A SCOPE FOR MANET ROUTING AND SECURITY THREATS

Lathies Bhasker T
Department of Computer Science and Engineering, Manonmaniam Sundaranar University, India
E-mail: lathiesbhasker@gmail.com

Abstract
The mobile Ad-hoc networks (MANET) are wireless networks which utilize mobile nodes for communicating among them and in the external transmission range. The vulnerable nature of the network causes various security threats which upset its growth. In this survey, initially the existing security attacks in MANET are analyzed. The attacks categories fall under two stages that include internal and external attacks. The former attack is due to the malicious nodes within the network and later attack is caused by the nodes which do not belong to the network. Then the secure, efficient dynamic routing techniques which are main issues concerned with ad hoc networks are surveyed. Overall, our survey mainly concentrates the existing security attacks and possible routing solution in MANET.

Keywords:
Proactive, Reactive, Hybrid, AODV, DSDV, Blackhoel, Wormhole

1. INTRODUCTION

Mobile Ad-hoc networks are wireless networks in which multi-hop links are used to make a communication between the mobile nodes. In this Mobile Ad-hoc network every node acts as like a router to forward the data packets to/from other nodes in the network. The MANET doesn’t have any base station or centralized coordinator [3].

The important feature of MANET is dynamic in network topology which changes often due to the mobility of the mobile nodes. The MANETs are used to construct a wireless communication topology without a centralized coordinator [1].

In wireless communication, the MANET is a challenging field for the researchers. Because of the rapid growth in mobile communication devices, the mobile Ad-hoc network becomes a more active field of communication systems. Some basic properties of the MANET, changes the networking technology become a great opportunistic for the researchers [2].

2. ATTACKS IN MANET

2.1 CLASSIFICATION OF ATTACKS

The threats for MANETs are classified as follows.

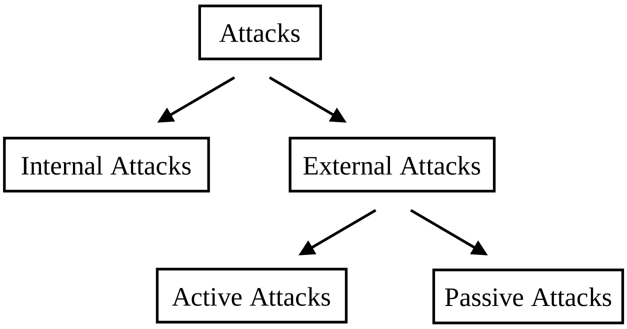


Fig.1. Attacks Classification

Giving security to the Mobile Ad-hoc Network is a difficult task. In order to given better solution for security attack, First we must identify and understand about the attack. Because of the unavailability of centralized coordinator in MANET, the security is a challenging task in wireless communication. The security attack classification is given below:

1. Internal Attack: The internal attacks are initiated from the compromised nodes in the mobile Ad-hoc network. In here the attacker node gets the unauthorized access and showing that as a normal mobile node. It analyses the data flows between the nodes in the network.
2. External Attack: These attacks are created by the nodes that are outside the network. It creates wrong routing information or service unavailability [2].

The External Attacks have two different classifications. They are:

- Active Attack
- Passive Attack

2.1.1 Active Attacks:

The active attacks are harmful one this attacks prevent the data flows between the source and destination nodes. This active attack either may be internal or external. The active external attacks created by the nodes which belong to the outside of the network. The internal attacks are more harmful and difficult to detect. This internal active attacks are created by the malicious nodes which are belongs to the network. These attacks are more supported for the attackers to modify the data packets and that creates the congestion in the network. In here the malicious node modify the routing information and advertise its wrong routing path as the best routing path.

2.1.2 Passive attacks:

The passive attack does not create any changes in the rouging data packet. It just monitors the network traffic. It does not affect the routing protocol operation but listen the protocol’s routing functionality. In order to avoid this type of attacks we need strong encryption and decryption algorithms for data transmission [4].

2.2 TYPES OF ATTACKS ON VARIOUS LAYERS

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack [4].

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing,

	Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Evasdropping, Jamming active interference.

2.2.1 Wormhole Attack:

This Wormhole attack is one of the harmful attacks in mobile Ad-hoc network in which the intruder makes a tunnel between two malicious nodes. The tunnel between two attacker nodes is called as wormhole. In here the data recorded at one node is relayed to the other end of the tunnel and this data will re-broadcasted to the network. Detecting the wormhole attack is a challenging issue. In this worm hole attack the attacker attacks without revealing their identities.

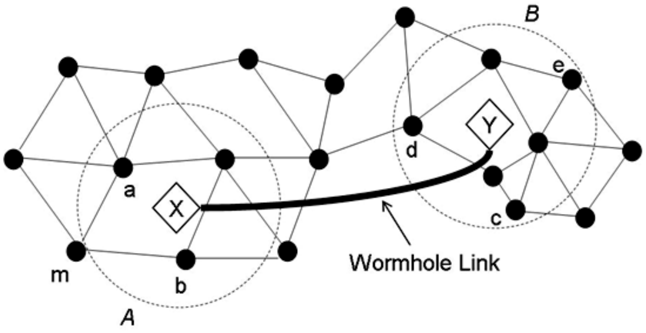


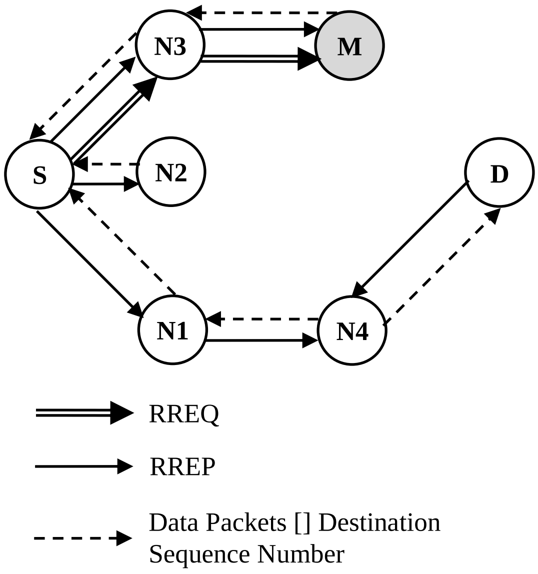
Fig.2. Wormhole Attack

In Fig.2, X and Y are wormhole nodes. These wormhole nodes are connected together by a link (tunnel). The nodes which are present in area A and B consider they are neighbors [24].

