Methods For Detecting Attacks In Mobile/Wireless Ad-Hoc Networks: A Survey

Wellington Mapenduka

Abstract: Use of Mobile/Wireless ad hoc networks (MANET) is growing mostly in situations there is need for temporary data exchange such as in emergency services, conference meetings, virtual classrooms due to their low cost and easy in setting up, since they are infrastructure-less. However none existence of centralized administration of standard support services, dynamic topology, and air interface makes them highly vulnerable to attacks. The autonomous nature of the network results in security solutions being implemented mainly at the nodes, which are resource constrained i.e. limited computing power and memory, low bandwidth, and low battery life, thereby limiting the tightness of these solutions. It is extremely important to have flexible and robust methods of detecting attacks and their sources looking at the diversity of MANET application areas, so that appropriate countermeasures can be put in place. Detection based schemes can be incorporated to complement prevention techniques implemented in the network protocols. These methods should work through the whole protocol stack since attacks target specific layers. This paper discusses MANET attacks detection methods that are currently in use taking note of their performance. In the paper we also suggest a hybrid cross layer approach capable of detecting more than one known and new attacks, which can be researched on to complement existing methods in building effective security solutions for MANET.

Keywords: Ad hoc, autonomous, attack, detection, intrusion, MANET, vulnerability.

1 Introduction

Wireless ad-hoc network is becoming one of the highly active and dynamic field of communication and networks because of fame of movable devices and wireless networks that has increased significantly in recent years [1]. Wide use of handheld devices such as smartphones, tablet computers, PDAs, mobile internet devices and many others which are equipped with wireless network connection technologies has resulted in growth in the application of MANET in education, health, business, emergency situation management, environmental monitoring, and military surveillance and so on. With advantages such as easy installation, infrastructure-less, flexibility and scalability, the popularity of MANET has been on an upward trend. However the autonomic nature of the network nodes, air interface, multi-hop environment, limited bandwidth, computing power constraints and lack of a clear central line of defence presents challenges in securing such networks. These challenges in MANET bring about security vulnerabilities that are taken advantage of by attacks which target different layers of the network protocol i.e. application, transport, network, link, and physical layers. The attacks can be broadly classified as passive (e.g. eavesdropping, traffic analysis) and active (e.g. jamming, worm-hole, grey hole, replay attack). These attacks can also be viewed as internal (e.g. compromised node that is part of network) or external (coming from a node which is not part of network). Classification of different attacks on MANETs in accordance with network protocol stack as articulated in [2] is as shown in below:

Table 1:

Layer	Attack	
	Active	**Passive**
Application	DoS attack, Malicious code injection, Repudiation attack.	
Transport	Session hijack attack, TCP Syn attack, Jelly Fish attack.	
Network	IP Spoofing attack, Sybil attack, Sleep deprivation attack, Packet dropping attack, Impersonation attack, Man-in-the-middle attack, Flooding attack, Puppet attack, Black Hole attack, Gray Hole attack, Wormhole attack, Replay attack, Routing Tables attacks, DoS attacks etc.	Location disclosure attack
Data link	DoS attacks	Eavesdropping, traffic analysis and monitoring
Physical	Interference attack and Jamming attack	Eavesdropping, traffic analysis and monitoring

A number of intrusion prevention techniques are used to deal with these attacks, such as authentication and redundant transmission, and these need to be complemented by detection techniques to monitor security status of these networks and identify malicious behaviour of any participating nodes [3]. Detection methods monitor and recognises abnormal activities that attempt to compromise the integrity, confidentiality or availability of resources of a system and pass a trigger to a prevention solution in the system. The following are some of the rules as detailed in [4] used to monitor and recognise attacks;

- Interval rule: time interval between arrivals of two consecutive messages must be within acceptable limits because the intruder may increase the message sending ratio to exhaust the network resources. Helps in detecting denial of service (DoS) attacks.
- Retransmission rule: Each node monitors the behaviour of its neighbour nodes and calculates the number of packets successfully forwarded by them. This rule helps in detecting the black hole, sinkhole, and selective forwarding attacks.

