.3.1 SIMULATION PARAMETERS

Our simulation environment contains the nodes as 8 to 12 in each topology We have considered the world size as an area of 250*250m The simulation time specified for these scenarios are 30 minutes The parameters of this simulation are shown in Table 6 1 The topology will be mesh and static considered in all cases

Num of Nodes	8, 12,20 (mesh and static topology)
Num of Suspicious Nodes	1
Simulation World Size	250*250m
Packet Size	1024KB
Traffic	CBR
Protocol used	AODV Routing Protocol
Wireless Standard Specified	802 11b
Data Rate Used	2Mbps
Traffic Load	50pps

Table 6 1 Network Parameters[8]

6.4 PERFORMANCE AND EVALUATION

The testing and validation of the system is proved through the simulation of the three topologies as 8 nodes, 12 nodes and 20 nodes mentioned below

6.4.1TEST CASES AND COMPARISON RESULTS OF 8 NODE TOPOLOGY

The Figure 6 1 shows the 8 node static and partially connected mesh topology with the stationary mobility model This topology will be used for testing the effectiveness of the proposed technique using the throughput, packet drop rate, overhead and number of sources matrices

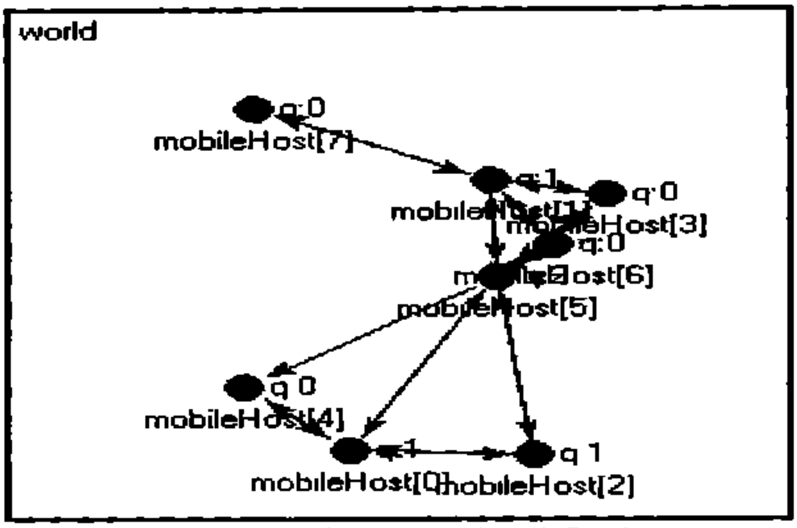

Figure 6 1 8 Nodes Static And Mesh Topology

6.4.2 1 TESTS AND COMPARISONS RESULTS FOR THTOUGHPUT

This is a topology of 8 static nodes in partially connected mesh layout to test the throughput of the proposed solution The mobility model used here is stationary mobility in which nodes are on fixed positions and do not move using any speed The throughput of this technique is about 25 % better than the previous like SFAM in both attack and normal cases as shown in figure 6 2

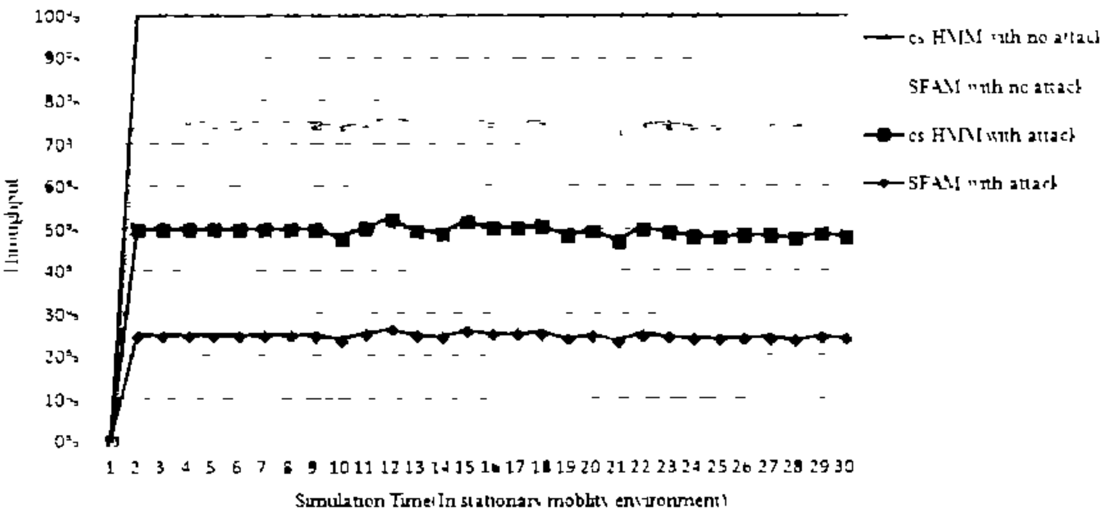

Figure 6 2 Throughput Verses Mobility In Case Of 8 Node Static Mesh Topology

6.4.1.2 TESTS AND COMPARISONS RESULTS FOR PACKET DROP RATE

Here the topology and its arrangement is considered the same such as in previous one The packet drop rate of this technique is 15% better than the previous as it uses the drop rate threshold is 2*RTT Its detection rate is also more better than the previous technique Figure 6 3 shows the packet drop rate of this approach and previous approach in both cases with attack and without attack considered

