Journal of Computer and Communications, 2015, 3, 41-66
Published Online December 2015 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2015.312005

Security: A Core Issue in Mobile *Ad hoc* Networks

Asif Shabbir[1], Fayyaz Khalid[1], Syed Muqsit Shaheed[2], Jalil Abbas[3*], M. Zia-Ul-Haq[3]

[1]Department of Computer Science, University of Gujrat, Gujrat, Pakistan
[2]Department of Computer Science, University of Lahore, Lahore, Pakistan
[3]Department of Computer Science& IT, Government Collage University Faisalabad (Layyah Campus), Layyah, Pakistan
Email: rabtabox4u@gmail.com, fayyazrao@yahoo.com, syedmuqsit@hotmail.com, *sjshah786@gmail.com, ziaulhaq.arain@gmail.com

Received 26 October 2015; accepted 6 December 2015; published 9 December 2015

Abstract

Computation is spanning from PC to Mobile devices. The Mobile *Ad hoc* Networks (MANETs) are optimal choice to accommodate this growing trend but there is a problem, security is the core issue. MANETs rely on wireless links for communication. Wireless networks are considered more exposed to security attacks as compared to wired networks, especially; MANETs are the soft target due to vulnerable in nature. Lack of infrastructure, open peer to peer connectivity, shared wireless medium, dynamic topology and scalability are the key characteristics of MANETs which make them ideal for security attacks. In this paper, we shall discuss in detail, what does security mean, why MANETs are more susceptible to security attacks than wired networks, taxonomy of network attacks and layer wise analysis of network attacks. Finally, we shall propose solutions to meet the security challenges, according to our framed security criteria.

Keywords

Mobile Devices, Optimal Choice, MANET Security, Wireless Network, Taxonomy, Intrusion Detection, Network Security Threats, Layer Wise Network, Vulnerabilities of Wireless, Security Criteria

1. Introduction

Nowadays, computing is the need of everyone, everywhere. Everyone is looking for on the spot handy computa-

[*]Corresponding author.

How to cite this paper: Shabbir, A., Khalid, F., Shaheed, S.M., Abbas, J. and Zia-Ul-Haq, M. (2015) Security: A Core Issue in Mobile *Ad hoc* Networks. *Journal of Computer and Communications*, **3**, 41-66. http://dx.doi.org/10.4236/jcc.2015.312005

tional solutions. In this need based scenario, advancement in Hardware Engineering made it possible, the invention of a number of mobile computing devices. PDA's, Pocket PC's and smart phones can be seen everywhere. In the last decade, the massive growth in mobile computing devices brought a revolutionary change in computing, the evolution of ubiquitous computing. At present, the concept of ubiquitous computing is a research hot spot in Computer Science society [1]. In ubiquitous computing environment, the individual users may retrieve information smoothly whenever and wherever they are by utilizing heterogeneous electronic platforms simultaneously [2].

MANETs are the best choice for practical implementation of the ubiquitous computing and wireless medium is a natural ally of MANETs for ubiquitous computing because wired link does not support heterogeneous devices, on demand connectivity and device mobility. There are numbers of practical applications of MANETs [3] such as:

- Personal area networks
- People sitting in airport lounge
- Kids playing in ground
- Rescue and emergency services
- Military movement on vehicles
- Healthcare services
- Stock market brokers

The word "MANET" is a self descriptive. It is a temporary wireless network of arbitrary self organized mobile nodes that is why it is viewed as Mobile *Ad hoc* Network [4].

MANET is an art of networking without formal networking which is quite easy to develop. In the infrastructure less network environment, there is no concept of node dominancy or centralized control. The nodes within the radio range of each other directly communicate with each other while the node(s) which are not in direct communication range, form a multi-hop communication environment, where intermediate nodes are used for multi-hop communication.

Multi-hop routing is the core of multi-hop communication. An efficient and power aware routing protocol with reduced traffic over head is required for this multi-hop routing [5]. Different routing protocols like Dynamic Source Routing (DSR) [6], *Ad hoc* On-Demand Distance Vector (AODV) [7], The Optimized Link State Routing (OLSR) [8] and Destination-Sequenced Distance-Vector (DSDV) [9] are available multi-hop routing.

Formation of the MANET is quite easy and interesting. Heterogeneous devices with varying capability and processing power are allowed to join the network, even at runtime. There is no specific topology and limit of nodes in a network. Nodes are free to join, leave and move with any mobility pattern, on the fly. Following are the typical key features of the MANETs [10] [11].

- Absence of Infrastructure
- Peer to peer connectivity/communication
- Dynamic topology
- Shared wireless medium
- Scalability

The above mentioned features make the MANETs highly susceptible to security attacks. In the section two of this paper we discuss in detail, what does security mean? In section three vulnerabilities of MANETs, in section four taxonomy of network attacks and in section five layer wise analyses of network attacks are discussed. We proposed some solutions to meet the security challenges in section six. At the end of the paper conclusion of our study and future research is given.

2. What Does Security Mean?

It is highly debatable that:

- What does security mean?
- Is there exists any safety measurement criteria?
- How to assess security state of mobile *ad hoc* network?

We must have to formulate some security criteria to answer the above said questions. Following are the guide lines to evaluate the security state of the MANETs.

2.1. Availability

Availability ensures the guaranteed access of all the services of the network, to all the privileged nodes, under any circumstances [10]. It is a challenging issue to provide the network services smoothly, especially, in the presence of selfish nodes and Compromised nodes and denial of service attacks.

2.2. Integrity

Integrity means a message will never altered or tampered after the transmission. At runtime a message could be truncated, replayed or even altered due to any malicious attack or even due to accidental hardware failure [12]. Integrity guarantees the protection of information against Malicious as well as Accidental altering.

2.3. Confidentiality

Confidentiality means the privacy of information. There should exist a mechanism to protect information from being exposed to unauthorized entities. Only privileged nodes should be given access to private information.

2.4. Authorization

In a network environment certain entities are assigned with specific credentials. These credentials define their privileges to access certain network services. Authorization enables the receivers to verify that message is from trusted entity. It is usually implemented via certificate or digital signature.

2.5. Authenticity

Authenticity means that both sender and receiver are genuine in nature, not the impersonate one [10]. There should be a mechanism like handshaking to verify that both the sender and receiver are legitimate to communicate.

2.6. Non Repudiation

Non repudiation means that the sender can't deny whatever it has transmitted and likewise receiver whatever it has received. They must own their mutual communication. It is necessary and helpful, especially, in tracking of compromised nodes in a network. If a node identifies erroneous messages it would alert other nodes with an evidence to be aware of expected abnormal behavior of that particular transmitter node.

2.7. Anonymity

The term anonymity is closely related to privacy. Anonymity demands that information about the ownership of current node should be kept private by the node itself as well as by the system software. It is the only way to protect a privacy of a node from being exposed to the other nodes.

3. Why MANETs Are More Exposed to Security Attacks

Wireless medium is considered more exposed to security attacks than wired links due to its vulnerabilities. Since Wireless medium is a backbone of the MANETs, therefore MANETs inherit all the features of wireless links. These inherited vulnerabilities of wireless medium make the MANETs highly vulnerable in nature and a hive for all season attacks. Let's discuss these vulnerabilities, one by one, in detail.

3.1. Transitive & Non Secure Boundary

Radio waves are transmitted in a broadcast fashion. During broadcast unguided signals spread all around and cover some specific elastic circular range. In that particular range, strength of the signal is primarily dependent upon the distance from the transmitter that is why there is no sharp boundary in wireless links [13] [14]. Since there is no sharp border line in Wireless links, therefore, they are considered more exposed to security attacks than wired links. Physical links are more secure because the malicious attack must have to pass through several lines of defense such as fire walls, gateways, routers and filters before reaching to target node [15]. MANETs are dependent upon Wireless medium for communication; therefore, it is quite easy to inject malicious code in MANETs in the absence of sharp boundary line of wireless links. There exists no safety mechanism against unauthorized network access due to mobile and *ad hoc* nature of MANETs. In the absence of the secure boundary different types of attacks may affect performance of the network *i.e*. passive eavesdropping, Active Interfering, exposure of secret information, data tempering and denial of service attacks [10].

3.2. Varying Strength of Signals

Varying strength of signals is another problem with wireless medium. Signal strength is mainly dependent on the transmitter, radio antenna and even on battery power at some extent. Signal strength is inversely proportional to the distance from the transmitter. Signals get weaken as the distance from the transmitter is increased. So on intermediate walls and building may also weaken the signals, considerably. Weak signals may leads to the unavailability of certain intermediate network nodes and ultimately the unavailability of certain network services. Varying strength of signals may cause QoS issues in network and even may generate the illusion of denial of service attacks.

3.3. Interference with External Signals

Since MANETs use wireless as a communication medium so it is highly susceptible to be attacked by external signal interference. External signal interference is, often seriously destructive and may tamper your vital information. It is also considered that external signal interference may leads to active interfering, data tampering and information leakage attacks.

3.4. Hidden Nodes and Signal Collision

In MANETs nodes flood packets in broadcast fashion. Only nodes within the specific radius of transmitter can detect the signals. This distance-dependent carrier sensing can generate a hidden/exposed node problem. The situation when a node receives the same packet from two different sources but the source nodes are hidden from each other is called a hidden node problem which leads to the signals collision [13]. As a result of collision loss of data occurs and ultimately there may generate illusion of denial of service attacks.

3.5. Lack of Infrastructure and Central Management

MANETs are infrastructure less networks hence the lack of central management is a major threat to MANET's security. There exists no network server in MANETs hence there is no centralized entity to impose network policies, trust management and authorization. In the absence of network infrastructure there is no incorporation of any security feature in MANETs. Due to the non incorporation of security features and heavy traffic flow, it is quite difficult to detect any malicious activity in highly dynamic networks like MANETs [16]. Some algorithms of MANETs are dependent upon mutual participation of nodes and require network infrastructure. In the absence of network infrastructure an adversary node may take the advantage of decentralization of MANET to break the cooperative algorithms [17].

3.6. Compromised Nodes

Wireless links make the MANETs a hot cake for security attacks. The attacker takes the advantage of vulnerable nature of MANETs and launches a compromised node inside the network. A compromised node is an adverse node inside networks that has been captured by any unfair means and executes the further malicious activities in the network. Then it is easier for the attacker to employ a compromised node inside the network to get access and control the ongoing communication [18] [19].

3.7. Adaptive Routing Protocols

Instead of designing specialized routing protocols Many of MANET routing protocols are borrowed from wireless routing protocols, which were designed and configured for static wireless environment. Mobility is the key feature of MANETs hence statically configured routing protocols are not capable to handle the security threats, caused of mobility. There are required special secure versions of the protocols to protect MANETs from security attacks. Different secure versions of protocols are recommended such as sDSR, sAODV, sOLSR and sDSDV are the secure versions of DSR, AODV, OLSR and DSDV protocols respectively.

3.8. Shared Bandwidth

Wired links always provide a better bandwidth than wireless links because they transmit data over confined physical lines. In wireless communication, radio channels are shared among many users. Wireless communication is taken place in broadcast manner hence a lot of bandwidth is shared and consumed during the broadcasting of the wireless signals. Periodic hello messages for neighbor sensing might also utilize a lot of bandwidth which ultimately leads to network overhead. Shared bandwidth is the major drawback of wireless medium that limits the data transfer rate, quality of service and successful delivery of packets. The attackers may launch the denial of service attacks by utilizing extensive bandwidth of the wireless medium.