- *Department of Computer Science, Bindura University of Science Education, Bindura, Zimbabwe*
- *Emails:* wmapenduka@buse.ac.zw, mapendukawelly@gmail.com

- Integrity Rule: The originality of the content of the message remains the same along the route from sender to destination, beside a number of retransmission by the intermediate nodes. This rule helps in detecting the modification attack.
- Delay Rule: The delay in relaying a message via intermediate nodes. This rule helps in detecting the jellyfish delay variance attack.
- Repetition Rule: The number of times, a message with same ID can be retransmitted from the same node. This rule helps in detecting the DoS attacks and packet replay attack.
- Radio Transmission Range: The messages should not be fabricated by the intermediate nodes. This rule helps in detecting the fabrication and wormhole attacks.
- Jamming Rule: The number of collisions associated with a packet transmission must be within acceptable limits. This rule helps in detecting the interference and jamming attack.

This paper makes a survey of detection methods looking at how they monitor and recognise attacks at different layers of the network protocol stack of MANETs, analyse their performance and makes suggestions on cross layer approach capable of detecting known and new attacks across the whole protocol stack, which can be researched on to complement existing ones with the aim of improved security in MANETs. This paper is divided into five sections which proceeds as follows: Section II explores the common attacks on MANETs, explaining their characteristics and effects on network performance. Section III makes a survey of the detection methods or techniques used in MANETs. Section IV gives an outline of suggested research in improved attack detection methods that can be used in MANETs. Finally Section V gives a conclusion on the current status and the future work in attack detection methods.

2 Exploring Manet Attacks

Attacks in MANETs are broadly classified as passive i.e. attacks that do not affect the operation of the network (e.g. eavesdropping and traffic analysis) and active i.e. attacks that disturb the operation of the network (e.g. worm hole, sink hole, replay and jamming attacks). These attacks can be further viewed as internal or external depending on whether the source of attack is a compromised node that is part of the network or node outside the network respectively. In exploring these attacks we group them according to the layer of the network protocol stack which they target, starting form higher layers as follows:

2.1 Application layer attacks

As the highest layer in the protocol stack, it contains user data that support many protocols such as HTTP, FTP, SMTP, POP3, which have multiple vulnerabilities and points of attack. The following are some of the set of attacks that target the highest layer of the protocol stack:

2.1.1Malicious code injection: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. Malicious hackers (crackers) frequently used snooping to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions [5]. Some of these attacks mostly seek the specific information on the legitimate node and sent information to malicious node which will be used to collect personal information and specifics information to attack on other nodes [6].

2.1.2Nonrepudiation attack: due to repudiation attack deny of participation is happened in whole communication, or in part of communication [7]. This attack compromises the ability of the network to ensure that the origin of the message cannot later deny sending and receiver cannot deny receiving.

2.2 Transport layer attacks

The transport layer in MANET is based on the Transmission Control Protocol (TCP) which is an end to end protocol. Attacks at this layer disrupt TCP connection which is established for communication between two ends. Some of the attacks that target the transport layer are discussed below:

2.2.1TCP Syn attack: is a Denial of Service (DoS) attack in nature, so the legitimate user does not get the service of the network when the attack happens. TCP Syn attack is performed by creating a large number of halt in opened TCP connection with a target node [7]. When the malicious node sends SYN by spoofing the IP address of the client, the server responds to it by a SYN ACK. The malicious node will not respond to it by the final acknowledgement. As the client's address is spoofed the client also does not respond by a final ACK. The connection remains half open. The malicious node sends a lot of SYNs and the server acknowledges to it .The server starts maintaining information in the buffer. At one point the buffer becomes full; all the resources of the client are occupied. The server cannot consider the further legitimate requests [8].