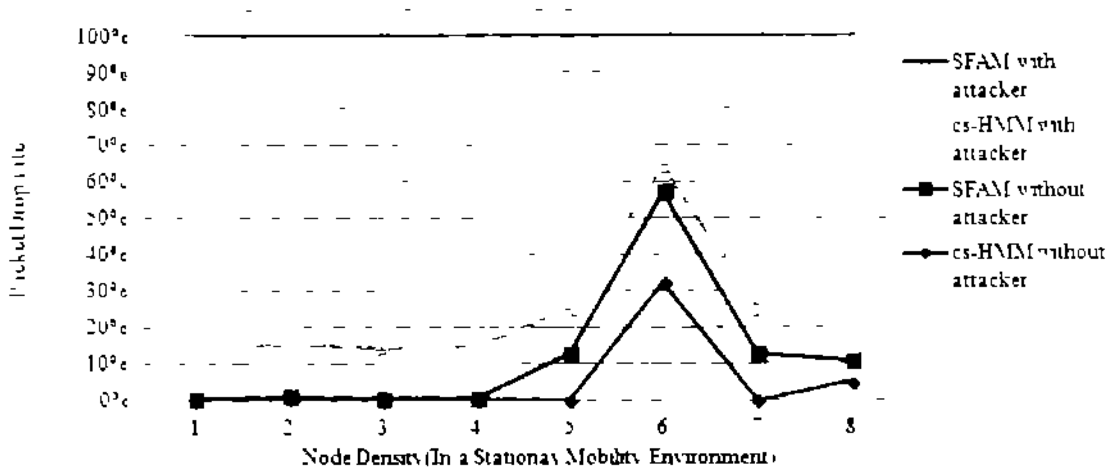

Figure 6 3 Packet Drop Rate Verses Mobility In 8 Node Topology

6.4.1.3 TESTS AND COMPARISONS RESULTS FOR OVERHEAD

This topology is of static 8 nodes in partially connected mesh layout using the stationary mobility model In this technique, we have used periodic monitoring and unsupervised learning to reduce overhead and they minimized the overhead up to 88% and it is the improved and latest technique to the previous to handle grayhole attacks effectively The figure 6 4 shows its results both in normal case scenario and its attack oriented scenarios The figure 6 4 also gives the comparison details to its previous approach

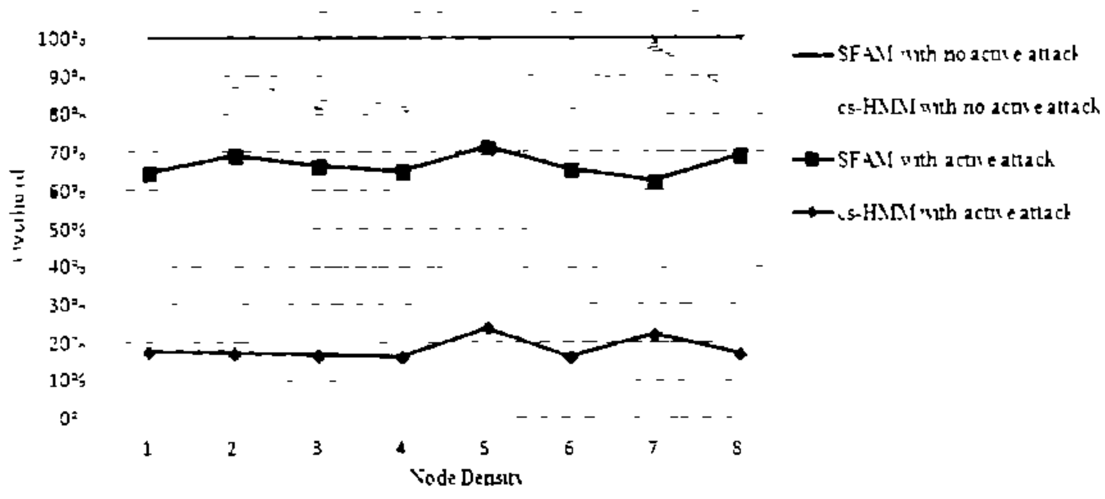

Figure 6 4 Overhead In Case Of 8 Static Mesh Topology

6.4.1.4 TESTS AND COMPARISONS RESULTS FOR NUMBER OF SOURCES

This Figure 6 5 shows us the number of sources traced out during the simulation As, in our case sources maintained the suspicious node entries for their future prevention In normal case scenario source only changes when it finishes its transmission otherwise it does change but in attack oriented cases it can change when some link break occurs, when maximum of the packets are timed out or due to medium access collisions in our case So this figure shows that there are maximum numbers of sources in attack oriented scenario rather than normal scenario and it is the best detection and prevention technique

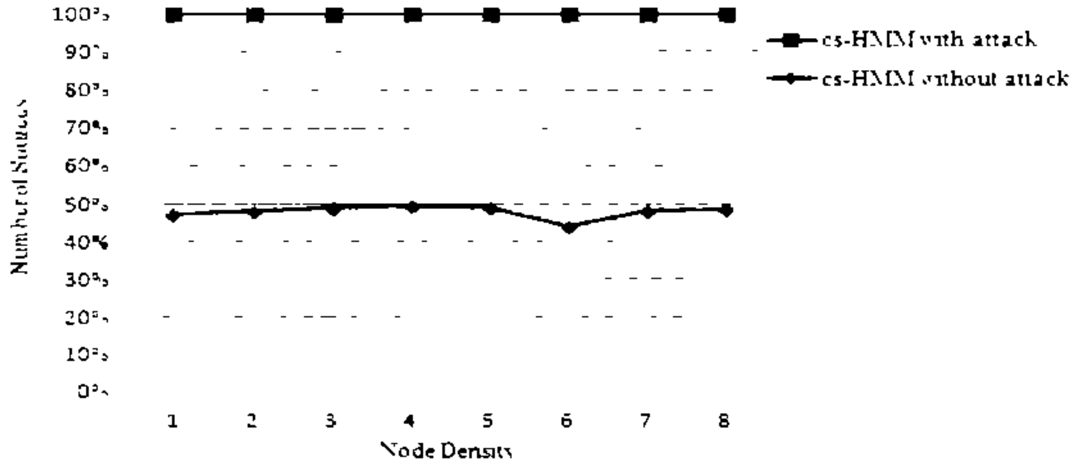

Figure 6 5 Number Of Source For Static Mesh 8 Nodes Topology

6.4.2 TEST CASES AND COMPARISON RESULTS OF 12 NODE TOPOLOGY

The Figure 6 6 shows the 12 node static and partially connected mesh topology with the stationary mobility model This topology will also be used for testing the proposed technique using the throughput, packet drop rate, overhead and number of sources matrices