3.9. Scalability

Unlike wired networks MANETs can grow and shrink on the fly whereas the scalability of wired networks is usually predefined at design time. Freedom to join and mobility are two key features of MANETs, therefore, it is hard to predict the scale of networks like MANET. Scalability may leads to serious routing and QoS concerns. The network services like key management and routing protocols must be compatible with varying scale of the MANETs *i.e*. OLSR is more scalable than DSR due to the use of MPR [20]. It is also founded that hierarchal and GPS assisted routing protocols are more scalable then flat routing protocols because they are more capable of affording node density than flat protocols [21]. Rapid change in scale at run times my invite security and QoS issues and destabilize the MANETs.

3.10. Limited Battery Power

Most of the devices of MANETs are mobile in nature so they strongly rely on battery power for radio transmission whereas wired networks are not battery constrained in nature because they get their power from electric power outlets.

Restricted battery power is major threat in MANETs. The adversary node may flood continuous routing requests to target any battery constrained node or it may grasp a target node to perform a kind of battery consuming activity. Such kind of tasks will exhaust the whole battery power and all the nodes beyond the target node might go out of service.

So on some nodes encountering limited power supply may behave like selfish nodes. As a result network will suffer from intentional non-cooperative behavior of selfish nodes. No doubt, selfish nodes are considered as a kind of security threat.

4. Taxonomy of Network Attacks

Network security attacks can be categorized in a number of ways on the basis of locality of attacker, nature of attack interaction and target layer of the OSI network model. Let's discuss major classifications.

4.1. External V/S Internal Network Attacks

In broader sense network attacks against MANETs can be classified into Internal and external attacks [15] [22]. External network attacks are caused due to unauthorized external entities. They may generate problems like network overhead, denial of service and destructive signal interference. External network attacks are comparatively easy to diagnose as compare to internal network attacks [23]-[25] because Internal network attacks are caused by trusted and authorized nodes which are located inside network. It is very difficult to track and diagnose the malicious behavior of internal compromised network nodes because these nodes are capable to generate valid digital signature and public keys. These nodes may broadcast invalid or modified routing information to other nodes by deceiving other nodes being as shorter path [23] [26].

4.2. Active Attacks V/S Passive Attacks

Based upon the nature of attack-interaction, the attacks against MANETs can be categorized into active and passive attacks. The word passive is self descriptive. These attacks act just like slow poising and do not perform any serious alter to packets and routine operations of the network. These attacks are difficult to detect due to mild in action. Passive attacks usually deduce some info from routed traffic instead of disturbing the routing [23] [25] [27]. On other hand active attacks are very hazardous in action and affect the network very badly. Active attacks may be either internal or external in penetration. These attacks do not hide their identity and prove their presence by altering packets or misrouting the information.

4.3. Stallings Classification of Routing Attacks

Routing is the core of communication in MANETs. Routing is the only mechanism which establishes the successful communication path between sender and receiver. The basic responsibility of a routing protocol is to establish an efficient path between sender and the receiver nodes. Since routing is the core of communication, therefore, its vital role invites the network attackers all the times to launch routing attacks against MANETs [14] [28]. Here we discuss the classification of attacks against MANETs that was suggested by Stallings. According to the Stallings, attacks against MANETs are classified as under [29]:

4.3.1. Modification Attacks

It is a special type of routing attack in which adversary node makes some potential changes in the routing message, as a result routing message may lose its integrity. Packet misrouting is the good example of such attacks in which a message is deviated from its original route [30]. Likewise node impersonation is another example where a malicious node hacks the identity of another node to receive all the messages of that particular node [31].

4.3.2. Interception Attacks

Someone may intercept the normal flow of routing messages by gaining an unauthorized access. In such situation there is a potential hazard of packet alteration before their further forwarding. Wormhole attacks, black hole attacks and routing packet analysis attacks are the major examples of interception attacks.

4.3.3. Fabrication Attacks

There is another technique to chaos the network operation that is fabrication. In fabrication attacks the attacker fabricates its own packets in network to cause the disorder in routine operations of the network. Lack of authentication in routing protocols of MANET leads to fabrication attacks which generate erroneous routing messages [32]-[34]. Sleep deprivation attacks and route salvage attacks are few examples of fabrication attacks.

4.3.4. Interruption Attacks

These attacks interrupt routine network traffic by blocking the routing messages before reaching to destination. In interruption attacks different techniques are used to disturb the normal flow of network traffic such as Packet dropping, flooding etc.

5. Layer Wise Network Attacks

The ISO (International Organization for Standardization) proposed a conceptual model of networking, the OSI model. According to the OSI model, internal functions of communication system are divided into abstraction of seven layers [35]. Since OSI model is a well organizes model of network operations, therefore, it will be better to analyze network attacks according to layer wise stack. Now we discuss the layer wise network attacks in **Table 1**.

5.1. Physical Layer Attacks

Since physical layer deals with physical medium and network devices so in this section we shall discuss network attacks that are originated from physical medium and the hardware. In the absence of secure boundaries [13] [14], it is quite easy to attack wireless medium at physical layer. Physical medium attacker does not need to know the network technology details and attacking techniques in depth. Physical layer is quite sensitive against network attacks; even the failure in communication hardware can generate a considerable problem at physical layer.

Table 1. Layer wise network attacks.

OSI Layer	Attacks
Physical Layer	Eaves dropping, Jamming, Active Interference
Data Link Layer	Selfish node behaviour, Malicious node behaviour, DoS (Denial of service), Integrity, Misrouting Traffic
Network Layer	Black Hole, Wormhole, Sinkhole, Replay, Link spoofing, Resource consumption, Sybil
Transport Layer	SYN Flooding, Session Hijacking
Application Layer	Malicious behavior, Data corruption, Virus

5.1.1. Eaves Dropping Attacks

In eaves dropping is a special technique where attacker makes it sure, the passive listening of messages by an unintended receiver [36]. **Figure 1** shows the attacker between the communication of Sender and Receiver.

There is a simple technique; wireless medium can easily be intercepted, just by proper tuning up the receiving node to specific frequency. The eaves dropping is usually aimed to steal secret information by unauthorized entity such as capturing private keys, public keys and password etc. it is usually done by tapping the wireless link. Captured information could be used for subsequent attacks.

5.1.2. Jamming Attacks

Network Jamming attacks are specific to wireless medium only as oppose to wire networks, where, there is no concept of signal jamming. Jamming is a special technique to degrade the performance of wireless medium by lowering the signal availability [37]-[40]. The attacker or adversary, who is known as jammer, continuously emits the radio signals to rush up partially or even fill up completely the entire wireless band. As a result of the abundance of adverse signals, the legitimate network traffic will be blocked [41] [42]. To launch jamming attacks, first the frequency of legitimate signals of network is determined and then the jamming attack is initiated by the jammer. Usually jammer blocks the legitimate traffic by flooding and filling up the available band. Jamming attacks can be detected and counter fetched by finding signal strength and applying location consistency checks.

5.1.3. Active Interference Attacks

Active interference is the major problem with wireless signals. Interference of Internal or external Electromagnetic signal can strongly disturb the wireless signals and ultimately leads to the denial of service. Active interference may change the order of messages and even may replay old messages. Active interference is the special clause of jamming attacks. During jamming, the transmitted messages are corrupted by challenger node due to electromagnetic interference with the operational frequencies of the targeted receivers [43]. The worst case of destructive interference occurs when the attacker propagate signal with the difference of half wave length of legitimate network signals. That scenario totally nullifies legitimate signals of the network. **Figure 2** gives a comparison of constructive and destructive interfence.

5.2. Data Link/Mac Layer Attacks

The Mac layer attacks are classified in terms of their penetration level and their effect on issues like route discovery failure, energy consumption and link breakage etc [44] [45]. At this layer certain algorithms are used which susceptible to denial of service attacks. The adversary nodes may behave as a just selfish or may exhibit some malicious behavior.

5.2.1. Selfish Nodes Behavior

A selfish node is special type of compromise node which does not suppose to attack the other nodes of a network. It does not cooperate with other nodes and simply refuse its services to other network nodes to save its battery life, CPU cycles and available bandwidth. Networks often encounters a situation when a node is connected to the network but it refuses to forward packets, intentionally, to save its resources like battery power and bandwidth. Such behavior is known as free riding [46]. Sometimes selfish behavior of nodes may exhibit the denial of service.

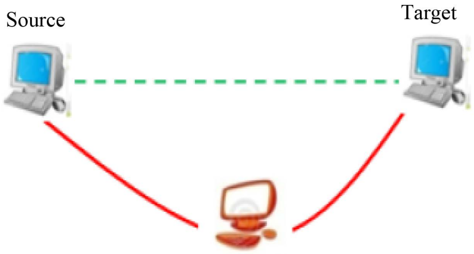

Figure 1. Attacker on communication between sender and receiver.

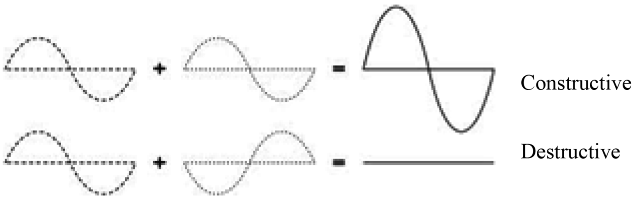

Figure 2. Constructive v/s destructive interference.

Selfish nodes can be classified into three categories according to their level of selfishness.

SN1—A node takes part in network route discovery and maintenance tasks but do not forward packets to other nodes.

SN2—A nodes does not take part in any routing and maintenance operation but just transmit its own packets.

SN3—The nodes which behave normal when the energy level is up to some threshold but if battery level lowers below the threshold value then it behave like SN2.

The level and technique of selfish behavior of a node is dependent upon a protocol in use. Such as a node using DSR protocols may exercise a number of misbehaviors to save its energy and resources like: [47] [48]

- Don't respond to route request (RREQ)
- Don't respond to route replies (RREP)
- Set hop limit/TTL to some minimum value
- Don't send acknowledgements
- Don't forward packets
- Drop data packets

5.2.2. Malicious Nodes Behavior

Another common misbehavior of nodes is identified as malicious nodes. Malicious nodes are considered more risky than selfish nodes because these are capable to launch malicious attacks to the other network nodes where as selfish nodes just refuses to take part in network operations. Malicious nodes may exhibit a number of misbehaves in addition to misbehaves exhibited by selfish nodes. Detail is as given below:

1) Denial of service (DoS) Attacks

Denial of service DoS attacks are aimed to grab the availability of the entire node or some of its services, offered to the network. In other words denial of serve means the unavailability of services to the intended receiver. Denial of service attacks are usually originated from a malicious compromised node in the network. DoS attacks usually prevent the victim to get benefit from the network services. Denial of service can be launched in a number of ways. Taking the advantage of vulnerabilities of Link Layer a attacker may utilize the binary exponential back-off scheme of IEEE 802.11 to refuse access to its local neighbors in a wireless link [49]-[51]. Most of the network services are distributed in nature. DoS attacks may target a node for intensive fake traffic routing to exhaust its processing and battery power. As a result a node may go into hibernate state and break cooperative algorithms [17]. Attackers some time use jamming techniques to launch denial of service attacks. Flooding a network with adverse signals may block the legitimate network [41] [42].