2.2.2Jelly Fish (JF) attack: the JF attacker disrupts the TCP connection which is established for communication. JF attacker intrudes into forwarding group and delays data packets for some amount of time before forwarding them. Due to JF attack high end to end delay is introduced resulting in poor performance of the network. JF attacker disrupts the whole functionality of TCP. It is the same as Black hole attack but the difference is that the Black hole node attacker drops all the data packets but the JF attacker node produces delay during forwarding packets [9].

2.2.3Session Hijack attack: one of the attacks which severely affect the MANET is the session hijack attack. It occurs by hijacking the session established between the source and destination. When the valid session is exploited, the unauthorised access gain the highly valuable and confidential information from these session [10].

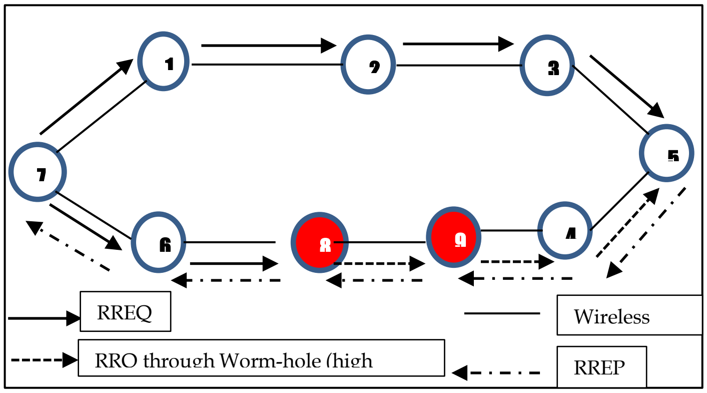
2.3 Network layer attacks

Route discovery and forwarding operations in the network can be disturbed or performed by malicious nodes in case of attack. This will solely disturb the network operation from correct delivering of packets, like the malicious nodes can give stale routing updates or drop all the packets through them. Below we describe some of the attacks at the network layer:

2.3.1Worm hole attack: a wormhole attack is one of the most sophisticated and severe attacks in MANET. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality making it difficult to detect [7].

Below is an illustration of a worm-hole attack.

Figure 1:



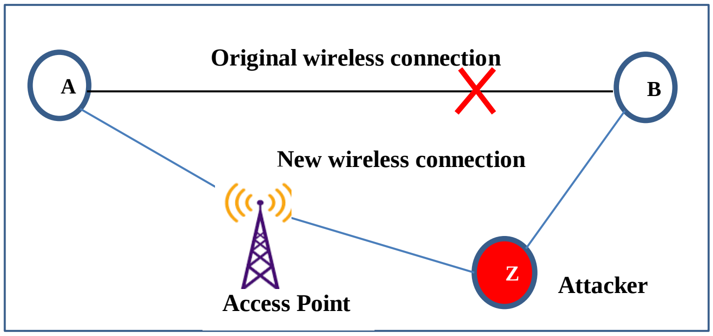
Node 7 sends a route request (RREQ) to discover a route to node 5 which it intends to communicate with. The path through two colluding malicious nodes 8 and 9 reaches the destination first due to a high speed link between the two. Route reply (RREP) packet is send back to node 5 and it takes the link as the best option for communicating with node 5. The malicious nodes then records packets transmitted between node 7 and 5. The packets are then replayed at another location disrupting genuine communication in the network.

2.3.2Black hole attack: A single black hole attack can easily happen in a mobile ad hoc network when an intruder utilize the loop hole to carry out their malicious behaviors because the route discovery process is necessary and inevitable [11]. An attacker node sends fake routing information in the network to claims that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example in an Ad-Hoc on demand distance vector routing (AODV), attacker can send fake RREQs including a fake destination sequence number that is fabricated to be equal or higher than the one contain in the RREQ to source node, claiming that it has a sufficient fresh route to the destination node. This causes the source node to select the route that passes through the attacker node. Therefore all the traffic will be routed through the attacker and therefore, the attacker can misuse the information or sometime discard the traffic [7].

2.3.3Gray hole: In Gray Hole Attack a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination [7].

