INTRUSION DETECTION AGAINST DENIAL OF SERVICE ATTACKS IN MANET ENVIRONMENT

Anubha Dhaka
M.Tech (Computer Science)
I.F.T.M. University,Moradabad

Anurag Kumar
M.Tech (I.T.)
UGC-NET Qualified

Garima Chaudhry
B.Tech (Computer Science)
GATE-2012 & GATE-2013 Qualified

Surbhi madam
B.Tech (I.T.), NIIT
GATE-2013 Qualified

Abstract:
This paper provides a survey of possible solutions for intrusion detection system (IDS) against DoS attacks. In a Denial of Service (DoS) attack, legitimate users are prevented from access to services or network resources. Distributed DoS (DDoS) occurs if a group of attackers coordinate in DoS. When a DDoS attack occurs in a mobile ad hoc network (MANET), the attacker compromises a number of mobile nodes, which can follow different mobility patterns and have different speeds. Any node under attack in ad hoc network exhibits an anomalousbehavior called the malicious behavior. We first analyze the main vulnerabilities in
the mobile ad hoc networks. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.

Keywords - Mobile Ad Hoc Network, Security, Intrusion detection system,, Denial of service, Secure Routing

1- Introduction

Ad Hoc Network provides quick communication among nodes (like mobile or a laptop) to transfer the packets from one node to other. An example of an ad hoc network is given in figure 1 where nodes are communicating directly with each other. All the links
between nodes are wireless. Bluetooth [1] is a typical example of such networks. These networks are independent of any fixed infrastructure or central entity like cellular networks [2] which requires fixed infrastructure to operate. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.

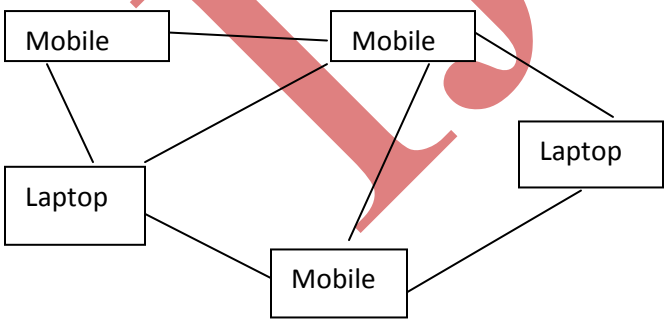


Fig 1: Example of Ad Hoc Network

Since mobile ad hoc networks (MANET) are autonomous, self-configuring, infrastructure-less distributed systems, these networks are extremely susceptible to large range of security challenges. The increased instances of security threats and attacks have brought the need of providing different defense measures, which unfortunately cannot eliminate all possible intrusions, but can reduce their success probability.

2- MANET Features

The mobile ad hoc network has the following typical features:

- Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

- Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

- Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.The objective of this paper is to find methods of intrusion detection.

3- MANET Vulnerabilities

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

3.1 Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

3.2 Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3.3 Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

3.4 Cooperativeness: Routing algorithm for MANETs usually assumesthatnodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

3.5 Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

3.6 Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited.

3.7Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

4- Security Criteria

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

4.1. Availability

The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it .

4.2.. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways :

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

4.3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

4.4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators . It is necessary for the communication participants to prove their identities as what they have claimed .

4.5.. Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need todiscriminate if a node with some abnormal behavior is compromised or not.

4.6.. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

5- Various Attacks in MANET

A- External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

B- Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

5.1 Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

5.2 Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

5.3 Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

5.4 Routing Attacks: The malicious node make routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

5.5 Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

5.6 Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

5.7. Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

5.8Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

5.9 Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability

6- An overview of DoS attacks in MANET

DoS attacks can be launched in two basic forms: software exploit and flooding, as illustrated in Figure below. In the case of the **software exploits attack**, the attacker node will send few packets to exercise specific software bugs within the target node application, disabling this way the victim. They can usually be addressed by adequate software fixes. Flooding tends to inject a large amount of junk packets into the network. Flooding attacks are further classified to single (DoS) and multisource (DDoS).