2) Attacks on network Integrity

Integrity means a message will never altered or tampered after transmission. At runtime a message can be truncated, tampered or altered due to any malicious attack. So the integrity attacks must be handled.

3) Attacking Neighbor sensing protocols

Links between neighboring nodes may be marked as broken links due to advertisement of fake error messages by a malicious node. As results of fake error messages a link between two neighboring nodes remain no more active and even neighboring nodes remain failed to sense availability of each other.

4) Traffic Analysis

In MANET the adversary node may take the advantage of traffic patterns by analyzing the traffic flow between different nodes. Confidential information about the topology and traffic flow can be extracted from traffic patterns. Traffic patterns guide the attacker about to track the active and high valued candidate target in a network. Following information can be extracted by analyzing traffic patterns:

- Location of active nodes
- Topological information
- Available source & destination nodes

5.3. Network Layer Attacks (Routing Attacks)

In MANET nodes are connected in hop-by-hop manner [44] [45] [52]. Network layer protocols mange the routing of packets, where each node takes routing decisions for packet forwarding. Routing attacks are very common in MANET. The idea of routing attacks is so simple and straight forward. Routing attacks can be launched by injecting a malicious node in between source and destination to either divert or absorb the network traffic, even a routing loop can be established to create service congestion in a network. The concept is elaborated in **Figure 3** where “M” is a malicious node which intercepts and diverts the traffic between nodes “B” and “C”.

Routing is core of communication in a network. Different routing protocols such as DRS [6], AODV [7], OLSR [8], DSDV [9] are used to route the packets to their destination. Routing protocols are the major area of attack. Attackers target the routing protocols at different phases of routing. Message flooding, routing table overflow and routing loop attacks are major attacks at route discovery phase [53] [54]. Even the route maintenance and packet forwarding phases are not the exceptions. A lot of routing attacks may target packet forwarding and may exploit the packet forwarding functionality at network layer [16] [55]. Attacks on routing protocols are aimed to block the delivery of packets from source to destination. Let’s discuss routing attacks in detail.

5.3.1. Black Hole Attacks

In black hole routing attacks a malicious node uses a trick and advertises itself as an optimal choice for routing from source to destination. On receiving a route request from the source node the adversary node rapidly replies with a fake shortest path [56]. On receiving fake route reply the source node forwards its packets via adversary node. Once the adversary node succeeded to get routing privilege as an intermediate node it can do anything with packets before further forwarding to next hop neighbors. To demonstrate the concept see the **Figure 4**, where node “M” is a malicious node and issues a fake reply to cheat sender node “S” as an the next hop to the shortest path to the destination “D”.

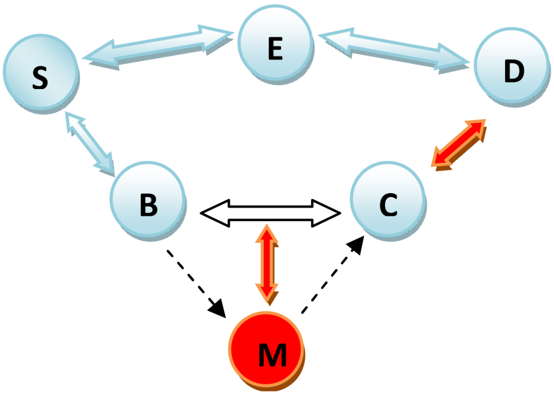

Figure 3. Routing attack by malicious attack.

Consider the AODV protocol for case scenario (**Figure 4**). When the source node "S" advertise a route request RREQ. The malicious node "M" rapidly replies with a higher value of *dest_seq_number* than existing route entry of the routing table of source node "S". In this way node "M" succeed to deceive source node "S" by claiming itself being as a fresh and optimal path towards destination "D". As a result of this black hole data packets are sent over path S->N->M->P->D instead of the path S->N->P->D.

5.3.2. Rushing Attacks

In [57] the authors introduced new routing attack called Rushing attack. Routing protocols, specifically on-demand routing protocols are more susceptible to these attacks where rout discovery is subverted by using duplicate route suppression during process of route discovery [44] [57] [58]. Flooding of the route discovery requests (RREQ) is a major issue in on-demand protocols therefore the protocols like DSR and AODV follow a mechanism to control this flooding. In order to control the flooding, nodes forwards only those request that arrive first. All later same RREQs are simply discarded. The rushing attacks take the advantage of this vulnerability. Let's explain mechanism of rushing attacks. When a route discovery request is initiated by the sender node "S", the malicious node "M" acts very quickly. It passes the same request to all neighbors of the destination "D" very quickly before the arrival of legitimate RREQ from the legitimate route. **Figure 5** elaborates the scenario where nodes "X" and "Y" receive the RREQ from compromised node "M" earlier than any other neighbor, later on when a RREQ is received from nodes "B" and "E" , it is simply discarded by both "X" and "Y" nodes. In this way source "S" always remains fail to find any safe path other than the involvement of compromised node "M" due to the rushing attack of node "M".

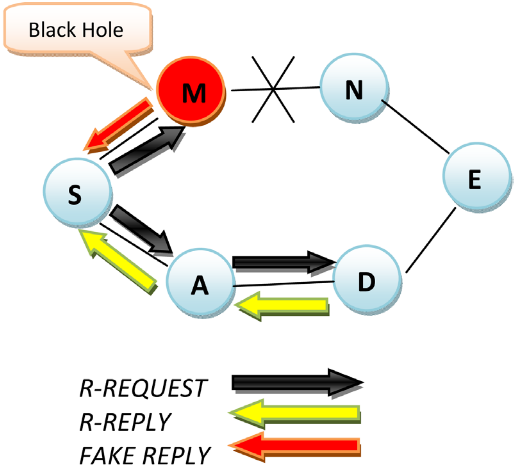

Figure 4. Black hole attack.

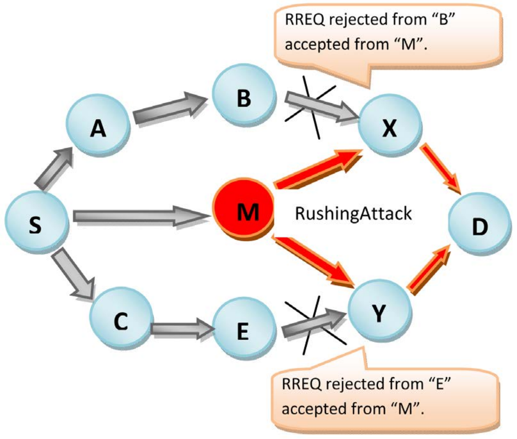
RREQ rejected from "B" accepted from "M".
A
B
X
S
M
RushingAttack
D
C
E
Y
RREQ rejected from "E" accepted from "M".

Figure 5. Rushing attack.

5.3.3. Wormhole Attacks

In wormhole attacks, there participates more than one malicious node as compare to rushing attacks, where, there was a single malicious node. In wormhole attacks when a malicious node receives packets, it sends them to another malicious node through a tunnel, that controlled tunnel between two malicious nodes is actually called a wormhole [57]. Attacker uses the wormhole to get more and more network traffic by creating an illusion of the best available path to other nodes. In this way a lot of network traffic is passed through a controlled tunnel [59] [60]. Wormhole attacks disturb the routing protocols and prevent them from finding a reliable route other than the wormhole. **Figure 6** clearly shows that there are two high speed Malicious nodes “M” and “N”. There exists a wormhole between them. Route reply path will always be S->M->N->D.

5.3.4. Sinkhole Attacks

Sinkhole attack is another dangerous attack in MANET’s. In sinkhole attacks a malicious node broadcasts the wrong routing information to advertize itself as a specific node. In this way the adversary node get attention the whole network traffic and alter the incoming packet before their re-forwarding or even drop the packets. Malicious node tries to capture the secure information of other nodes as shown in **Figure 7**.

Sinkhole attacks effect the performance or routing protocols such as AODV either by maximizing the Sequence_No or minimizing the hop count [52] [61]. In this way the malicious node succeeds in claiming that the best available path passes through it.

5.3.5. Replay Attacks

MANET is the network of self organizing and arbitrary moving network nodes. At run time nodes dynamically change their location. Replay attacks take the advantage of this vulnerability of MANET. In replay attacks [49] a

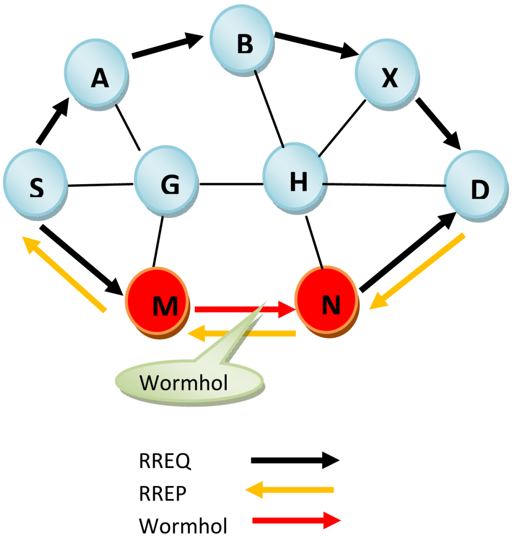

Figure 6. Wormhole attacks.

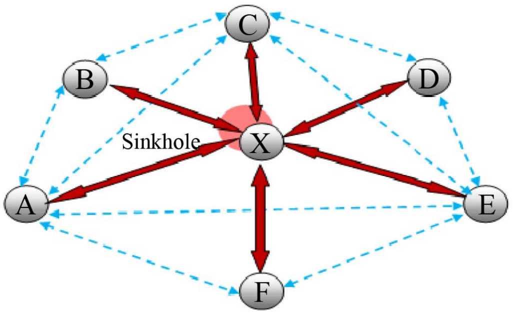

Figure 7. Sinkhole attacks.

malicious node records control packets (TC messages in case of OLSR) of other nodes, move its location and resend them on some later time. In this way other nodes are being cheated by adversary node and they record the stale routes in their routing table that even does not exist, at all. Usually packets are delayed or fraudulently repeated by the malicious node.

5.3.6. Link Withholding and Spoofing Attacks

In link spoofing attacks the malicious node withholds the link and does not broadcast routing information to the specific nodes or it advertize the fake link information to the non neighboring nodes to disturb the routing operations [59]. Kannhavong *et al*. [62] showed that in OLSR protocol the attacker broadcasts the fake link to next two hop neighbors of the target node. In this way the target is black mailed to choose the infected node as a MPR node (see **Figure 8**).

5.3.7. Resource Consumption Attacks

In resource consumption attacks, the compromised node targets a node to exhaust its resources like battery power and bandwidth by engaging the victim node in some fuzzy network operation. Usually excessive route requests are sent to the victim to consume its resource like battery power and band width [59] [63]. Flooding is the major technique to launch a resource consumption attack. S. Desilva *et al*. [64] have demonstrated their work that flooding can degrade up to 84% overall throughput of MANET. As the result of this resource consumption the victim node remain no more available for routing and cooperative network algorithms.