2.3.4Man in the Middle attack: An attacker eavesdrop on communication taking place between two target nodes. The attack takes place in between two legitimately communicating nodes, allowing the attacker to listen to a conversation they should normally not be able to listen to. The sniffed traffic is recorded and can be replayed on another part of the network later disrupting legitimate communication by competing for bandwidth and straining energy. Figure 2 below illustrates an example of man in the middle attack:

Figure 2:



Man in the middle attacks can be executed in the following ways: Rogue access point: Wireless devices equipped with wireless cards will often try to auto connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. ARP spoofing: ARP is the Address Resolution Protocol used to resolve IP addresses to physical MAC (media access control) in a local area network. An attacker wishing to pose as another host could respond to requests it should not be responding to with its own MAC address. With some precisely placed packets, an attacker can sniff the private traffic between two hosts. DNS spoofing: When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name. This leads to the victim sending sensitive information to malicious host, with the belief they are sending information to a trusted source. Man in the middle attack uses techniques such as sniffing, packet injection, session hijacking and SSL stripping.

2.3.5Flooding attack: Flooding attack is one of the forms of DDoS attack whereby certain nodes in the network miss-utilizes the allocated channel by flooding packets with very high packet rate to its neighbours, causing a fast energy loss to the neighbours and causing other legitimate nodes a denial of routing and transmission services from these nodes. Flooder node receives the RREQ and it will generate the RREP with higher sequence number so source node assumes that it has the path for destination node. Flooding attacks main aim is to consume the power in terms of battery power and bandwidth. It will cause some issues regarding the network performance. Flooding attack leads to the degradation in terms of result of throughput, exhaustion of battery power and wastage of bandwidth [12]. There are mainly three types of flooding attack.

RREQ flooding: In this type of attack, the flooder node broadcast several RREQ packets for the node which exist or not exist in the network. To complete RREQ flooding the attacker deactivate the RREQ rate so it will consumes network bandwidth [13].

Data flooding: In this type of attack, data packets are used to flood the whole network. The attacker or flooder node, construct a route towards all the node then send the huge quantity of fake data packet and this bogus data packet fail the network resources so it will be hard to detect the flooder node [13].

Syn flooding: In syn flooding attack, attacker or flooder node sends a succession of synchronization packet to the destination node. Hence the large amount of memory will be consumed through this attack [13]

2.4 Data link layer attacks

The protocols used in link layer / MAC layer are susceptible to many DoS attacks. MAC layer attacks can be classified as to what effect it has on the state of the network as a whole. The effects can be measured in terms of route discovery failure, energy consumption, link breakage, initiating route discovery and so on. The misbehaviour of a node can be either selfish or of malicious nature. What follows is a discussion on some of the attacks on the data link layer [14]:

2.4.1Traffic monitoring and analysis: In this type of attack the adversaries analyse the traffic patterns to gain important information on network topology that in turn reveals the information about the nodes. Information such as location of nodes, network topology used to communicate and roles played by the nodes can be gathered [14]. This attack is some kind of a passive attack however the gathered information could be used later to perform malicious activities in the network by an intruder.

2.4.2Selfish misbehavior of nodes: These are selfish nodes that either deny forwarding the packets or drop the packets intentionally in order to conserve battery power or gains unwanted share of bandwidth. Packet dropping is one of the major attacks by selfish node which causes congestion in network. These attacks exploit the routing protocol to their own advantage because most of the routing protocols have no mechanism to detect whether the packets are being forwarded or not except the Dynamic Source Routing protocol [14].

2.5 Physical layer attacks

These attacks are hardware based and require assistance from hardware sources to occur. The execution of these attacks is simple as we do not require in-depth knowledge about the technology being used [14]. Some physical layer attacks are discussed below:

2.5.1Eavesdropping: It is defined as interception and reading of messages and conversations by unintended receivers. As the medium is wireless anyone within the radio range and receiver tuned to the proper frequency can listen to the ongoing communication. The main goal of this attack is to gain access to the confidential information transmitted such as private key, public key or node passwords [14].