DDoS attack is typically performed by means of zombies or reflectors. A **zombie is** a node compromised by a cracker, computer virus or Trojan horse worm, and is intended to be used to perform malicious tasks in network or system that belongs to. There are generally four extensive categories of defense against
DoS attacks: (1) attack prevention, (2) attack detection, (3) attack source identification,
and (4) attack reaction.

Attack prevention aims to stop attack before it can reach the target. For example, it may refer to filtering spoofed packets close to or at the attack sources. In that
case, one of the most important tasks is to efficiently specify a filtering rule for differentiating accurately legitimate traffic from spoofed.

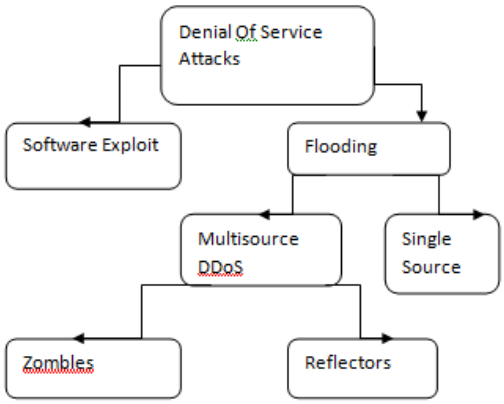


Figure 1. A basic DoS attacks taxonomy .

Attack detection aims to detect DoS attack when it occurs, which precedes any further action. The efficiency of DoS attack specific detection mechanisms can be evaluated in terms of their assumption strength and technical complexity.

Attack source identification intends to locate the attack sources regardless of whether the source address field in each packet contains erroneous information. The main feature of majority DoS source identification techniques is based on applying traceability, and dealing with the widespread problem of IP address forging by attackers.

Attack reaction tries to eliminate or limit the effects of an attack. It is the final step in defending against attacks, and therefore determines the overall performance of the defense mechanism. The challenge for attack reaction is how to filter the attack traffic without disturbing legitimate traffic.

7- Defining Normal and Malicious Behaviour of a Node

The vulnerabilities discussed in previous section provide intruder a way to compromise legitimate nodes and make them malicious in nature. In this section, an attempt has been made to define a normal and malicious behavior of a node. First of all, normal behavior of a node is defined and then malicious behavior.

6.1. Normal Behavior – "When any operation is performed in an adhoc network (for example-all the packets from source node (S) to destination node (D) is delivered) while maintaining the security principles (Confidentiality(C), Integrity (I), Availability (Av),
Authenticity (Au) and Non-Repudiation (NR)), then it is called the normal behavior of a node."

6.2. Malicious Behavior- "When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior:

Packet Drop- Simply consumes or drops the packet and does not forward it.

Battery Drained- A malicious node can waste the battery by performing unnecessarily operations.

Buffer Overflow- A node under attack can fill the buffer with fake updates so that genuine updates cannot be stored further.

Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering- A malicious node can enter in the network without authentication.

Stale Packets- This means to inject stale packets into the network to create confusion in the network.

Delay- Any malicious node can purposely delay the packet forward to it.

Node Not Available- An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.

Stealing Information- Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.

Session Capturing- When two legitimate nodes communicate, a malicious node can capture their session so as to take some meaningful information.

Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Message Tampering- A malicious node can tamper the content of the packets.

Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes.

Others- There are other ways also in which a node behaves in a malicious manner.

The normal and the malicious behavior of a node described above can be easily understood by the algorithm below.

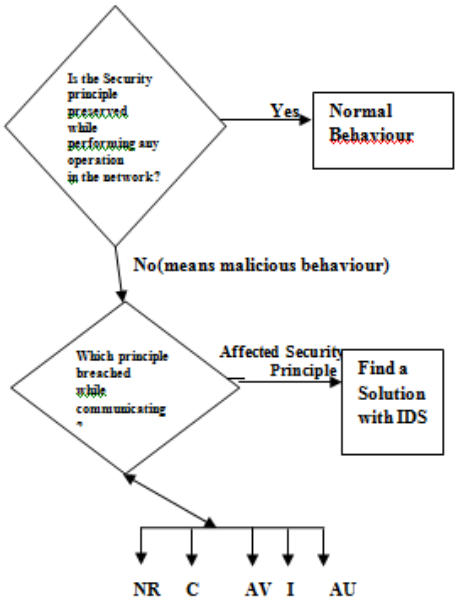


Fig.3. Defined Algorithm for Intrusion Detection system to find Normal & Malicious Behavior of a Node

8.Security Solution to Defend Malicious Behavior

In order to defend the malicious behavior which is defined in previous section, there are several security solutions which are used in ad hoc networks. Security can be provided through the methods of Cryptography, Protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP) which are discussed below.