5.3.8. Sybil Attack

The Sybil attacks are launched in a network by generating a number of fake identities of the network node. A single malicious node exhibit itself as a many independent nodes. Actually these additional fake identities acquired by the malicious node are called Sybil nodes [65] [66]. The Sybil node may steal the identity of another legitimate node or even fabricate new identity for itself. In the presence of Sybil nodes in the network it is too much difficult to track the misbehaving nodes. The presence of these virtual Sybil nodes may generate network issues like unfair resource allocation among network nodes, absorption a lot of network traffic, denial of service by redirecting the packet of legitimate nodes to their self etc.

See the **Figure 9** where a malicious node "M" get three additional Sybil identities "X", "Y" and "Z". Actually

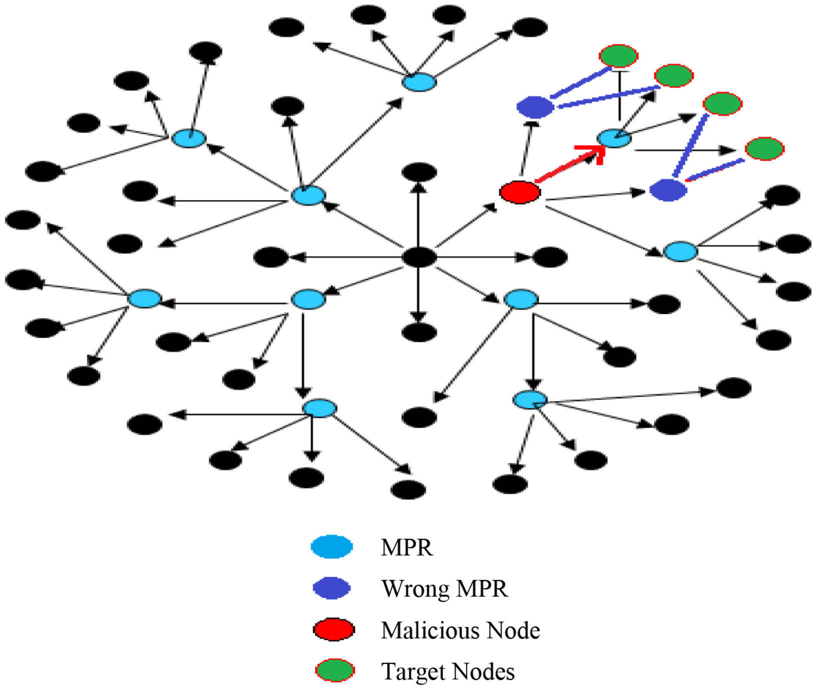

Figure 8. Wrong Selection of MPR.

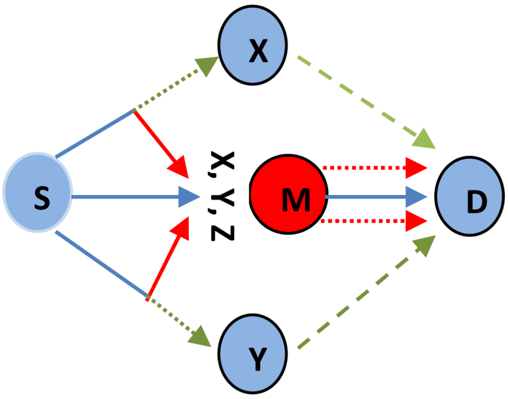

Figure 9. Malicious node M with Sybil identities X,Y,Z.

"Z" is the brand new Sybil identity while the identities "X" and "Y" are stolen from legitimate nodes to get diversion of their traffic to pass through the node "M". Now the node "M" is capable either to pass or block the traffic towards the node "D".

5.3.9. Byzantine Attacks

The Byzantine attacks may involve single or group of compromised nodes in a network. Usually byzantine attacks target the MANETs either by creating routing loops or sending packets via non-optimal path to degrade overall routing services of the network [67].

5.4. Transport Layer Attacks

Transport layer accepts messages of variable length from session layer and pack them into packets and submit them to the network layer for transmission. On reaching destination these packets are again reassembled at transport layer. So sequencing and reassembling are two key operations at transport layer. Transport layer assigns a sequence number to each packet during segmentation, prior to transmission. This sequence number is used to reassemble packets in a proper order at destination. TCP and UDP are two major protocols used at transport layer. Transport layer attacks may change the packet sequence number to disturb the reassembling.

5.4.1. Session Hijacking

In MANET there is a concept of just initial setup of the session. There exists no proper session protection mechanism during the communication. Attacker takes the advantage of this vulnerability and spoofs the IP address of the victim node and gives opportunity to the malicious node to behave as a legitimate node. After spoofing, attacker captures the intended Sequence_No from the packets and becomes in a position to launch denial of service attacks (DoS) on the basis of captured Sequence_No. usually secret information like password, logion name etc. are captured during session hijacking attacks.

TCP-ACK storm is the good example of session hijacking. See the **Figure 10** where malicious node "M" injects a TCP_ACK hijacking attack and injects a session data to node "A". The node "A" sends a acknowledgment packet (ACK) to node "B" but this packet does not contain a sequence_number that was expected by the node "B". So on receiving packet at node "B", when node "B" tries to synchronize the TCP session with node "A", it remain fails due to change in session data attack, launched by node "M". Node "B" becomes confused and sends lost ACK back to node "A" for resynchronization. In this way TCP-ACK loop is established and due to TCP- ACK storm system becomes unavailable to other nodes.

5.4.2. SYN Flooding Attacks

It is a special kind of denial of service attacks where a attacker sends a successive SYN requests to the target node to consume its resources and make it unavailable to legitimate traffic. Normally there is a three way hand shaking mechanism between sender and receiver nodes that is:

1) Node "X" requests for connection by sending SYN message to node "Y".

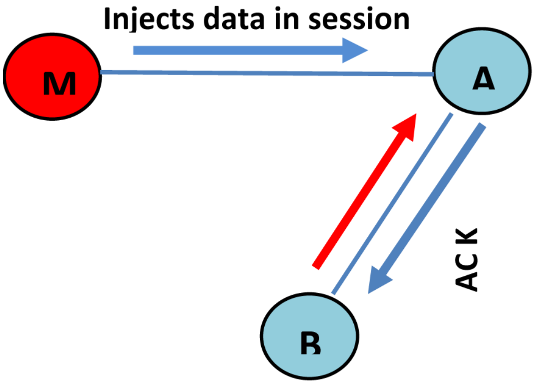

Figure 10. Session hijacking example.

2) Node "Y" acknowledges request by sending SYN-ACK message to node "X".
3) Node "X" again responds with ACK and connection is established between "X" and "Y".

But in SYN attacks the node "X" floods the SYN request at all ports of the node "Y" but does not acknowledge the SYN-ACK that was generated by node "Y" to establish the connection. In some cases it replies with the spoofed source IP. So there will form a loop of half opened connection between node "X" and "Y". The node "Y" will reply again and again and ultimately it will go to the denial of service due to non availability of free ports. This situation occurred due to flooding of SYN attacks.

5.5. Application Layer Attacks

Application layer is the actual layer where user interacts with the data. Many protocols work at this layer such as HTTP, SMTP, FTP, TELNET etc. These protocols are vulnerable in nature so they can be attacked by the expert attacker at the application layer.

5.5.1. Malicious Code Attacks

There is a general rule of data processing that is, GIGO (garbage in garbage out).This rule also applies at data communication. If we shall transmit a wrong data definitely target will also receive a wrong data. At application layer great care is needed to protect data against the malicious code, worms and virus attacks before the transmission and even after the reception at target. Viruses, spywares, trogon horses and other malicious codes can damage application, data and even operating system. Data corruption attacks are very common at application layer. These attacks may change the format of data even convert data into some unreadable format. Therefore certain measures should be taken to protect data at application layer and counter fight against application layer attacks.

5.5.2. Repudiation Attacks

Repudiation means the denial from active participation in network communication and abstain from the taking the ownership of what has been transmitted or received by the node. In the presence of repudiation attacks it becomes difficult to isolate the origin of malicious activity if no one will accept the responsibility. At the level application layer still there are chances of network attacks. Many of security measures taken at different layers are still not sufficient to protect the packets. Application layer programs such as antivirus and firewalls must be configured properly to avoid such attacks. Firewalls and logical port security is also very important. Attacker may take advantage of open ports. So, mutual cooperation of running application and operating system should guarantee the security and availability of under lying logical communication ports for smooth network communication.

MANET attacks are summarized in **Table 2**.

6. How to Meet Security Challenges?

As so for we have done a lot of deal with MANET, its vulnerabilities, different types of MANET attack. After the detailed analysis of wireless network vulnerabilities and network attacks, we are now in a position to propose

Table 2. Summary of MANET attacks.

Attacks			
External and Internal Attacks			
Active and passive attacks			
Stalling classification of routing attacks	Modification of attacks		
	Interception attacks		
	Fabrication attacks		
	Interruption attacks		
Layer Wise Network attacks	Physical Layer attacks	Eaves Dropping	
		Jamming attacks	
		Active interference Attacks	
	Data/Mac Layer attacks	Selfish Nodes behavior	
		Malicious nodes behavior	DoS Attacks
			Attacks on network integrity
			Attacking neighbor sensing protocols
			Traffic Analysis
	Network Layer Attacks	Black hole attacks	
		Rushing Attacks	
		Warm hole attacks	
		Sinkhole Attacks	
		Replay attacks	
		Link withholding and spoofing attacks	
		Resource consumption attacks	
		Sybill Attacks	
		Byzantine Attacks	
	Transport Layer Attacks	Session Hijacking	
		SYN Flooding Attacks	
	Application Layer	Malicious code Attacks	
		Repudiation Attacks	

some solutions. It is the time to meet the security challenges to make the MANET more and more secure. In broader sense there are three possible techniques of solutions:

- Cryptography/Encryption
- Intrusion detection system
- Secure routing

6.1. Cryptography

Cryptography is the one the earlier solutions that were proposed for the data security during its transmission from sender to receiver. In cryptography data is usually encrypted before transmission at source and a mutual agreed key is shared to decrypt it, reaching at destination. At reaching the destination data is again reformed into understandable format using decryption. Many techniques are used in the field of cryptography such as a public key, authentication and digital signature etc.

6.2. Intrusion Detection

Once there was a time when cryptography was considered enough for the intrusion prevention but very soon it was realized that it was not more than just a first aid to security threats. With the passage of time the idea of a proper intrusion detection system was introduced in network security. Intrusion detection is mechanism to monitor the activities of the network at run time. An intrusion detection system (IDS) performs this duty. It collects the data about network activities and evaluates data to trace any security violation in a network. If it finds any security hazard, it alerts the whole network and launches defense line to combat against the threat. Intrusion detection systems are developed on the basis of two basic assumptions that [68]:

- It is possible to monitor the activities of the user and the program.
- A clear line of differentiation can be drawn between normal and intrusive network activities.

Historically early intrusion detection systems were developed for wired networks, where traffic must go through several network devices like routers and gateways, hence an IDS can easily be implemented and hard coded into these devices [69] [70]. These IDS's were not compatible with MANET due to mismatching characteristics of wired and wireless networks. Therefore, a modified version of IDS was required for the MANET. On the basis of auditing data intrusions detection system can be classified into two types:

- Host based IDS
- Network based IDS

A host based intrusion detection system depends upon operating system and application logs for intrusion detection while on other hand network based intrusion detection systems rely on packets captured from network traffic. IDS's are classified into three categories on the basis of the techniques of intrusion detection [71].