2.5.2Jamming: is a special class of DoS attacks which are caused by a compromised node after learning the frequency of communication. The jammer transmits signals with security threats and also prevents receiving the legitimate packets [14].

2.5.3Interference: An Active Interference is a Denial of Service attack which blocks the wireless communication channel. The effect of this attack depends on the routing protocol used and the duration of it. The intruder can reorder the messages or replay the old messages [14].

3 Discussion on Attack Detection Methods

Implementation of attack detection methods ensure that the security mechanism in the ad hoc mobile wireless network can monitor and recognises abnormal activities that attempt to compromise the integrity, confidentiality or availability of resources of a system and pass a trigger to a prevention solution in the system. Detection complements or is an important component of every prevention solution. Having an effective detection component plays a critical role in realising a robust security solution in MANETs. Most methods target specific types of attacks and using a combination of these makes the security solution achieve more in terms of recognizing the attacks as they surface in the MANET. In this discussion we make review of some of the methods that are used to detect attacks and analyse their performance.

3.1 Statistical analysis approach

In this approach, analysis of the MANET behaviour and performance is done using statistical models that work with network metrics i.e. average route discovery time, packet delivery rate, throughput of the network, packet drop ratio etc. Below are some of statistical based algorithms used for attack detection.

Statistical Process Control (SPC)

The design of MNET is characterized by its vulnerability to denial of services attacks (DoS). Application of statistical process control (SPC) to detect jamming or interference attack is suggested in [15] that works with the packet drop ratio (PDR) which refers to the number of packets dropped to the packets sent. The PDR is assimilated to the fraction nonconforming. The basis of this detection method is the supervision of the packet drop ratio by two limits in a graph. These graphs are called control charts. The detection of deviation is one of the basic principle of this control. The SPC method provides a strong tool to separate the ordinary from the extraordinary by plotting powerful control charts.

The control chart for fraction nonconforming

The fraction nonconforming is defined as the ration of the number of nonconforming items in a population to the number of items in that population and usually expressed as a decimal. The base of the control chart for fraction nonconforming is the binomial distribution.

The average of fraction of nonconforming is expressed by:

$$\overline{p} = \frac{\sum_{i=1}^{m} D_i}{mn} \quad (1)$$

Where m is the number of samples, n is the sample size and Di is the number of nonconforming in the sample size n. The centre line (CL), the upper control limit (UCL) and the lower control limit (LCL) for fraction nonconforming are calculated as follows:

$$\mathrm{UCL} = \overline{p} + 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}} \quad (2)$$

$$\text{Centre line} = \overline{p} \quad (3)$$

$$\mathrm{LCL} = \overline{p} - 3\sqrt{\frac{\overline{p}(1-\overline{p})}{n}} \quad (4)$$

The metrics in (1), (2) and (3) are calculated based on collected statistical measure of PDR in normal case (without jamming). A minimum of 20 values is used in regard to the calculation of thresholds (control chart parameters).The calculated parameters (UCL, Centre line and LCL) on the chart. The PDR is monitored using the control chart for fraction nonconforming. If the curve oscillates on either side of the mean and that all points are inside the limits then our communication is under control and no jamming attack exits. If there has been a great deviation the network is under jamming attack. They are many benefits of the SPC identification scheme. In the scheme they is no need to make changes to the IEEE 802.11 protocol also, the identification scheme can be implemented at any diffusion node and the most important benefit is the identification of an identical attach in the guanine time by a visual graph. However the scheme is not broad enough to identify other attacks in the MANET and they is need to make an implementation of the identification strategy in a realistic situation. Wormhole attack detection using statistical analysis approach [16]. This approach detect wormhole in MANET by using average time delay to detect anomalies based on statistical information of packets in the networks. Three features of the network are monitored including: the number of incoming packets, the number of outgoing packets and the average route discovery time related to each node, throughput of the network, retransmission attempts and load on the network. The network is having wormhole if any abrupt change of one of these features is reported. The proposed wormhole detection model based on statistical analysis works without any extra hardware requirements, the basic idea behind this work is that the wormhole attack reduces the length of hops and data transmission delay.