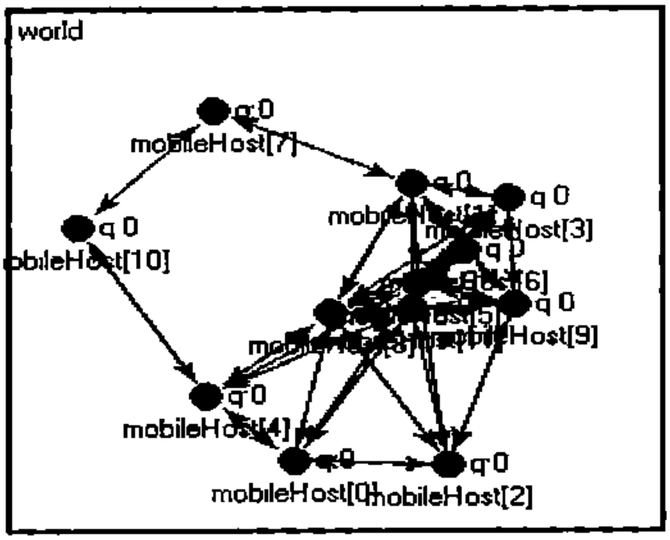

Figure 6 6 Network Topology Of 12 Nodes In Static And Mesh Layout

6.4.2.1 TESTS AND COMPARISONS RESULTS FOR THTOUGHPUT

This is topology of 12 static nodes in partially connected mesh layout The mobility model used here is stationary mobility in which nodes are on fixed positions and do not move using any speed The throughput of this technique is 4% better than the previous like SFAM in both attack and normal cases as shown in figure 6 7

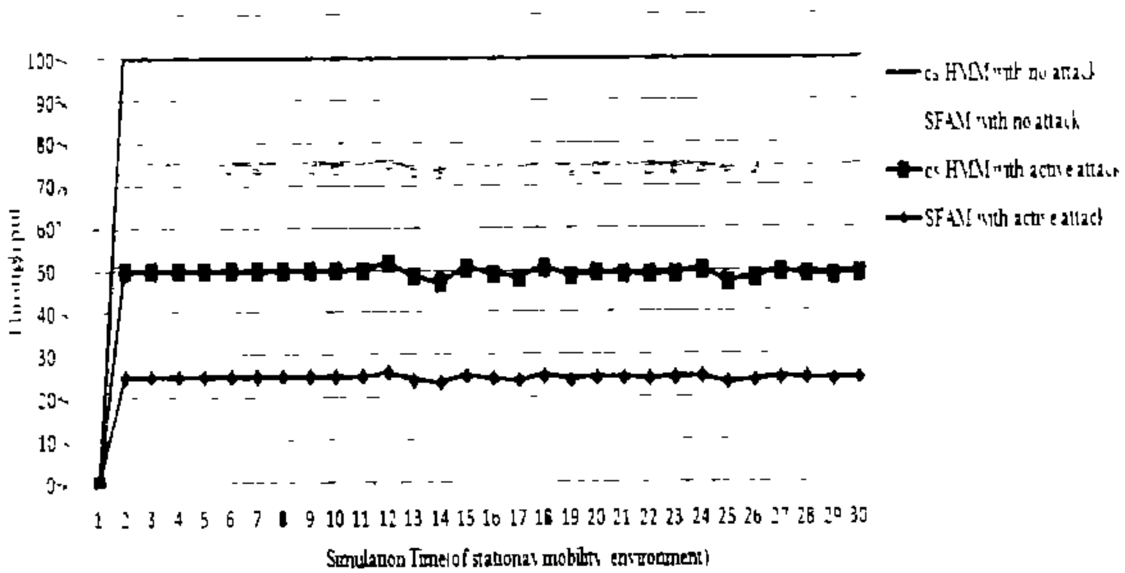

Figure 6 7 Throughput Verses Mobility Of 12 Node Static And Mesh Topology

6.4.2.2 TESTS AND COMPARISONS RESULTS FOR PACKET DROP RATE

Here the topology and its arrangement is considered the same The packet drop rate of this technique is 20% better than then the previous as it uses the drop rate threshold is 2*RTT So its detection rate is more better than the previous technique Figure 6 8 shows the packet drop rate of this approach and previous approach in both cases with attack and without attack considered