1) Anomaly detection system: it keeps the record of normal network behavior and periodically compares the captured data with the recorded normal behaviors of the network. If there found any deviation from the baseline recorded data it is treated as intrusion.
2) Misuse detection system: it keeps the definitions (patterns) of the known attacks and compares these patterns with captured data to find any intrusion.
3) Specification based detection: it is the definition based intrusion detection where set of constraints define a normal behavior of network. The system continuously monitors the network operations according to the defined parameters.

Now the issue is that which intrusion system is best for the MANETs? Different architectures of IDS's are available but the optimal IDS architecture for a MANETs may depend on the network configuration itself [72]. Following is the list of major architectures of MANET IDS's.

- Stand alone IDS
- Distributed and cooperative IDS
- Hierarchal IDS
- Mobile agent

6.2.1. Stand Alone Intrusion Detection System

In stand-alone architecture, the IDS run on each node independently. The IDS just monitors the behavior of that particular node only, on which it is installed. There is no exchange of data and cooperation among different nodes of the network even in the same network nodes remain unaware of what is happening with neighboring nodes. Although this architecture is not so much effective due to its limitations but it may be implemented where each node is capable of running IDS. It is not recommended for MANET.

6.2.2. Distributed and Cooperative Intrusion Detection System

Keeping in mind the vulnerable nature of MANET, the distributed and cooperative model of IDS was first proposed by Zhang and Lee [73]. They stated that the intrusion detection system may be, both, distributed as well as cooperative. Every node participates actively by having an intrusion detection agent running on it. An intrusion detection agent is responsible monitoring local event, data collection, identifying the possible intrusion, as well as launching response independently. Although each intrusion detection agent works well locally, however, neighbouring nodes also share their investigations with each other for mutual cooperation. See **Figure 11**

Especially Inter node cooperation occurs when a node detects an anomaly but don't have enough evidence to figure out the kind of intrusion that was occurred. In that scenario, a node shares its data with other nodes within the communication range to check their security logs to trace the possible intruder. Let's us now discuss the internal structure of the IDS agent. Here is the conceptual model comprising of four major functional modules as in **Figure 12**.

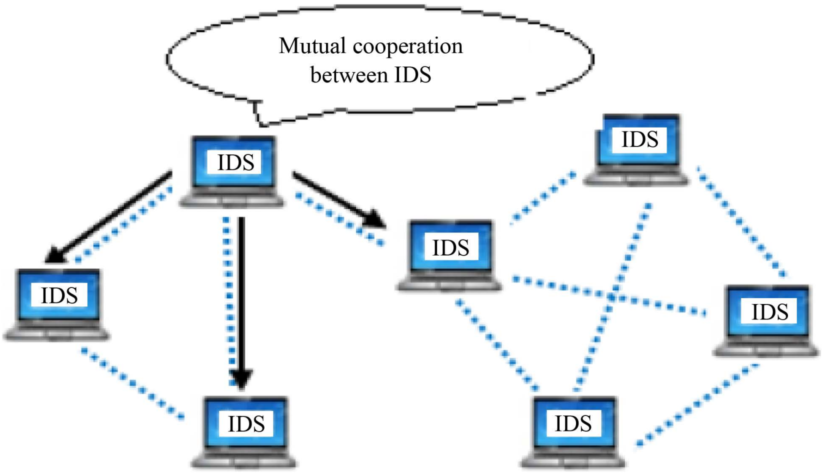

Figure 11. Mutual cooperative IDS architecture.

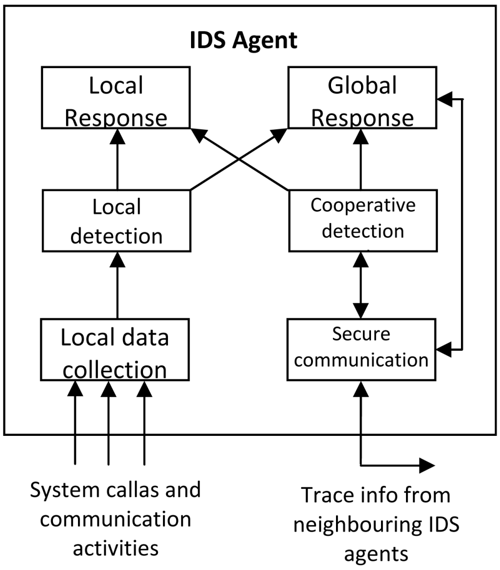

Figure 12. Conceptual model of an IDS agent.

1) Local data collection module: it is responsible to handle the collection of real time auditing data coming from different sources.
2) Local detection engine: it examines and evaluates the collected data by local data collection module. It inspects the data for any possible anomaly. The IDS should not rely on misuse detection technique to find intrusion because it is based upon the comparison of collected data with the known patterns of the attacks. Successful IDS should relay on statistical Anomaly Detection Technique rather than the use of misuse Detection Technique, which is not capable detect novel attacks.
3) Cooperative detection engine: this module is responsible for inter node sharing of suspicious anomalies. If there found any ambiguous anomaly at any particular node, the cooperative detection engine initiates a cooperated intrusion detection process by advertizing its state information to all nearby neighbors. As a result of this initiation all other nodes also check their current states and reach to consciences about intrusion and its origin.
4) Intrusion response module: this module is responsible for launching anti response against the possible intrusion. The anti intrusion response is dependent upon the nature and level of the intrusion found. Some time it simply reassigns the keys or rearranges the network nodes. The communication with compromised nodes can be blocked or even these nodes may be removed from the network community.

6.2.3. Cluster-Based Intrusion Detection System

As we discussed in the previous section about distributed and cooperative IDS, where all the nodes equally participate in the process of cooperative intrusion detection even then it was not necessary, the participation of each node. It may leads to a lot of power consumption in network. As a result of such consumption of energy a node may behave as selfish node to save its energy and regret to participate in cooperation network operations. To solve this problem Huang *et al.* presented the idea of cluster-based intrusion detection system [74]. In cluster-based IDS the network is divided into cluster so that the cluster head, usually, have to perform more functionality than member nodes. The cluster head functions as control point like router or gateway of wired networks. The IDS agents of the member nodes are responsible for local detection and response but the cluster head is responsible for local detection as well as inter cluster intrusion detection. In this way only cluster heads participate in network Intrusion while member nodes only monitor their local intrusion. All the nodes in the network are organized in such a way that every node becomes a member of at least one cluster. Usually a cluster is composed of the one hop neighbors within the direct communication range of each other. There will be a single node in a cluster that will play a role of cluster head for some period of time. Cluster head is chosen on fairness and efficiency basis. By fairness we mean that every node have equal chances for the selection being as a cluster head and each node will act as cluster head for some period of time. There should exist a mechanism to choose a cluster head periodically, a node with higher efficiency. Here is the finite state machine of the cluster formation protocol in the **Figure 13**.

There are four states in cluster formation protocol *i.e*. initial, clique, done and lost. At first all the network nodes will be in initial state, which means they will monitor their behavior for intrusion detection locally. There is a pre requisite prior to the selection of cluster head that is the clique computation. A clique is defined as the group of nodes where each pair has a direct link with each other. After the clique computation every member in a clique is aware of its clique fellows. Then a node with higher efficiency will be selected as cluster head, at random. There are further two protocols that assist cluster for doing validation and recovery tasks.

1) Cluster valid assertion protocol: A node periodically uses this protocol to maintain its link with cluster-head. If the link is broken with cluster-head, the node looks for another cluster-head for link establishment. In case of failure it goes into a LOST state and generates a route recovery request. There should re-election timeout for cluster-head to ensure fairness in cluster-head selection mechanism. At the timeout expiry all the nodes go into INITIAL state from the DONE state.
2) Cluster Recovery protocol: this protocol is used when a cluster member loses its connection with cluster-head and goes into LOST state. It helps the node in discovering a new cluster-head. It is proven by Huang *et al*. [74] that cluster-based IDS performs very well with low CPU utilization and power consumption as compare to distributed and cooperative IDS's.

6.2.4. Mobile Agents for IDS's

There is another idea of mobile agents for the intrusion detection systems. Due to its ability to move through in a

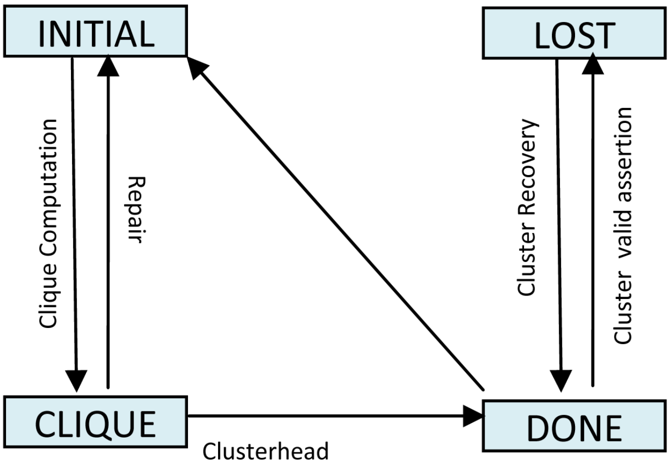

Figure 13. Finite state machine of cluster.

large network, each mobile agent is assigned a single particular task. Different mobile agents are distributed over a large network to distribute the intrusion detection task among all nodes. There are several advantages of mobile agents. Since each mobile agent is assigned a single task so the intrusion detection overhead is distributed among the whole network and a lot of energy is saved from consumption. IDS also become a fault tolerant. In case of the failure of any node the mobile agent of the other node handles the situation.

6.2.5. Intrusion Detection through Cross Layer Analysis

Multi layered IDS may produce better results than single layered intrusion detection systems because different attackers use different network layers to attack. So multi layered IDS is the better approach because on the spot detection and remedy is more effective than later diagnosis and therapy but multi layered IDS has its own pores and coins. For example it may produce more processing overhead on the nodes than the single layered IDS's. The idea of cross layer analysis and intrusion detected was proposed by *Parker and his colleagues* [75]. In their paper they elaborated that how smartly an attacker takes the advantage of multiple vulnerabilities at multiple layers to stay below the detection threshold of the single layered IDS. In multi layered IDS data from different layer stacks is analyzed comprehensively. There is no debate about the efficiency of cross layered IDS, definitely a cross layered IDS is better in performance against security threats as compare to single layered IDS but we have to do something to balance the processing overhead.

6.2.6. Watch Dog Path Rater

Watch dog rating is a special technique to improve the performance of the network even in the presence of nasty nodes. Let's have a look at working principal of the watch dog as it explained with detail in [76] [77]. Watch dog detects the misbehavior of the adjacent nodes by keeping a copy of sent packets in a buffer of the node. It continuously spies the neighboring nodes to determine whether they have forwarded the packet as it is or forwarded a modified version of packets. If the packets are forwarded without modification than they are removed from the buffer of observing node otherwise after some timeout they are considered as dropped are modified. In that case the neighboring node that was responsible for packet forwarding is assumed being as malicious node. Each successive violation by the specific node increases its chances to be declared as malicious one. If the number of violations crosses the some predefined threshold then the node is declared as malicious one and its information is passed to the path rater component. At each node the path rater component rates all the known neighbor nodes with respect to their reliability regarding violations. Initially nodes start with a neutral rating but ratings are updated at run time according to the perspective of any particular node. The nodes which are found misbehaving by the watchdog are immediately rated as −100. A packet modification by the node is considered as misbehavior while link breakage is considered as unreliability. Nodes are selected for the routing based upon their rating and reliability so watch dog is a good way to detect and boycott the malicious nodes in the network to improve the network security.