7.1 Security through Cryptography-

In Ad Hoc Network, the data is sent using cryptography .Cryptography means to convert (or encrypt) the original data(which is to be send) into the unreadable format. Even if the intruder accesses the data, it should not be able to understand the content of it. Cryptography can be symmetric (which uses same key to encrypt and decrypt the data) and asymmetric (which uses one key to encrypt and other to decrypt the data). This security
Preserves he integrity and confidentiality of data.
Techniques like MD5 (Message Digest 5), Digital Signature, SHA (Secure Hash Algorithm), MAC (Message Authentication Codes) are used to preserve the security principles.

7.2 Security through TTP (Trusted Third Party)-

This service comes in picture when the security to the nodes in ad hoc network is provided by the some third party which can be trusted. A common example can be Public Key infrastructure (PKI) in which a trusted third party like Certifying Authority (CA) issues a certificate to the legitimate nodes for authenticating them. This preserves authentication security principle.Another example can be a watchdog node [7] which monitors all the nodes for availability. This node checks the packet forwarding from source node to intermediate node and then to destination node. A Random Walker Detector (RWD) [8] also monitors the node's activity to check whether a node is under attack or not.

7.3 Security through IDS (Intrusion Detection Systems)-

Intrusion Detection System [9][10] in ad hoc network monitors the node for malicious behavior. Anomaly based IDS is used in such process where any anomaly in the network confirms an attack. Profiles are maintained in the database of IDS which is the normal behavior of a node. These profiles are made under training period. Such profiles can either be static or dynamic in nature.
IDS can be designed inside the node or can even work as TTP.

7.4 Security through Secure Protocols-

In recent research, many secure protocols have been proposed which are intended to provide security to the network. Protocols like SEAD (Secure Efficient Ad Hoc Distance Vector Routing Protocol) , SAR (Secure-Aware Ad Hoc Routing protocol) , ARAN (Authenticated Routing for Ad Hoc Networks) , ES-AODV (Efficient Security Ad-Hoc On-Demand Distance Vector) [14] are the example of secure protocols. These protocols are designed with the concept of certification system, cryptography and other security solutions. It is possible that MN moves to a NR which resides on the current path. In this case, NR merely changes the MN's location information in its cache or database without establishing the tunnel to the former MR. However, it needs to keep track this MN in order to send updates towards itsoriginator as described above.

8- Intrusion detection techniques against DDoS attacks

If one were given all events in a MANET like nodes joining/leaving, route requests/replies, amount of errors, packets and data etc. then an observable pattern of normal net operation as well as other observable patterns for various anormalities and attacks might be assumed. It is suggested that every node runs an intrusion detection agent that collects network events, analyses them, shares its data with other nodes' agents, and derives appropriate responses to detected attacks .

First the system has to be trained with data from normal network operation. From then on the collected data is analyzed by calculating the information-theoretic entropy and conditional entropy. If the conditional entropy from recent measurements differ from the previously trained values then an abnormality is detected and a reaction can be initiated.

Once a local abnormality is detected it should be passed to neighbouring nodes. By exchanging their data the mobile IDS agents should be able to detect abnormalities more accurately and to initiate not only local but a global reaction (e. g. excluding a malicious node from the MANET).