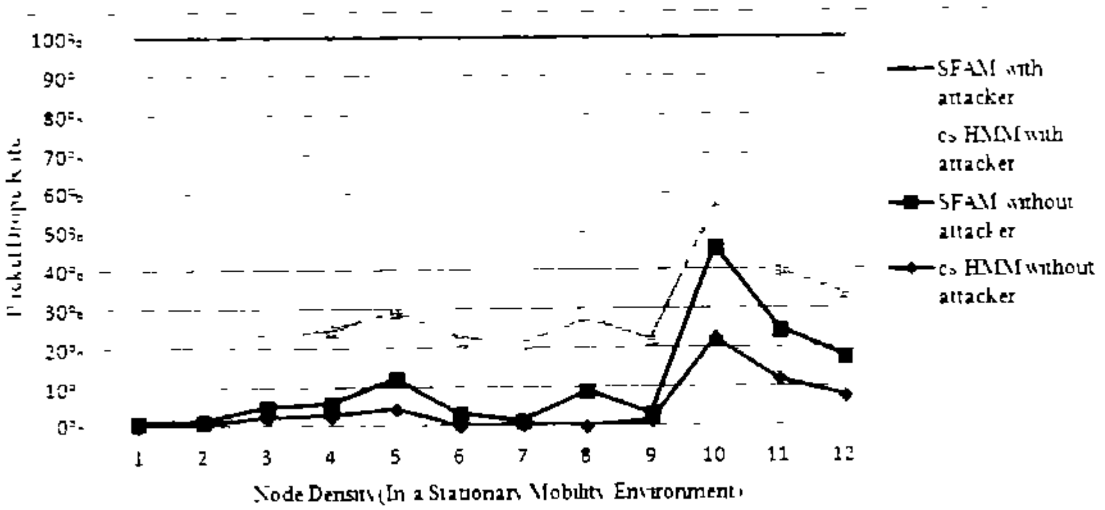

Figure 6 8 Packet Drop Rate Verses Mobility Of 12 Nodes Static And Mesh Topology

6.4.2.3 TESTS AND COMPARISONS RESULTS FOR OVERHEAD

The topology is again of static 12 nodes in partially connected mesh fashion using the stationary mobility model In this technique periodic monitoring and unsupervised learning has been used to reduce overhead and they have minimized the overhead up to 86% and it is the improved and latest technique to the previous to handle grayhole attacks effectively The figure 6 9 shows its results both in normal case scenario and its attack oriented scenarios The figure 6 9 also gives the comparison details to its previous approach

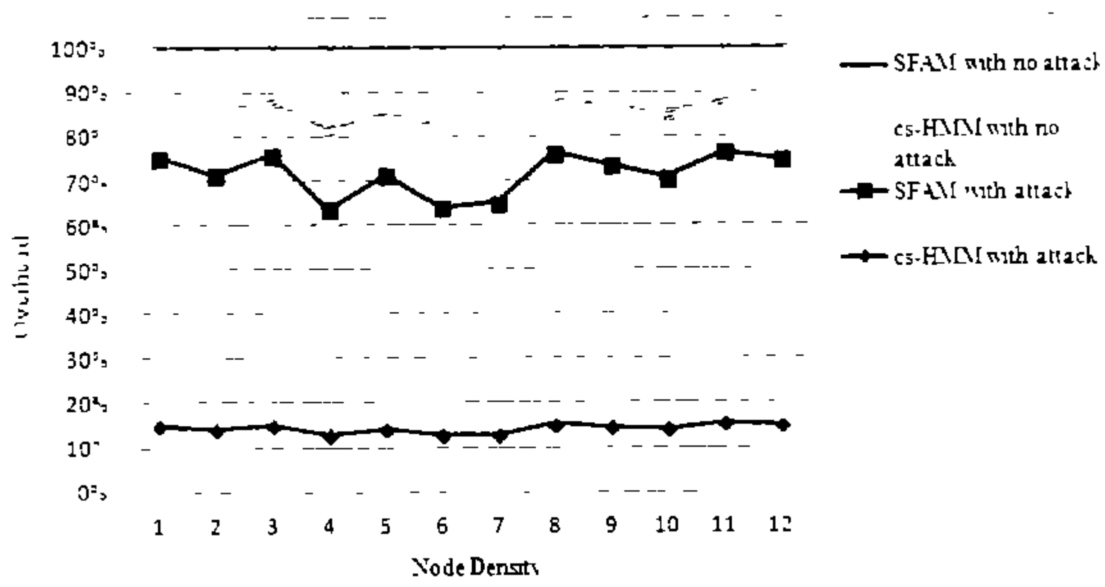

Figure 6 9 Overhead Of The Network 12node Static And Mesh Topology

6.4.2.4 TESTS AND COMPARISONS RESULTS FOR NUMBER OF SOURCES

Here the topology and the layout is again the same we have traced out the number of sources for the topology throughout the simulation because they maintain the attacker node information for their future prevention In normal case scenario source node only changes when its finishes its transmission But in attack oriented scenarios it changes because of the link breaks, timeout of the maximum packets or medium access collisions in our case so in attacks oriented scenario we traced out the maximum number of the sources for the active and accurate detection of the attacks Figure 6 10 shows the number of sources tracked out in both normal and attack oriented scenarios

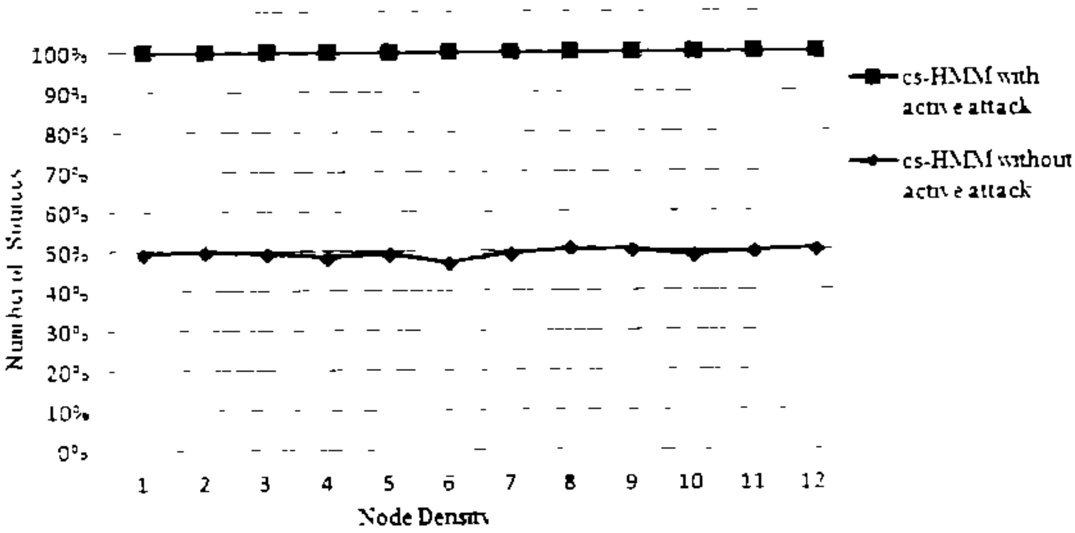

Figure 6 10 Number of Sources of 12 nodes static and mesh topology

6.4.2 TEST CASES AND COMPARISON RESULTS OF 20 NODE TOPOLOGY

The Figure 6 11 shows the 20 nodes static and partially connected mesh topology with the stationary mobility model This topology will also be used for testing the proposed technique using the same matrices such as throughput, packet drop rate, overhead and number of sources etc