The steps of the algorithm are as follows:

1. Randomly generate a number 0 to maximum number of nodes.
2. Make the node with same number as transmitter node.
3. Generate the route from selected transmitting node to destination node.
4. Start counter and send RREQ using reactive routing technique.
5. Receive the RREP packet from each path; associate it in route list with time delay.
6. Now calculate the average time delay.
7. Select the route within covariance range of average delay.
8. The routes that are not within the covariance range are black listed hence they are not involved in future routes discovery.
9. Whole process (from step 1 to step 8) is repeated for limited assumed time.

The statistical analysis approach is very useful if sufficient information about the routes is available from multi path routing and can detect the wormhole. Simulation results show that the algorithm is successful at detecting wormhole attacks and locating malicious nodes. The limitations of the approach are that; it does not specify how the sufficiency of information about the routes is determined, addresses only one attack and has no clear implementation strategy in realistic environments.

3.2 Graph based

These approaches make used of the graph theory to analyse the relationship between nodes in a MANET. Pair wise relationships are modelled using graph theory. A graph theory in this context is made up of nodes which are connected by edges that are links between nodes. Graph is and ordered pair $G = (V, E)$ consisting of a set of nodes 'V' and together with a set of edges 'E'. V is a set formed with a relation of incidence that associates with each of two vertices [17]. Typically in MANET, nodes and links between them fits well in the definition of a graph. Some methods that implement a graph framework in attack detection are explained.

Detection of DoS using graph theory [17].

The method I used for detecting DoS attack and has the following steps:

1. Let N be the total number of nodes and x be the number of DoS nodes. Let S be the source node.
2. Input values of N and x.
3. Randomly assign x nodes as DoS nodes among N nodes.
4. Initially topology control (TC) and HELLO messages are passed and multi point relay (MPR) chosen by the nodes. MID (Multiple Interface Declaration) are transmitted by nodes to get address of each node.
5. The node selects the shortest distance between itself and one of the destinations node. MPRs and hence the shortest path to the destination is found.
6. The MPR until the destination chosen may act as attacker by sending many HELLO messages. Based on the probability by HELLO message easily all nodes can detect attacker. Then the node is announced as attacker and node details are sent to each to eliminate that node.

7. The source node S forwards the packets to destination through the secured route.
8. Compute the performance metrics, namely, throughput, packet delivery ration, packet received, delay, jitter, good put, normalised overheads, dropping ratio.
9. Stop.

The algorithm does not increase computational complexity in nodes and is quite effective in detecting DoS attacks in MANET. However it is limited in terms of attack detection scope. A Graph-theoretic Algorithm for detection of multiple wormhole attacks [18]. The method works with an adjacency matrix and is most suitable for proactive protocols which maintain updated routing tables. The method implements the following steps:

1. Construct an adjacency matrix from the route table. This is a symmetric $n x n$ binary matrix where n is the total number of nodes in the ad hoc network.
2. Compute X2 =XxX where x is an ordinary matrix multiplication in the ring of integers. The value of off-diagonal entries in X2 gives the number of nodes that are common neighbours to both ith and jth nodes.
3. If all non-zero entries are examined in X, go to step 5. For every unexamined non-zero entries in X, if the corresponding value in X2, the ith and jth nodes are showing themselves as neighbours, but they do not have any common neighbours. Both of them may be possible adversary nodes in wormhole attack. For these entries do step 4.
4. Let the neighbours of i and j be denoted as set of nodes N and M respectively. An inequality [18] is used to check for existence of an attack.
5. Terminate the wormhole detection algorithm and inform the rest of neighbouring nodes about the possible wormhole attack. The neighbouring nodes will accept the finding based on the trust relationship they have with the detection node which has run the algorithm
   If symmetric links are assumed, the upper triangle of the matrix is sufficient to store all the neighbourhood information making the method effective in detecting wormhole attack. The methods is limited in the number of attacks it can detect and has no defined realistic situation implementation strategy.