An intrusion represents a set of actions that promises confidentiality, availability, and integrity of a system. The IDS mission is to provide a specific security technology against certain threat by identifying potential intruders and proceed with adequate procedure of blocking, denouncing and excluding them from the network.IDS performance is mainly evaluated through the following two metrics:

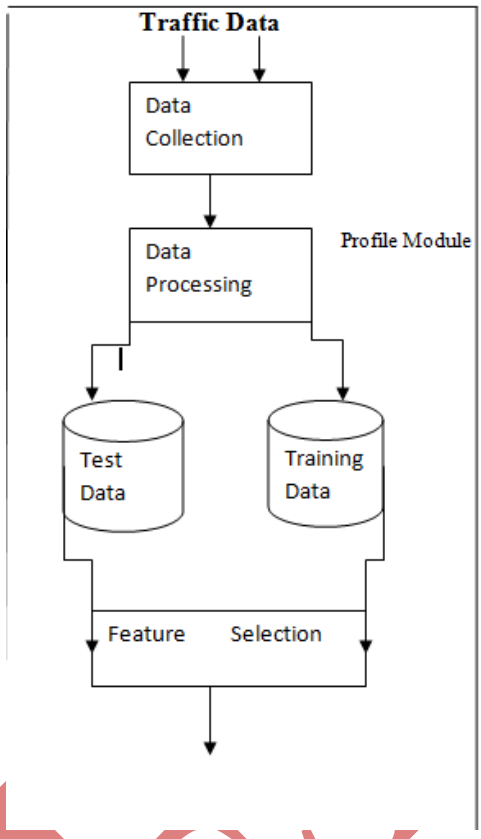
- **detection scheme coverage and**
- **false positives**.

Coverage represents a proportion of actual attacks that can be detected. Actually, it is a measure of IDS etection effectiveness. In the case of DoS attacks this is relatively easy to measure, as this type of attacks expose themselves with obvious degradation of target's services (e.g. high packet drop rate), though they can be easily detected. **False positive** is each event in the network that is, by mistake, reported as malicious**.** Usually, this metric is represented as value obtained by normalizing number of reported false positives versus the number of reported attacks. According to this, the perfect IDS will have the *coverage* of 100% and 0% *false positives*. In addition to these two metrics, the **intrusion detection time** should be as short as possible.hidden nodes.

The main task of the intrusion detection system (IDS) is to discover the intrusion from the network packet data or system audit data. One of the major problems that the IDS might face is that the packet data or system audit data could be overwhelming. Some of the features of audit data may be redundant or contribute little to the detection process. So the reduction in the size of data set is needed. To perform the reduction, two methods of feature selection, namely, markov blanket discovery and genetic algorithm are proposed.

The Intrusion Detection System is distributed in nature so each node of a mobile ad hoc network equipped with an IDS. System architecture of IDS comprises four components:
Data collection module
Profile module
Feature selection module
Intrusion Detection and Response module

8.1. Data collection module
The module collects audit data for each node. The proposed system considers unknown attacks. So the IDS need normal behavior of the system (normal profile) and violation of normal behavior (attack profile). Normal profile is created using the data collected during the normal scenario. Attack profile is created by simulating the attacks.



8.2. Profile module

In this module audit data is transformed into appropriate format for the detection process. From the attack data, training data set is created to train the bayesian classifier. Training data consists of labeling of events whether it is a normal event or an attack. Test data is collected under simulated attack environment and it is given to the bayesian classifier to identify an event whether it is an attack or normal.

8.3. Feature selection module

Feature selection is the process of selecting important features from the large data set. The selected features are relevant to the detection process. In order to perform this operation the following feature selection method is proposed. GA-based Feature selection algorithm is based on the wrapper model. In the adapted algorithm, the search component is a GA and the evaluation component is a bayesian network.The initial population is randomly generated. Every individual of the population is represented by means of genes, each of which represents a feature. If the feature value is '1', it is used during constructing of bayesian network if it is '0' that feature is not used.

8.3.1. Random population:

In Genetic feature selection the initial population is randomly generated. Each feature of a data set is represented in the form of gene and each record of a data set is represented in the form of chromosome. Each individual of a population consists of string of 1's and 0's.

8.3.2. Bayesian constructor:
Bayesian network is constructed by using the selected features. It is trained by using training data. Training data consists of normal and intrusive events with labels. Each label is used to identify whether the particular event is normal or an attack.

8.3.3. Bayesian Evaluator
Constructed bayesian network is evaluated by using validation data. Validation data is like training data. Resulting bayesian network is tested with nine validation data sets based on the labeling. Each validation data finds the classification error rates and it will be used during fitness computation.