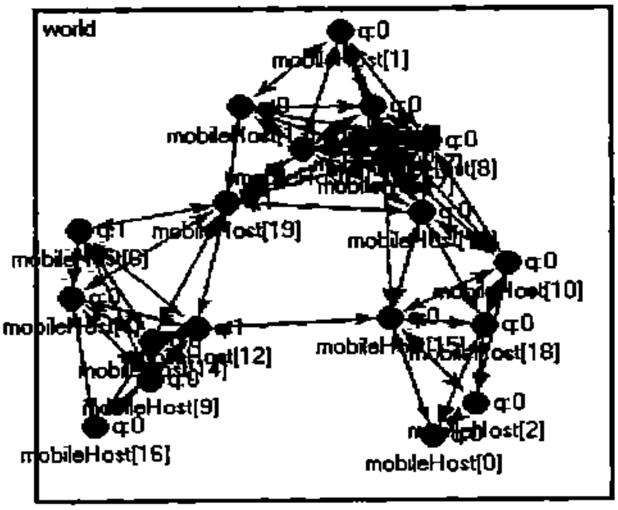

Figure 6 11 20 Nodes Static And Mesh Topology

6.4 3.1 TESTS AND COMPARISONS RESULTS FOR THTOUGHPUT

This figure 6 12 shows comparisons of the throughput of this approach to the previous approach in both normal and worst case scenarios This approach has the highest packet delivery ratio than the previous technique because it is using the threshold 2*RTT

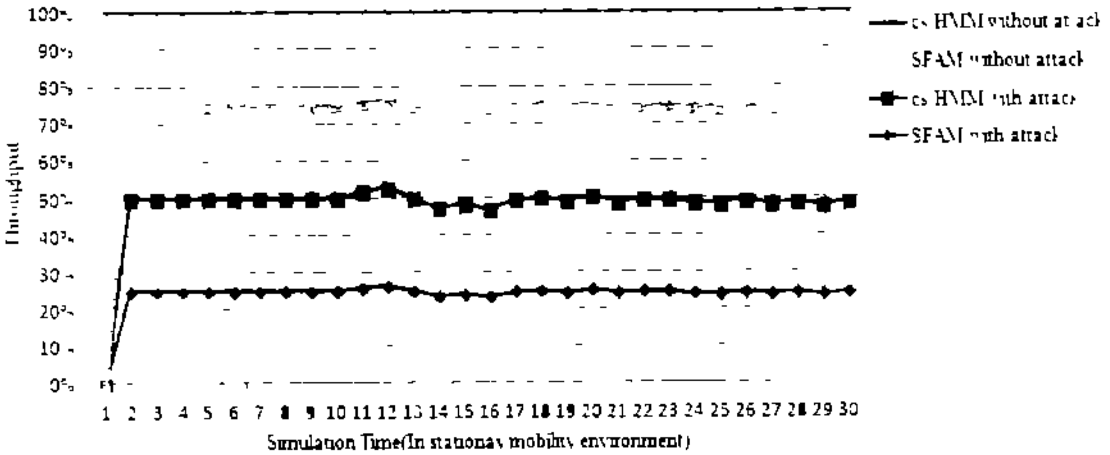

Figure 6 12 Throughput Verses Mobility Of 20 Nodes In Stationary Mobility Environment

6.4.3 2 TESTS AND COMPARISONS RESULTS FOR PACKET DROP RATE

The network topology has extended to 20 node with the same mobility environment and the topology is also static here The packet drop rate is less than the previous in normal and in attack oriented cases As the threshold is 2*RTT so its packets drop rate to the mobility is less and it is efficient to the previous technique Figure 6 13 shows the packet drop rate of this proposed approach to the previous SFAM

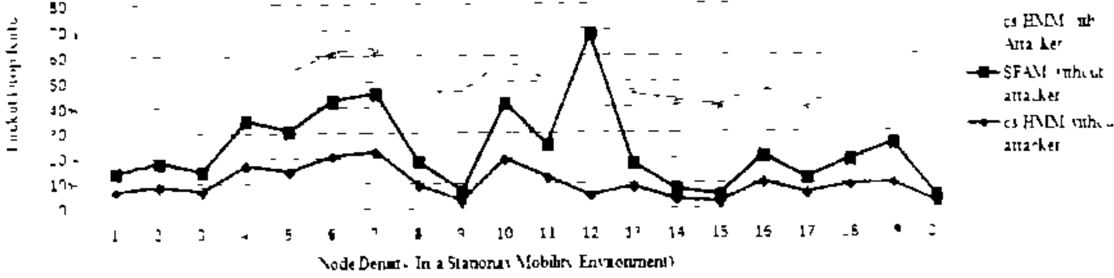

Figure 6 13 Packet Drop Rate Verses Mobility Of 20 Nodes Static And Mesh Topology

6 4.3.3 TESTS AND COMPARISONS RESULTS FOR OVERHEAD

The figure 6 14 shows the Overhead of this approach to the previous approach as it is showing reduced overhead to the previous one because in this we have used unsupervised learning technique to avoid excessive overhead during attackers and when there are no attackers are present in the system