3.3 Location Information based

In this approach the location of nodes plays an important role. Here they is also focus on the distance between nodes with respect to transmission rage. The location feature can be used in the detection of wormhole and link spoofing attacks. One way of implementing this approach is to equip each node in the network with a Global Positioning System (GPS) device. To reduce cost, some special nodes having GPS receiver can be deployed at specific locations in the network to get locations of neighbours nodes. The relative location information can also be collected by using special antennas, which are able to detect the direction from which data is received. The use of GPS device or special antenna will increase the cost of nodes and make the network expensive. This will also decrease the battery timing of mobile nodes [19].

3.4 Trust based

In MANET, each node not only works as a host but can also act as a router in multi hop communication. It is assumed that each node will be reliable, trustworthy and cooperative in routing of packets. Hence to detect the malicious nodes a trust value should be calculated for each and every node in the routing process. Trust values can be calculated for each and every node based on the ratio of number of packets dropped by number of packets forwarded by that neighbouring node. Then specific threshold value should be kept, to see the range of trust values. That is, if the trust value is less that the threshold value range then those nodes involving in the routing will be ignored. If the node's trust value exits below the specific range then those nodes will be considered as malicious nodes. When they is use of Dynamic Source Routing (DSR) protocol, based on the trust value the malicious node detected will be ignored in further routing strategy. The method improved the detection of malicious nodes in MANET. The trust value can be calculated as ratio of number of packets dropped by the number of packets to be forwarded which will improve the approach significantly. The approach can be improved by extending it to mitigate combined attacks [20].

3.5 Fuzzy based

Fuzzy logic uses various measures of number of packets dropped against various parameters. The fuzzy logic technique is very easy to implement and produce precise output by removing various ambiguities. They is use of a fuzzy inference system for making the fuzzy rules to take the decision. There are some parameters for checking the behaviour of node if it is malicious or not [20]. Fuzzy based detection approach has the following steps:

- Threshold evaluation
- Calculate fuzzy matrix
- Identify attack
- Notify the prevention mechanism

The approach can be used to effectively detect various attacks such as black hole attack, warm-hole attack and grey-hole attack. However it do not cover all features for data collection used in threshold evaluation [20].

4 Suggested Future Research

It has been noted that most methods can effectively detect one or a few attacks, this brings the need for other methods to be deployed in MANET to detect more attacks. This arrangement will strain the resources of nodes due to the number of methods that will require computational resources, memory and other resources. Some techniques only detect attack at specific layer of the node protocol stack. Future works should focus on coming up with a detection scheme that mitigate combined attacks. In this paper we suggest a hybrid cross layer based approach with a complete design and implementation strategy for working in realistic situations. This may involve building the detection strategy by combining as set of known working detection techniques into a hybrid technique that recognize attacks across the whole node protocol stack with little complexity. The attack detection scheme should recognize most if not all attacks in MANET without adding complexity in nodes.

5 Conclusion

This research clearly outlines attacks in MANET in accordance with network protocol stack, indicating whether they are passive or active. Importantly it makes a survey of methods used to monitor and recognizes abnormal activities that attempt to compromise the integrity, confidentiality or availability of resources of a system and pass a trigger to a prevention solution in MANET. A closer look has been made on statistical based, graph based, location information based, trust based and fuzzy based approaches in intrusion detection. A discussion on these approaches is made outlining how detection is implemented, advantages and their limitations. These methods have been noted to be effective in recognizing specific type of attack, for example; the wormhole attack using graph based approach.

REFERENCES

[1] N. Raza, M.U. Aftab, M.Q Akbar, O. Ashraf, and M. Irfan, ”Mobile Ad-Hoc Networks Applications and Its Challenges,” Communications and Network, Vol 8, pp 131-136, (2016). http://dx.doi.org/10.4236/cn.2016.83013.