6.3. Secure Routing Techniques

Routing is the core of communication in MANETs so routing protocols are the hot target for security attacks. In the sub-section of section 5.3 we have discussed in detail different security attacks against routing protocols. Now we discuss the proposed solutions to these attacks.

6.3.1. Defense against Wormhole Attacks

Wormhole attack is the one of the major attacks against the routing protocols [78]. For detailed information about wormhole attacks please refer to section 5.3.4 of this paper. In [79] Y. Hua, A. Perrig and D. Johnson presented a solution of wormhole attacks that is a packet leashing. It is a mechanism to detect and launch a defense against wormhole attacks [78] [79]. Leash is the additional information that is added to packet to restrict it maximum life and distance covered by the packet. There are two types of leashes (Temporl leash and Geographical leash). Both of these leashes protect the network by restricting the packets, not to go away from the certain distance limit.

1) Temporal leash: it restricts the upper bound on life time of the packet. Every node calculates the expiry time "t_e" and padded it into its packets so that it may not travel far farther than certain distance "L". At the arrival of packets each node evaluates the "t_e" contained in packets, compare it with the current time and decide

about, whether the RREQ was possibly tunneled through a malicious high speed link? To implement temporal leashes the TIK protocol is used. TIK stands for TESLA with instant key disclosure and it is the extension of TESL protocol [80]. TIK protocol provides defense against wormhole attacks by preventing the packet to travel longer distance than the nominal radio range.

2) Geographical leash: it ensures that the receiver is within the certain distance range from the sender. Every node must be provided with respective geographical position and the transmission time of the packets. This can be used along with signature to catch attackers that are supposed to be residing on multiple locations.

Based upon geographical location, a similar solution was also proposed by D. Dhillon *et al.* [81]. However, it requires the integration of the public-key infrastructure with the time synchronization between all nodes. According to them in MANETs using OLSR as a routing protocol, each node should insert its current location and time stamp in HELLO messages. At the arrival of messages this embedded information is used compute the travelled distance. If the distance exceeds some maximum limit, the messages are considered highly suspicious. Some authors have proposed different detection techniques of wormhole attacks. The L. Hu and D. Evans in [82] have shown the antenna based detection techniques of wormhole attacks that do not require clock synchronizations among nodes. So on Qian *et al*. [83] introduced a new technique of detection that is statistical analysis over multiple path routing but this technique is not valid for AODV because it does not maintain multiple paths.

6.3.2. Defense against Rushing Attacks

Rushing attack is kind of denial of service attacks that acts against routing protocols On-demand protocols are more susceptible to these attacks where rout discovery is subverted by using duplicate route suppression during process of route discovery [44] [57] [58]. For detailed discussion about rushing attacks, refer to section 5.3.2 of this paper. When a route discovery request is initiated by the sender, the attacker acts very quickly. Attacker passes the same request to all neighbors of the destination very quickly before the arrival of legitimate request from other legitimate route. There is a problem with on demand routing protocols that is they restrict an intermediate node to choose at most single route request for further forwarding to the destination. As a result of this efficiency of the attacker and the limitation of protocol all the legitimate request are discarded by the neighbors of the destination because they have already forwarded such request sent by the attacker node. So the denial of service occurs. To undermine the rushing attacks a frame work of techniques was introduced by Y. Hu, A. Perrig and D. Johnson [57]. This frame work is comprised of secure neighbor detection, secure route delegation and randomized route request forwarding.

1) Secure neighbor detection: it allows the neighbors to verify each other that they are within the maximum transmission range of each other. Now if a node "X" determines in advance that node "Y" is neighbor (within allowable communication range), it sign a *Route delegation message* allowing the "Y" for further forwarding of the request. Now when "Y" determines that "X" is within a allowable range it accepts the delegation message of node "X". in this way genuine neighborhood of the nodes can be guaranteed.

2) Randomize Selection of R_REQ: it ensures the randomize selection of R_REQ for further forwarding which replaces the duplicate suppression in on-demand protocols. So the path with low latency is more likely to be selected but not guaranteed. Relationship between different security mechanisms is elaborated in **Figure 14**.

6.3.3. Defense against Black Hole Attacks

Different efforts were made to combat against black hole attacks. Designing of security-aware *ad hoc* routing protocol SAR [84] is the one of those which based upon on-demand protocols. SAR uses two techniques to countermeasure the black hole attacks. First it inserts a security metric in RREQ packets and secondly it uses alternate route discovery mechanism. Security metric is inserted for achieving an acceptable security level. At

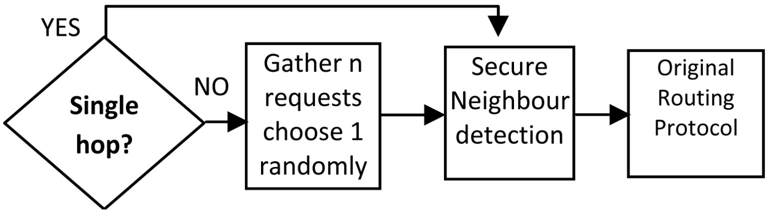
YES
Single hop?
NO
Gather n requests choose 1 randomly
Secure Neighbour detection
Original Routing Protocol

Figure 14. Combined mechanism to MANET against rushing attacks.

each trust level packets are encrypted with a shared symmetric cryptographic key. Nodes with different trust levels remain unable to read encrypted packets. Whenever a node receives a RREQ from a particular source, it verifies the trust level associated with it from the security metric information attached with packet. On satisfaction, the packet is forwarded otherwise it is dropped by intermediate nodes. Likewise when the packets reach at destination, they are evaluated. If destination is satisfied of complete end-to-end path then it generates a RREP otherwise source is notified to adjust its security level to any other alternative route. Another approach to combat against black hole attacks was introduced by S. Lee *et al.* [36]. They introduced the idea of sending confirmation CRREQ and CRREP prior to sending routine RREQ and RREP requests to verify the validity of the path from source to destination. However this approach is fail against pair of nodes working in collusion. Al-Shurman *et al.* [85] proposed a solution of this problem that the source node should wait for arrival of RREP from multiple nodes and then decide the accuracy of path information.

6.3.4. Defense against Byzantine Attacks

In [86] Robust source routing (RSR) was introduced by Cr' epaue *et al.* as the solution of byzantine attacks. RSR uses a fore runner (FR) packet to notify the intermediate nodes with expected route and data flow time frame. If the intermediate node does not receive any data flow within the notified time period it informs the source node about this event. In this way the links with selfish and malicious behavior could be isolated.

6.3.5. Defense against Resource Consumption Attacks

In [63] Yi *et al.* proposed an effective security mechanism to control resource consumption attacks. This is particularly effective for MANETs, using AODV as a routing protocol. According to the proposed mechanism each node computes and records the RREQs arriving from neighboring nodes. If the RREQ rate from the particular nodes exceeds from some particular threshold rate, the node is blacklisted and its further requests are simply discarded. The technique seems a good but there is a problem with this technique. It may even block some legitimate because it is prone to false positive.

Similarly in [64] S. Desilva and R. V. Boppana introduced an anomaly-based detection mechanism, where, threshold rate of RREQs is calculated on the fly based upon statistical analysis of RREQs.

6.3.6. Defense against Link Spoofing Attacks

B. Kannhavong *et al.* [62] showed that a link withholding attack against (TC) messages of OLSR protocol can isolate and prevent a particular node from communication. They also proposed a solution to detect link withholding and spoofing attacks. Their solution is based upon a hypothesis that if a node receives "hello" messages form its MPR but does not receive "TC" messages then the node is supposed to be a suspicious one. In that situation the node is allowed to switch to another node. However this technique works very well but it is fail to detect attacks launched by two malicious partners, where first partner pretend to advertize "TC" messages while the second one discard them. D. Raffo *et al.* In [87] introduced a new detection scheme of link spoofing attacks which relies on the information obtained from GPS and encrypted time stamps. In this scheme every node is bound to advertise its GPS coordinates along with time-stamp. From these two pieces of information, It is possible to detect link spoofing by calculating inter nodal distance of particular nodes. Likewise it could also be verified whether the nodes are in between or beyond the maximum transmission range. The major limitation of this solution is that each node must be equipped with GPS all the times.

6.3.7. Defense against Replay Attacks

In order to protect MANETs against replay attacks C. Adjih *et al.* [55] proposed a solution that is based upon time-stamps and asymmetric encryption. Every receiver node compares its current time with the embedded time-stamp of the control messages. If the time difference is much more than some threshold duration the packet is considered as replayed and discarded by the receiver. In this way routing protocol avoids to update its routing table with stale routes.

7. Conclusion

Throughout the paper we addressed each and every aspect of the MANET that is concerned with the security in any way at any extent. We started from the scratch; we discussed the architecture of MANET, vulnerabilities of the MANET, different security threats and even different types of security attacks in this paper. Non-stable architecture of MANETs and wireless vulnerabilities helped us to understand, why the MANETs are easy to attack. Layer wise network attacks and their proposed solutions enlightened us to understand the way of action and execution plan of different network attacks. From the whole scene one thing is crystal clear that MANETs will go on the way in the same fashion without any major change. Wireless is their natural ally as a communication medium; there is no substitution or alternative of wireless medium. These things will persist at least in near future unless the emergence of any new technology. Even though there is the invention on any substitution, it will take long to switch to that particular technology. At present we have to accept the MANETs and wireless vulnerabilities as a good evil. We can make effort to improve the things by keeping in mind these vulnerabilities. For a moment if we think positively, in fact we are blessed with a great room, from research point of view due to these vulnerabilities of the MANET and wireless medium. A lot of research work has been done by the researchers but still there is a lot to do. Network security is a dynamic issue. New and new attacks are getting introduced. So the constant efforts are required to make the MANET more and more secure. There is a lot of research scope in the field of secure routing. Intrusion detection and its healing is another research hot spot for the network security researchers. Most of the intrusion detection systems and techniques look very beautiful and convincing on papers but still applied research work is waiting for the researchers in certain areas of network security. There is need to implement, evaluate and improve these intrusion detection systems practically.

8. Open Issues and Future Research

MANETs are the networks of the day and wireless is their natural ally as a communication medium. We discussed different vulnerabilities of wireless medium in detail. For a moment if we think positively, in fact we are blessed with a great opportunities, from research point of view due to these vulnerabilities of the MANETs and wireless medium. A lot of research work has been done by the researchers but still there is a lot to do. There is a lot of research scope in the field of MANETs security. Routing is the core of communication in networks therefore routing protocols are high valued target for the attackers. Most of the known routing attacks against MANETs take the advantage of the different vulnerabilities of the routing protocols therefore *development of new secure versions of the routing protocols is most demanding area for the researchers*, now a days.