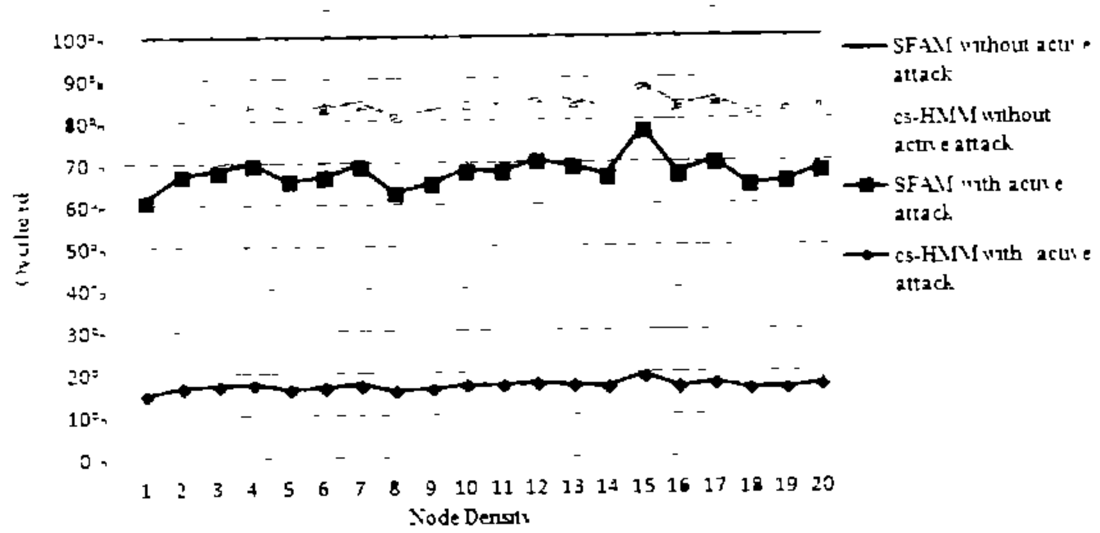

Figure 6 14 Overhead In 20 Nodes Static And Mesh Topology

6.4.3.4 TESTS AND COMPARISONS RESULTS FOR NUMBER OF SOURCES

This Figure 6 15 shows the number of sources for efficient detection of the attack in this environment with the stationary mobility In normal case it represents that there are no more sources as compared to the attack oriented case because in normal case, there are no attackers and more packets are not lost but in attack oriented case more sources are required to detect the attacker nodes So this is the best monitoring and preventing technique for grayholes

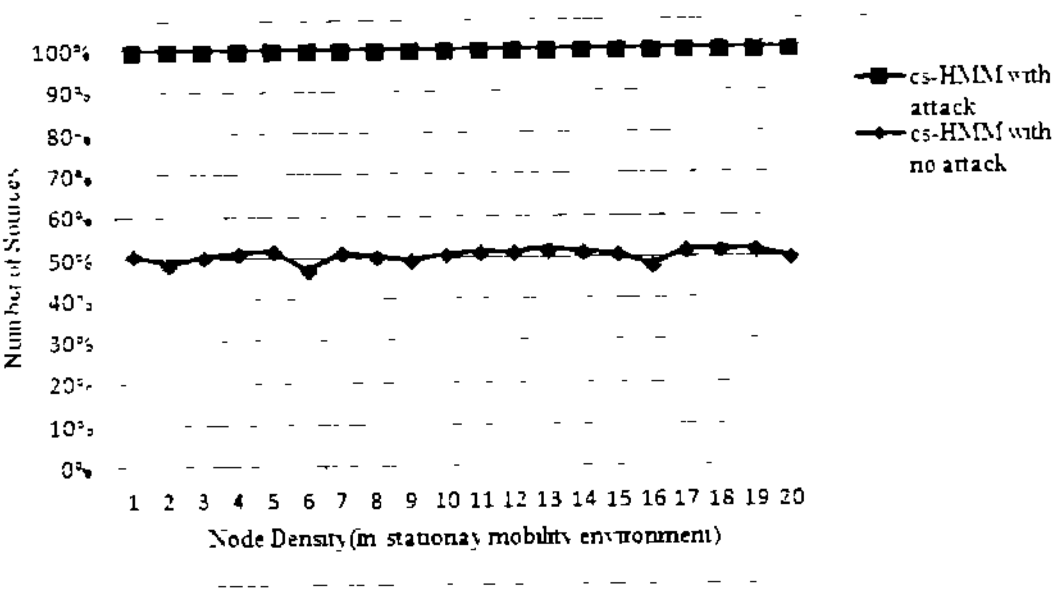

Figure 6 15 Number Of Sources In 20 Nodes Static And Mesh Topology

The detection accuracy of selective forwarding attacks approach is 89% to 92% in extreme case scenarios Now from the simulation results and graphs, it is proved that our approach is the best detection and identification scheme and robust enough to handle grayhole attacks as compared to previous ones The training and test detection results accuracies are mentioned below in the table 6 2

Simulation Time = 30 mins			
	For 8 nodes Topology	For 12 nodes Topology	For 20 Nodes Topology
	Training and Testing Accuracy	Training and Testing Accuracy	Training and Testing Accuracy
With no attacker environment	99 70%	99 39%	99 00%
With the attacker scenario	98 89%	97 64%	95 11%

Table 6 2 Training And Tests Verification Results

These are all the training and testing results with the simulation time mentioned along them These results are taken from both the normal network communication and the attacker node included in it

6.6 SUMMARY

By using the OMNeT++, We checked our cs-HMM based Grayhole Detection Scheme on two different topologies for the identification of grayhole\suspicious node in the network The network communication is done with the help of the AODV reactive routing protocol We have utilized 8 and 12 nodes network environment with the attacker nodes by considering the different channel error rates during communication If attack is detected in evaluation phase based on the training, it is identified as grayhole node in our network The dynamic threshold is used to minimize false positive and accurate detection of true positives rates We have also discussed the performance of the network by the metrics as packet sent, received, throughput and packet drop ratio Finally, we have presented our results by plotting the graphs for its final verification of training and testing

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSIONS

In short, this technique gave us the verified results to overcome some previous challenges Our research thesis and its verification has done through simulations and it shows that it has been working efficient at the cost of 97% or above in both attacked or non attacked environments It is more effective and accurate to the earlier solutions by the following points

- It has used Unsupervised Learning to improve its accuracy in learning and identification up to 95% which is extremely good
- This scheme has enhanced its detection rate by specifying dynamic threshold
- Technique has improved the true positive rate