[2] S. Kumar and K. Dutta, “Intrusion Detection in Mobile Ad-Hoc Networks: Techniques, Systems and Future Challenges,” Wiley Online Library, Vol 9 Issue14, pp 2484-2556. http://doi.org/10.1002/sec1434 (2010).

[3] S. Kaushal and R. Aggarwal, “A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack,” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4 Issue 2, February 2015.

[4] APR. da Silva, MH. Martins, BP Rocha, AA Loureiro, LB Ruiz, and HC Wong, “Decentralized intrusion detection in wireless sensor networks,” In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Quebec, Canada, pp 16-23, October 2005.

[5] R. Verma, and M. Mannan, “A Review on Various Approaches for Attack Detection in MANET,” International Journal of Science and Research (IJSR), Vol 5, Issue 1, pp 873-876, January 2016.

[6] A.M. Holkar, N.S. Holkar, and D. Nitnawwre, “Investigative analysis of repudiation attack on MANET with different routing protocols,” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, pp 356-359, May – June 2013.

[7] M. Seyyedtaj and M.A.J. Jamali, “Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network,” International Journal of Computer Applications Technology and Research, Volume 3– Issue 9, pp 541 - 546, 2014.

[8] K. Geetha, “SYN Flooding Attacks in Mobile Ad hoc Networks,” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4), pp 5033-5037, 2014.

[9] C. Gupta1 , P. Singh, and R. Tiwari, “Network and Transport Layer Attacks in Ad-hoc Network,” International Journal of Advanced Research in Computer and Communication Engineering: ICACTRP 2017, Noida Institute of Engineering & Technology, Greater Noida Vol. 6, Special Issue 2, February 2017.

[10] K. Geetha and N. Sreenath, “Mitigation of session hijacking in mobile ad hoc networks,” International Journal of Applied Engineering Research, Vol 10(14), pp 34281-34287, January 2015.

[11] F. Tseng, L. Chou and H Chao, “A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks,” Human-centric Computing and Information Sciences, https://doi.org/10.1186/2192-1962-1-4, November 2011.

[12] S.Bhalodiya, and K. Vaghela, “Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol,” International Journal of Computer Applications (0975 – 8887), Volume 125 – No.4, September 2015.

[13] R Meher and S Ladhe, ”Review Paper on Flooding Attack in MANET,” International Journal of Engineering Research and Applications, pp. 39- 46, January 2014.

[14] S.R. Venna1, and R.B. Inampudi, “A Survey on Security Attacks in Mobile Ad Hoc Networks,” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1), pp. 135-140, 2016.

[15] M El Houssaini, A Aarouda, A El Horea, and J Ben-Othman, “Detection of Jamming Attacks in Mobile Ad Hoc Networks using Statistical Process Control,” The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016), Procedia Computer Science 83 (2016) pp 26 – 33.

[16] S Upadhyay and A Bajpai, “Avoiding Wormhole Attack in MANET using Statistical Analysis Approach,” International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.1, pp 15-23, March 2012.

[17] AT Preeti, “Exclusion of Denial of Service Attack using Graph Theory in MANETS,” International Research Journal of Engineering and Technology (IRJET), Volume (04) Issue (07), pp 3394-3399, July -2017.

[18] R Venkataraman, M. Pushpalatha, TR Rao and R Khemka, “A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks,” International Journal of Recent Trends in Engineering, Vol. 1, No. 2, pp 220-222, May 2009.

[19] M Imrana, FA Khanb, T Jamala and MH Durada, “Analysis of Detection Features for Wormhole Attacks in MANETs,” International Workshop on Cyber Security and Digital Investigation (CSDI 2015), pp 384 – 390, Procedia Computer Science 56 (2015).

[20] M Nachammai and N. Radha, “An Improved Trust Based Approach For Detecting Malicious Nodes in MANET,” International Journal of Computer Trends and Technology (IJCTT), Volume 41 Number 1, pp 54-58, November 2016.