8.4. Intrusion Detection and Response module
This module detects deviation from the norm. In order to detect the anomalies Bayesian classifier is used. Classifier will be trained by the training data. The test data will be given as input to the trained Bayesian classifier. Any deviation from the threshold level is considered level as anomalies. Once all the attacks are identified then the notification will be given to all the nodes in the ad hoc environment.

8.5. System Implementation
The IDS uses NS-2 simulator under LINUX environment for simulating the attacks in mobile ad hoc networks. The various parameters and its corresponding values of NS-2 simulation environment are given in table 4.1.AWK script is used for preprocessing the data sets.

9- Routing Protocols

Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as:

9.1. Proactive (Table-Driven): The pro-active routing protocols are the same as current Internet routing protocols such as the RIP(Routing Information Protocol), DV(distance-vector), OSPF (Open Shortest Path First) and link-state . They attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Some of the existing pro-active ad hoc routing protocols are: DSDV (Destination Sequenced Distance-Vector, 1994), WRP (Wireless Routing Protocol, 1996), CGSR (Cluster head Gateway Switch Routing, 1997), GSR (Global State Routing, 1998), FSR (Fisheye State Routing, 1999), HSR (Hierarchical State Routing, 1999), ZHLS (Zone based Hierarchical Link State,1999),STAR (Source Tree Adaptive Routing, 2000).

9.2. Reactive (Source-Initiated On-Demand Driven): These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Some of the existing re-active routing protocols are DSR (Dynamic Source Routing, 1996), ABR (Associativity Based Routing, 1996), TORA (Temporally-Ordered Routing Algorithm, 1997), SSR (Signal Stability Routing, 1997), PAR (Power-Aware Routing,1998), LAR (Location Aided Routing, 1998), CBR (Cluster Based Routing, 1999), AODV (ad hoc On-Demand Distance Vector Routing, 1999). In pro-active routing protocols, routes are always available (regardless of need), with the consumption of signaling traffic and power. On the other hand, being more efficient at signaling and power consumption, re-active protocols suffer longer delay while route discovery. Both categories of routing protocols have been improving g to be more scalable, secure, and to support higher quality of service**.**

9.3. Hybrid Protocols: Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing

protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay.

10- CONCLUSION AND FUTURE SCOPE

In this paper, normal and malicious behavior of nodes is defined.Security solution to defend such behavior is presented. Malicious behavior which is defined in section 6 cannot be confined to any number and depends on the operating environment and intruder's way to attack the network.

The future of ad- hoc networks is really appealing, giving the vision of ―anytime, anywhere‖ and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend in MANET is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad- hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen. We can say there will be more scope of MANET in coming generation.

REFERENCES

[1] B. Wu et al, ―A Survey of Attacks and Preventions in Mobile Ad Hoc Networks,‖ Wireless/Mobile Network Security, Springer, Vol 17, 2006.

[2 Trusted Computing Group, "Trusted Platform Module (TPM) Specifications," 2003. [Online]. Available: https://www.trustedcomputinggroup.org/specs/TPM

[3] A. H. M. Rezaul Karim et al**,** An efficient collaborative intrusion detection system for MANET using Bayesian Approach, Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems 2006,pp.187-190.

[4] Seddik-Ghaleb, A. Ghamri-Doudane, Y. Senouci, S.-M, "TCP WELCOME TCP variant for Wireless Environment, Link losses, and Congestion packet loss Models", IEEE Conferences on Communication systems and Networks, pp.1–8, Bangalore 2009.

[5] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Adhoc Networks", in Proceedings of the 6th International conference on mobile computing.

[6] Wei X, Chen G, Wan Y, Mtenzi F (2004) Optimized priority based energy efficient routing algorithm for mobile ad hoc networks. Ad Hoc Networks, Volume 2, Issue 3:231–239

[7] B. Sun, K. Wu, and U. Pooch. "Zone-based Intrusion Detection for Mobile Ad hoc Networks". Int. Journal of Ad Hoc and Sensor Wireless Networks, **2(3)**, 2003.