Here, we have tried to explain a solution of some of its security threats after the deep analysis from the previous work This work has provided the detailed description of the impact of the Grayhole attacks in MANET by using AODV and cs-HMM As we have implemented the artificially intelligent technique to reduce the grayhole attacks as well as their false detection rate by using OMNeT++ We have implemented and validated the results of this strategy with the help of simulations under the ideal and under attacked environments Grayhole attacks have occurred due to the packet lost ratio in network under attack environment The results of this approach have also plotted in normal and worst case scenarios with the simulations These results clearly indicate that Grayhole attacks could badly effects the network performance and could be caused of important data drop of its users in MANETs

7.2 FUTURE WORK

The future directions of this work are as follows

- To enhance its performance efficiency and to decreasing its false detection rate, someone might use other protocols with this strategy
- It could be implemented with the SVM to compare its efficiency and effectiveness of working in MANETs

- It might be extended to build intrusion detection system for monitoring the other attacks

7.3 SUMMARY

This technique is artificially intelligent, very effective and accurate up to 95 percent for the identification of the Grayhole attacker node in the network Here we have developed and algorithm to the successful identification of the attacking node in the network We have specified the dynamic threshold to twice of the RTT of the packet for handling the attacker's node in network This technique is based on unsupervised learning in which nodes will be detected and identified by the developed algorithm's decisions This is most recent and efficient to all of the previous schemes in this field of the study

REFERENCES

[1] Wahengbam, Monita. and Ningrinla Marchang "Intrusion detection in manet using fuzzy logic " *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on* IEEE, 2012

[2] Abdalla, Ahmed M Imane Aly Saroit, Amira Kotb, and Ali Hassan Afsari "An IDS for detecting misbehavior nodes in optimized link state routing protocol " In*Computer Technology and Development (ICCTD) 2010 2nd International Conference on* pp 1-5 IEEE 2010

[3] Yu, Shun-Zheng "Multiple tracking based anomaly detection of mobile nodes " (2005) 130-130

[4] S Sarafijanovic and J Y L Boudec, "An Artificial Immune System Approach (AIS) with secondary response for Misbehavior detection In Mobile Ad Hoc Networks", *IEEE Trans on Neural Networks*, Vol 16 Issue 5,ISSN 1045-9227, pp 1076-1087, 2005

[5] Li, Guorui, Jingsha He, and Yingfang Fu "A distributed intrusion detection scheme for wireless sensor networks " *Distributed Computing Systems Workshops 2008 ICDCS'08 28th International Conference on* IEEE, 2008

[6] Liu Qiang Jianping Yin Victor Leung, and Zhiping Cai "FADE forwarding assessment based detection of collaborative grey hole attacks in WMNs "*Wireless Communications IEEE Transactions on* 12, no 10 (2013) 5124-5137

[7] Shila, Devu Manikantan, Yu Cheng, and Tricha Anjali "Mitigating selective forwarding attacks with a channel-aware approach in WMNs " *Wireless Communications IEEE Transactions on* 9 5 (2010) 1661-1675

[8] Gul, Sahar and Sher, Mohammad "Selective Forwarding Attacks In MANET",MS Thesis, Islamic International University, Islamabad, Pakistan, 2012

[9] Djahel, Soufiene, Farid Nait-Abdesselam, and Zonghua Zhang "Mitigating packet dropping problem in mobile ad hoc networks proposals and challenges "*Communications Surveys & Tutorials, IEEE* 13 4 (2011) 658-672

[10] Yu Wei, and KJ Ray Liu "Defense Against Injecting Traffic Attacks in Wireless Mobile Ad-Hoc Networks " *Information Forensics and Security IEEE Transactions on* 2 2 (2007) 227-239

[11] Dokurer, Semih, Y M Erten, and Can Erkin Acar "Performance analysis of ad-hoc networks under black hole attacks" *SoutheastCon, 2007 Proceedings IEEE* IEEE 2007

[12] Buchegger, Sonja, and Jean-Yves Le Boudec "Performance analysis of the CONFIDANT protocol" *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* ACM, 2002

[14] Bradley, Kirk Alton, et al "Detecting disruptive routers A distributed network monitoring approach" *Network IEEE* 12 5 (1998) 50-60

[15] Marti Sergio, Thomas J Giuli Kevin Lai, and Mary Baker "Mitigating routing misbehavior in mobile ad hoc networks" In *Proceedings of the 6th annual international conference on Mobile computing and networking* pp 255-265 ACM, 2000

[15] Dalal, Renu, Yudhvir Singh and Manju Khari "A Review on Key Management Schemes in MANET" *International Journal of Distributed and Parallel Systems (IJDPS) Vol* 3 (2012)

[16] Prakash, Shiva Rajeev Kumar, Brijesh Nayak and Manindar Kumar Yadav "A Highly Effective and Efficient Route Discovery & Maintenance in DSR" *International Journal on Computer Science and Engineering* 3, no 4 (2011) 1546-1553

[17] Taneja, Sunil, and Ashwani Kush "A Survey of routing protocols in mobile ad hoc networks" *International Journal of Innovation, Management and Technology* 1 3 (2010) 2010-0248

[18] Shanmuganathan, V, and T Anand "A Survey on Gray Hole Attack in MANET" *International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN* (2012) 2250-3501

[19] A Rosenberg, "Lecture 12-Hidden Markov Model Machine Learning", available online at http //www scribd com/doc/77998240/Andrew-Rosenberg-Lecture-12-Hidden-Markov-Models-Machine-Learning (accessed 2 April 2015), 2010

[20] Ghahramani Zoubin "Unsupervised learning" *Advanced Lectures on Machine Learning* Springer Berlin Heidelberg, 2004 72-112

[21] Zhou, Peng, Zhengtao Xiang, and Yufeng Chen "Detection Method of Gray-Hole Node in Wireless Mesh Networks" *Computational and Information Sciences (ICCIS) 2013 Fifth International Conference on* IEEE, 2013