A lot of work has been done by the researchers in finding and combating against different attacks against routing protocols but still there is *wide research scope in detection of newly born security attacks and their solutions*. Up till now, most of the known attack detection techniques are attack specific. Even their proposed solutions are either specific to particular attack or protocol. Likewise most of the proposed solutions are not efficient in the presence of multiple cooperative malicious nodes. *From research point of view it is the open issue to develop a generic attack detection and prevention mechanism to handle a variety of network attacks.* System based intrusion detection system (IDS) is another attractive research hot spot in MANETs. Most of the intrusion detection techniques and combating systems are designed to handle security issues at particular network layer of the OSI model. *There are great research opportunities to develop intrusion detection systems based upon cross layer analysis of security attacks.*

We have discussed in detail different architectures of the intrusion detection systems. Intrusion detection systems utilize different strategies to find out possible intrusion. *Development of a specification based smart intrusion detection system is another demanding area for the researchers*. Researchers may conduct a research to find new constraints to improve the defined set of normal behaviors of the network. Known anomaly detection and healing techniques look very beautiful and convincing on papers but still *applied research work is waiting for the researchers in certain areas of network security*. A lot of work has been done in the field of intrusion detection systems but *running cost of detection systems is still an open research issue for the researchers*. Researchers may conduct their research to minimize the running cost of the intrusion detection system in the presence of battery constrained nodes.

Acknowledgements

I, personally feel extremely beholden to Prof(R) Ghulam Qasim Shah who with self-abnegation graciously spared his time and reviewed this paper.

References

[1] Conti, M. (2003) Body, Personal, and Local *Ad Hoc* Wireless Networks. In: Ilyas, M., Ed., *The Handbook of Ad Hoc Wireless Networks*, CRC Press, Inc., Boca Raton, 3-24.

[2] Weiser, M. (1991) The Computer for the Twenty-First Century. *Scientific American*, **265**, 94-104.

[3] Perkins, C.E. (2001) *Ad Hoc* Networking. Addison-Wesley, Reading.

[4] Corson, M.S., Macker, J.P. and Cirincione, G.H. (1999) Internet-Based Mobile *Ad Hoc* Networking. *IEEE Internet Computing*, **3**, 63-70. http://dx.doi.org/10.1109/4236.780962

[5] Macker, J. (1999) Mobile *Ad Hoc* Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, January1999.

[6] Johnson, D.B. and Maltz, D.A. (1996) Dynamic Source Routing in *Ad Hoc* Wireless Networks. In: Imielinski, T. and Korth, H.F., Eds., *Mobile Computing*, Springer, New York, 153-181. http://dx.doi.org/10.1007/978-0-585-29603-6_5

[7] Perkins, C., Belding-Royer, E. and Das, S. (2003) *Ad Hoc* On-Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[8] Gellens, R. (1999) Wireless Device Configuration (OTASP/OTAPA) via ACAP.

[9] Perkins, C.E. and Bhagwat, P. (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. *ACM SIGCOMM Computer Communication Review*, **24**, 234-244. http://dx.doi.org/10.1145/190809.190336

[10] Mishra, A. and Nadkarni, K.M. (2003) Security in Wireless *Ad Hoc* Networks. In: Ilyas, M., Ed., *The Handbook of Ad Hoc Wireless Networks*, CRC Press, Inc., Boca Raton, 499-549.

[11] Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004) Security in Mobile *Ad Hoc* Networks: Challenges and Solutions. *IEEE Wireless Communications*, **11**, 38-47. http://dx.doi.org/10.1109/MWC.2004.1269716

[12] Raffo, D., Adjih, C., Clausen, T. and Mühlethaler, P. (2005) Securing OLSR Using Node Locations. *Proceedings of the* 11*th European Wireless Conference* 2005—*Next Generation Wireless and Mobile Communications and Services* (*European Wireless*), Nicosia, 10-13 April 2005, 1-7.

[13] Myers, A.D. and Basagni, S. (2002) Wireless Media Access Control. In: Stojmenovic, I., Ed., *Handbook of Wireless Networks and Mobile Computing*, John Wiley & Sons, Inc., New York, 119. http://dx.doi.org/10.1002/0471224561.ch6

[14] Zhang, Y., Lee, W. and Huang, Y.A. (2003) Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks*, **9**, 545-556. http://dx.doi.org/10.1023/A:1024600519144

[15] Perkins, C.E. (2001) *Ad Hoc* Networking: An Introduction. *Ad Hoc Networking*, **40**, 20-22.

[16] Papadimitratos, P. and Haas, Z.J. (2002) Securing Mobile *Ad Hoc* Networks. In: Ilyas, M., Ed., *The Handbook of Ad Hoc Wireless Networks*, CRC Press, Inc., Boca Raton, 665-671. http://dx.doi.org/10.1201/9781420040401.ch31

[17] Zhou, L. and Haas, Z.J. (1999) Securing *Ad Hoc* Networks. *IEEE Network*, **13**, 24-30. http://dx.doi.org/10.1109/65.806983

[18] Vinayakray-Jani, P. (2002) Security within *Ad Hoc* Networks. *Proceeding of the PAMPAS Workshop*, London, 16-17 September 2002.

[19] Biswas, K. and Ali, M.L. (2007) Security Threats in Mobile Ad-Hoc Network. Master's Thesis, Department of Interaction and System Design School of Engineering, Blekinge, 9-26.

[20] Woo, S.C.M. and Singh, S. (2001) Scalable Routing Protocol for *Ad Hoc* Networks. *Wireless Networks*, **7**, 513-529. http://dx.doi.org/10.1023/A:1016726711167

[21] Parker, J. (2006) Discussion Record for the 1st MANET Reading Group Meeting. February.

[22] Viennot, L., Jacquet, P. and Clausen, T.H. (2004) Analyzing Control Traffic Overhead versus Mobility and Data Traffic Activity in Mobile Ad-Hoc Network Protocols. *Wireless Networks*, **10**, 447-455. http://dx.doi.org/10.1023/B:WINE.0000028548.44719.fe

[23] Amitabh, M. (2008) Security and Quality of Service in *Ad Hoc* Wireless Networks. Cambridge University Press, Cambridge.

[24] Gokhale, V., Ghosh, S. and Gupta, A. (2010) Classification of Attacks on Wireless Mobile *Ad Hoc* Networks and Vehicular *Ad Hoc* Networks: A Survey. In: Pathan, A.S.K., Ed., *Security of Self-Organizing Networks*, *MANET*, *WSN*, *WMN*, *VANET*, Auerbach Publications, Boston, 195-225. http://dx.doi.org/10.1201/EBK1439819197-12

[25] Papadimitratos, P. and Haas, Z.J. (2003) Secure Link State Routing for Mobile *Ad Hoc* Networks. *IEEE Symposium on Applications and the Internet*, 27-31 January 2003, 379-383.

[26] Ilyas, M., Ed. (2002) The Handbook of *Ad Hoc* Wireless Networks. CRC Press, Boca Raton.

[27] Burg, A. (2003) *Ad Hoc* Network Specific Attacks. In: *Seminar Ad Hoc Networking*: *Concepts*, *Applications*, *and Security*, Technische Universitat Munchen, Munich.

[28] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Royer, E.M.B. (2002) A Secure Routing Protocol for *Ad Hoc*

Networks. *Proceedings of the* 10*th IEEE International Conference on Network Protocols*, Paris, 12-15 November 2002, 78-87. http://dx.doi.org/10.1109/icnp.2002.1181388

[29] Li, H., Chen, Z., Qin, X., Li, C. and Tan, H. (2002) Secure Routing in Wired Networks and Wireless *Ad Hoc* Networks. Technical Report, Department of Computer Science, University of Kentucky, Lexington.

[30] William, S. and Stallings, W. (2006) Cryptography and Network Security: For VTU, 4/e. Pearson Education, India.

[31] Rajavaram, S., Shah, H., Shanbhag, V., Undercoffer, J. and Joshi, A. (2002) Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile *Ad Hoc* Networks. In: *Proceedings of the Student Research Conference*, University of Maryland at Baltimore County (UMBC), Baltimore County.

[32] Douligeris, C. and Mitrokotsa, A. (2004) DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. *Computer Networks*, **44**, 643-666. http://dx.doi.org/10.1016/j.comnet.2003.10.003

[33] Perkins, C. (1998) *Ad Hoc* On-Demand Distance Vector (AODV) Routing. *IEEE Internet Computing*, **2**, 58-69.

[34] DeCleene, B., Dondeti, L., Griffin, S., Hardjono, T., Kiwior, D., Kurose, J., *et al.* (2001) Secure Group Communications for Wireless Networks. *Proceedings of the IEEE Military Communications Conference*, *Communications for Network-Centric Operations*: *Creating the Information Force*, **1**, 113-117.

[35] Sun, B., Wu, K. and Pooch, U.W. (2004) Towards Adaptive Intrusion Detection in Mobile *Ad Hoc* Networks. *Proceedings of the IEEE Global Telecommunications Conference*, **6**, 3551-3555.

[36] Florian, D. (2008) Security Concepts for Robust and Highly Mobile Ad-hoc Networks. April.

[37] Lee, S., Han, B. and Shin, M. (2002) Robust Routing in Wireless *Ad Hoc* Networks. *Proceedings of the International Conference on Parallel Processing Workshops*, Vancouver, 20-23 August 2002, 73-78.

[38] Lazos, L., Liu, S. and Krunz, M. (2009) Mitigating Control-Channel Jamming Attacks in Multi-Channel *Ad Hoc* Networks. *Proceedings of the Second ACM Conference on Wireless Network Security*, Zurich, 16-19 March 2009, 169-180. http://dx.doi.org/10.1145/1514274.1514299

[39] Noubir, G. and Lin, G.L. (2003) Low-Power DoS Attacks in Data Wireless LANs and Countermeasures. *ACM SIGMOBILE Mobile Computing and Communications Review*, **7**, 29-30. http://dx.doi.org/10.1145/961268.961277

[40] Xu, W., Trappe, W., Zhang, Y. and Wood, T. (2005) The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In: *Proceedings of the* 6*th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ACM Press, New York, 46-57. http://dx.doi.org/10.1145/1062689.1062697

[41] Xu, W., Wood, T., Trappe, W. and Zhang, Y. (2004) Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In: *Proceedings of the* 3*rd ACM Workshop on Wireless Security*, ACM Press, New York, 80-89. http://dx.doi.org/10.1145/1023646.1023661

[42] Wood, A.D., Stankovic, J. and Son, S.H. (2003) JAM: A Jammed-Area Mapping Service for Sensor Networks. *Proceedings of the* 24*th IEEE Real-Time Systems Symposium*, Cancun, 3-5 December 2003, 286-297. http://dx.doi.org/10.1109/REAL.2003.1253275

[43] Pullen, J. and Wood, D. (1995) Networking Technology and DIS. *Proceedings of the IEEE*, **83**, 1156-1167.

[44] Omura, J.K. (1994) Spread Spectrum Communications Handbook. Volume 2, McGraw-Hill, New York.