[22] Khattak, Hizbullah, N Nizamuddin, and Fahad Khurshid "Preventing black and gray hole attacks in AODV using optimal path routing and hash " *Networking Sensing and Control (ICNSC), 2013 10th IEEE International Conference on* IEEE 2013

[23] Patel, Meenakshi, and Sanjay Sharma "Detection of malicious attack in manet a behavioral approach " *Advance Computing Conference (IACC), 2013 IEEE 3rd International* IEEE, 2013

[24] Usha, G and Sayan Bose "Impact of Gray hole attack on adhoc networks "*Information Communication and Embedded Systems (ICICES) 2013 International Conference on* IEEE, 2013

[25] Shakshuki, Elhadi M , Nan Kang, and Tarek R Sheltami "EAACK—A Secure Intrusion-Detection System for MANETs " *Industrial Electronics, IEEE Transactions on* 60 3 (2013) 1089-1098

[26] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi "Manet vulnerabilities challenges attacks, application " *IJCEM International Journal of Computational Engineering & Management* 11 (2011) 32-37

[27] Aarti, Dr SS "Tyagi,"Study Of Manet Characteristics Challenges Application And Security Attacks" " *International Journal of Advanced Research in Computer Science and Software Engineering* 3 5 (2013) 252-257

[28] M A Abdelshafy and P J B King, "Analysis of the security attacks on AODV Routing", *Internet Technology and Secured Transactions (ICITST)*, pp 290-295 2013

[29] M Vasava and H Patel, "Comparison of Different Methods for Gray Hole Attacks on AODV based MANET", IJEDR , ISSN 2321-9939, Vol 2, Issue 1, pp 60-66 2014

[30] Wu, Bing, et al "A survey of attacks and countermeasures in mobile ad hoc networks " *Wireless Network Security* Springer US, 2007 103-135

[31] Sahadevaiah Kuncha, and Prasad Reddy PVGD "Impact of security attacks on a new security protocol for mobile ad hoc networks " *Network Protocols and Algorithms* 3 4 (2011) 122-140

[32] Goyal Priyanka, Sahil Batra, and Ajit Singh "A literature review of security attack in mobile ad-hoc networks " *International Journal of Computer Applications* 9 12 (2010) 11-15

[33] Andras Varga, "OMNET++ Discrete event Simulation system, Version 3 3 user manual ", essay utwente nl/58509/1 scriptie_E_van_Eentennaam

[34] Taneja, Sunil, and Ashwani Kush "A Survey of routing protocols in mobile ad hoc networks " *International Journal of Innovation Management and Technology* 1 3 (2010) 2010-0248

[35] Ray, Indrajit, and Sudip Chakraborty "A vector model of trust for developing trustworthy systems " *Computer Security ESORICS 2004* Springer Berlin Heidelberg 2004 260-275

[36] Gong Wei, Zhiyang You Danning Chen, Xibin Zhao, Ming Gu and Kwok-Yan Lam "Trust based malicious nodes detection in MANET " In *E-Business and Information System Security 2009 EBISS'09 International Conference on*, pp 1-4 IEEE 2009

[37] Qureshi, Basit Geyong Min, and Demetres Kouvatsos "M-Trust A trust management scheme for mobile P2P networks " *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on* IEEE, 2010

[38] Cai, Chaoli, Aakash Gupta, and Rajib Paul "BANBAD-A Centralized belief-networks-based anomaly detection algorithm for MANETs " *Global Telecommunications Conference 2009 GLOBECOM 2009 IEEE* IEEE 2009

[39] Sujatha K S , Vydeki Dharmar, and R S Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET " *Recent Trends In Information Technology (ICRTIT) 2012 International Conference on* IEEE 2012

[40] Chang, Jian-Ming, Po-Chun Tsou, Isaac Woungang Han-Chieh Chao and Chin-Feng Lai "Defending against collaborative attacks by malicious nodes in MANETs A cooperative bait detection approach " *Systems Journal IEEE* 9 no 1 (2015) 65-75

[42] Ahsen KH Faraz, Nyla Khadam Muhammad Sharif and Noor Zaman "Conservation of flow with Lossy Channel in Wireless Mesh Network " *Journal of Information & Communication Technology* 1 (2007) 10-20

[43] Yoon Byung-Jun, and P P Vaidyanathan "Context-sensitive hidden Markov models for modeling long-range dependencies in symbol sequences " *Signal Processing IEEE Transactions on* 54 11 (2006) 4169-4184

Acronyms

MANET	Mobile Adhoc Network
IDPA	Injecting Data Packet Attacks
CAD	Channel Aware Detection
WD	Watchdog
PR	Pathrater
SD	Source Destination pairs
HSMM	Hidden Semi-Markov Model
RSS	Received Signal Strength
AFM	Attacker Finder Messages
IDS	Intrusion Detection System
OLSR	Optimized Link State Routing
DSR	Dynamic source routing
AIS	Artificial Immune System
GBGHD	Gateway Based Gray Hole Detection
SNMP	Simple Network Management Protocol
AODV	Adhoc On-demand Distance Vector
CONFIDANT	Cooperation of Nodes- Fairness in Dynamic Adhoc Networks
PDF	Packet Dropping Fraction
NRL	Normalized Routing Load
PDR	Packet Dropping Ratio
SHA	Simple Hashing Algorithm
RREP	Route Reply
RREQ	Route Request
DPE	Data Packet Error
DOS	Denial of Service
PMOR	Packet Modification Ratio

PMIR	Packet Misroute Ratio
PDER	Packet delivery Ratio
SVM	Support Vector Machine
CoF	Conservation of Flow
EAACK	Enhanced Adaptive Acknowledgment
DSA	Digital Signature Algorithm
MRA	Misbehavior report authentication
BLM	Baseline Local Monitoring
SADEC	Stealthy Attacks in Wireless Adhoc Networks Detection and Countermeasures
Num	Number
Min	Minute
HMM	Hidden Markov Model
cs-HMM	Context-Sensitive Hidden Markov Model
SFAM	Selective Forwarding Attacks In MANET