[45] Fadlullah, Z.M., Taleb, T. and Schöller, M. (2010) Combating against Security Attacks against Mobile *Ad Hoc* Networks (MANETs). In: Pathan, A.S.K., Ed., *Security of Self-Organizing Networks*, *MANET*, *WSN*, *WMN*, *VANET*, Auerbach Publications, Boston, 173. http://dx.doi.org/10.1201/ebk1439819197-11

[46] Gokhale, V., Ghosh, S.K. and Gupta, A. (2010) Classification of Attacks on Wireless Mobile *Ad Hoc* Networks and Vehicular *Ad Hoc* Networks. In: Pathan, A.S.K., Ed., *Security of Self-Organizing Networks*, *MANET*, *WSN*, *WMN*, *VANET*, Auerbach Publications, Boston, 195-225. http://dx.doi.org/10.1201/EBK1439819197-12

[47] Feldman, M., Papadimitriou, C., Chuang, J. and Stoica, I. (2006) Free-Riding and Whitewashing in Peer-to-Peer Systems. *IEEE Journal on Selected Areas in Communications*, **24**, 1010-1019. http://dx.doi.org/10.1109/JSAC.2006.872882

[48] Johnson, D.B. (2003) The Dynamic Source Routing Protocol for Mobile *Ad Hoc* Networks.

[49] Zhang, Y. and Lee, W. (2005) Security in Mobile Ad-Hoc Networks. In: Mohapatra, P. and Krishnamurthy, S.V., Eds., *Ad Hoc Networks*, Springer, New York, 249-268. http://dx.doi.org/10.1007/0-387-22690-7_9

[50] Gupta, V., Krishnamurthy, S. and Faloutsos, M. (2002) Denial of Service Attacks at the MAC Layer in Wireless *Ad Hoc* Networks. *Proceedings of the IEEE MILCOM*, **2**, 1118-1123. http://dx.doi.org/10.1109/milcom.2002.1179634

[51] Kyasanur, P. and Vaidya, N.H. (2003) Detection and Handling of MAC Layer Misbehavior in Wireless Networks. *Proceedings of the* 2003 *International Conference on Dependable Systems and Networks*, San Francisco, 22-25 June 2003, 173-182. http://dx.doi.org/10.1109/dsn.2003.1209928

[52] Radosavac, S., Benammar, N. and Baras, J.S. (2004) Cross-Layer Attacks in Wireless *Ad Hoc* Networks. *Proceedings of the* 2004 *Conference on Information Sciences and Systems*, Princeton, 17-19 March 2004, 1266-1271.

[53] Zimmermann, H. (1980) OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, **28**, 425-432. http://dx.doi.org/10.1109/TCOM.1980.1094702

[54] Lou, W. and Fang, Y. (2004) A Survey of Wireless Security in Mobile *Ad Hoc* Networks: Challenges and Available Solutions. In: Cheng, X.Z., Huang, X. and Du, D.-Z., Eds., *Ad Hoc Wireless Networking*, Springer, New York, 319-364. http://dx.doi.org/10.1007/978-1-4613-0223-0_9

[55] Hu, Y.C. and Perrig, A. (2004) A Survey of Secure Wireless *Ad Hoc* Routing. *IEEE Security & Privacy*, **2**, 28-39. http://dx.doi.org/10.1109/MSP.2004.1

[56] Gideon, N. and Edwin, B.K. (2014) Clustering Effects on Wireless Mobile *Ad-Hoc* Networks Performances. *International Journal of Computer Science & Information Technology* (*IJCSIT*), **6**, 1-19.

[57] Yi, S., Naldurg, P. and Kravets, R. (2001) Security-Aware *Ad Hoc* Routing for Wireless Networks. In: *Proceedings of the* 2nd *ACM International Symposium on Mobile Ad Hoc Networking & Computing*, ACM Press, New York, 299-302. http://dx.doi.org/10.1145/501416.501464

[58] Saini, A. and Kumar, H. (2010) Effect of Black Hole Attack on AODV Routing Protocol in MANET. *International Journal of Information Technology, Modeling and Computing* (*IJITMC*), **2**, 9-17.

[59] Li, W. and Joshi, A. (2008) Security Issues in Mobile *Ad Hoc* Networks—A Survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.

[60] Jawandhiya, P.M., Ghonge, M.M., Ali, M.S. and Deshpande, J.S. (2010) A Survey of Mobile *Ad Hoc* Network Attacks. *International Journal of Engineering Science and Technology*, **2**, 4063-4071.

[61] Chirala, A.P. (2010) Analysis and Diminution of Security Attacks on Mobile *Ad Hoc* Network. IJCA Special Issue on "Mobile Ad-Hoc Networks", MANETs, 105-110.

[62] Adjih, C., Raffo, D. and Mühlethaler, P. (2005) Attacks against OLSR: Distributed Key Management for Security. *Proceedings of the* 2nd *OLSR Interop/Workshop*, Palaiseau, 28-29 July 2005.

[63] Kannhavong, B., Nakayama, H., Kato, N., Nemoto, Y. and Jamalipour, A. (2006) Analysis of the Node Isolation Attack against OLSR-Based Mobile *Ad Hoc* Networks. *Proceedings of the* 2006 *International Symposium on Computer Networks*, Istanbul, 16-18 June 2006, 30-35. http://dx.doi.org/10.1109/iscn.2006.1662504

[64] Yi, P., Dai, Z., Zhang, S. and Zhong, Y. (2005) A New Routing Attack in Mobile *Ad Hoc* Networks. *International Journal of Information Technology*, **11**, 83-94.

[65] Kim, K. and Kim, S. (2007) A Sinkhole Detection Method Based on Incremental Learning in Wireless *Ad Hoc* Networks.

[66] Hu, Y.C., Perrig, A. and Johnson, D.B. (2003) Rushing Attacks and Defense in Wireless *Ad Hoc* Network Routing Protocols. In: *Proceedings of the* 2nd *ACM Workshop on Wireless Security*, ACM Press, New York, 30-40. http://dx.doi.org/10.1145/941311.941317

[67] Desilva, S. and Boppana, R.V. (2005) Mitigating Malicious Control Packet Floods in *Ad Hoc* Networks. *Proceedings of the IEEE Wireless Communications and Networking Conference*, **4**, 2112-2117. http://dx.doi.org/10.1109/wcnc.2005.1424844

[68] Mishra, A., Nadkarni, K. and Patcha, A. (2004) Intrusion Detection in Wireless *Ad Hoc* Networks. *IEEE Wireless Communications*, **11**, 48-60. http://dx.doi.org/10.1109/MWC.2004.1269717

[69] Hu, Y.C., Johnson, D.B. and Perrig, A. (2003) SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless *Ad Hoc* Networks. *Ad Hoc Networks*, **1**, 175-192. http://dx.doi.org/10.1016/S1570-8705(03)00019-2

[70] Jou, Y.F., Gong, F., Sargor, C., Wu, X., Wu, S.F., Chang, H.C. and Wang, F.Y. (2000) Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure. *Proceedings of the DARPA Information Survivability Conference and Exposition*, Hilton Head, 25-27 January 2000, 69-83.

[71] Douceur, J.R. (2002) The Sybil Attack. In: *Peer-to-Peer Systems*, Springer, Berlin Heidelberg, 251-260. http://dx.doi.org/10.1007/3-540-45748-8_24

[72] Chan, E.Y., Chan, H.W., Chan, K.M., Chan, V.P., Chanson, S.T., Cheung, M.M., *et al.* (2004) IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks. *Proceedings of the* 7th *International Symposium on Parallel Architectures, Algorithms and Networks*, Hong Kong, 10-12 May 2004, 581-586. http://dx.doi.org/10.1109/ISPAN.2004.1300541

[73] Brutch, P. and Ko, C. (2003) Challenges in Intrusion Detection for Wireless Ad-Hoc Networks. *Proceedings of the* 2003 *Symposium on Applications and the Internet Workshops*, Orlando, 27-31 January 2003, 368-373. http://dx.doi.org/10.1109/saintw.2003.1210188

[74] Parker, J., Patwardhan, A. and Joshi, A. (2006) Cross-Layer Analysis for Detecting Wireless Misbehavior. *Proceedings of the IEEE Consumer Communications and Networking Conference*, Las Vegas, 8-10 January 2006, 6-9. http://dx.doi.org/10.1109/ccnc.2006.1592977

[75] Zhang, Y., Lee, W. and Huang, Y.A. (2003) Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks*, **9**, 545-556. http://dx.doi.org/10.1023/A:1024600519144

[76] Perrig, A., Canetti, R., Tygar, J.D. and Song, D. (2000) Efficient Authentication and Signing of Multicast Streams over Lossy Channels. *Proceedings of the* 2000 *IEEE Symposium on Security and Privacy*, Berkeley, 14-17 May 2000, 56-73. http://dx.doi.org/10.1109/SECPRI.2000.848446

[77] Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000) Mitigating Routing Misbehavior in Mobile *Ad Hoc* Networks. In: *Proceedings of the* 6*th Annual International Conference on Mobile Computing and Networking*, ACM Press, New York, 255-265. http://dx.doi.org/10.1145/345910.345955

[78] Hu, Y.C., Perrig, A. and Johnson, D.B. (2003) Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, **3**, 1976-1986. http://dx.doi.org/10.1109/infcom.2003.1209219

[79] Huang, Y.A. and Lee, W. (2003) A Cooperative Intrusion Detection System for *Ad Hoc* Networks. In: *Proceedings of the* 1*st ACM Workshop on Security of Ad Hoc and Sensor Networks*, ACM Press, New York, 135-147. http://dx.doi.org/10.1145/986858.986877

[80] Hu, Y.C., Perrig, A. and Johnson, D.B. (2006) Wormhole Attacks in Wireless Networks. *IEEE Journal on Selected Areas in Communications*, **24**, 370-380. http://dx.doi.org/10.1109/JSAC.2005.861394

[81] Awerbuch, B., Holmer, D., Nita-Rotaru, C. and Rubens, H. (2002) An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In: *Proceedings of the* 1*st ACM Workshop on Wireless Security*, ACM Press, New York, 21-30. http://dx.doi.org/10.1145/570681.570684

[82] Dhillon, D., Zhu, J., Richards, J. and Randhawa, T. (2006) Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs. In: *Proceedings of the* 2006 *International Conference on Wireless Communications and Mobile Computing*, ACM Press, New York, 45-50. http://dx.doi.org/10.1145/1143549.1143560

[83] Hu, L. and Evans, D. (2004) Using Directional Antennas to Prevent Wormhole Attacks. *Proceedings of the Network and Distributed System Security Symposium*, San Diego, 5-6 February 2004, 131-141.

[84] Schreiber, F.R. (1973) Sybil. Regnery, Chicago.

[85] Qian, L., Song, N. and Li, X. (2005) Detecting and Locating Wormhole Attacks in Wireless *Ad Hoc* Networks through Statistical Analysis of Multi-Path. *Proceedings of the IEEE Wireless Communications and Networking Conference*, **4**, 2106-2111.

[86] Al-Shurman, M., Yoo, S.M. and Park, S. (2004) Black Hole Attack in Mobile *Ad Hoc* Networks. In: *Proceedings of the* 42*nd Annual Southeast Regional Conference*, ACM Press, New York, 96-97. http://dx.doi.org/10.1145/986537.986560

[87] Crepeau, C., Davis, C.R. and Maheswaran, M. (2007) A Secure MANET Routing Protocol with Resilience against Byzantine Behaviours of Malicious or Selfish Nodes. *Proceedings of the* 21*st International Conference on Advanced Information Networking and Applications Workshops*, Niagara Falls, 21-23 May 2007, 19-26.