2.2.2 Black hole Attack:

The node which responds positively with a RREP message for every RREQ in spite of an invalid route to the destination, that node is called as a black hole. It is not necessary for the black hole to check its routing table and in turn it is capable of responding first to the RREQ in most of the cases. The source node transmits data via the black hole node which in turn drops all the data packets and thus they are not forwarded to the destination. Thereby network traffic occurs when the malicious node diverts the route. The malicious node has to put a little effort in order to create this attack. The black hole nodes form a group and work.

In Fig.3, the freshness of a particular route is determined by the Destination Sequence Number which is a 32 bit integer coupled with every route. The node N3 sends it to another node. The RREQ control messages are broadcasted by node N1 and N2 since they do not have a route to node D. There is a possibility for the node N3 to broadcast RREQ control messages to the node M which is assumed to be a malicious node. This in turn leads to false RREP control message generated by node M and this sends a very high destination sequence number at the same time. However the destination sequence number is high in simple AODV, thus the route from node N3 is taken as a fresh route and it receives data packet from the node S [25].



S <<= Source Node
D <<= Destination Node
M <<= Malicious Node

Fig.3. Black hole Attack

3. ROUTING PROTOCOLS IN MANET

The Simulation modeling has become a helpful tool for understanding the operation of mobile ad hoc network. This is due to nature of the network. During the past few years, determination of optimized routes from a source to some destination in Ad hoc network is considered effectively and multiple routing protocols were also developed. The transmission range is limited and thus the data transmission between the two nodes can be established using multiple hops. The situation becomes worse due to the mobility of the different nodes. The following features are essential for a protocol to be used in the Ad Hoc network:

- Adaptation of topology changes is essential for the protocol and it should also provide Loop free routing.
- The congestion problem can be controlled by the protocol by providing multiple routes from the source to destination.
- The exchange of routing information causes topology changes to occur, so the protocol should have minimal control messages.
- The protocols may become invalid after sometime, so it has to be allowed for quick establishment of routes [5].

3.1 ROUTING PROTOCOLS TERMINOLOGY

The information about the linking node and neighbors are maintained by the routing table developed by the routing protocol. Both the wired and wireless networks consist of several routing protocols which are classified into four distinct categories based on their properties:

A. Centralized Vs. Distributed

The route selection for centralized algorithms and distributed algorithms are different. Selection is made at central node in centralized algorithm while, in the later algorithm the selection of route is shared among the network nodes.

B. Static Vs. Adaptive

The route used by source destination pairs in the static algorithms is fixed being independent of traffic conditions. The node or link failure response is considered for the change of the route for transitions. In a wide variety of traffic input patterns, high throughput cannot be achieved by these algorithms. The major packet networks changes the route t\between the source and the destination since it uses some kind of adaptive routing.

C. Flat Vs. Hierarchical

A flat routing approach can be established by the flat addressing. Each and every node in the routing is responsible as it plays a major role and no special nodes are considered. Hierarchical routing is quite different from the flat as it gives responsibility for each network node separately. [8]

D. Proactive Vs Reactive Vs Hybrid

The Ad-hoc routing protocols are classified as follows.

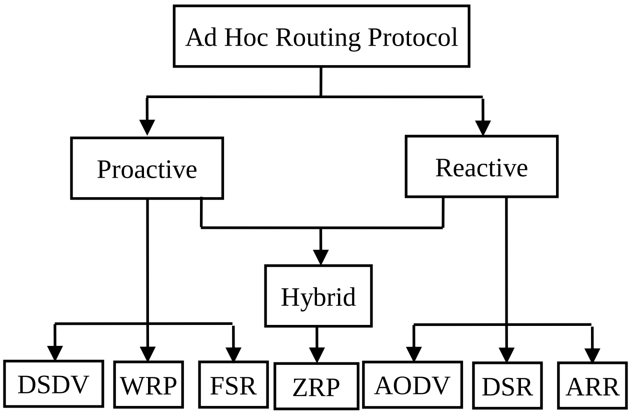


Fig.4. Routing Protocol Classification

1. Proactive or table driven routing protocols
2. Reactive or on-demand routing protocols
3. Hybrid routing protocols [7]

3.1.1 Proactive (Table Driven) Routing Protocols:

The information given by the table driven protocols are consistent and up to date when it is transmitted from each node to the other nodes in the network. In order to maintain the consistency the routing information is stored in a number of different tables and when the updates are propagated, these respond to the changes in the network topology. Traditional routing protocols are the basis for the proactive routing approaches which are designed for ad hoc networks. The routing information is maintained in the tables and thus they are named as table driven protocols. The major advantage of these protocols is that the routes are available as soon as they are required. But the control overhead is significant in large networks or in networks with rapidly moving nodes which happens to be a primary disadvantage. Destination-Sequenced Distance-Vector (DSDV) protocol, Wireless Routing Protocol (WRP), Optimized Link State Routing Protocol (OLSR) etc are included in the proactive routing protocols [7].

Advantages

- Routing information already present, reduce latency in the network.
- High storage capacity due to the routing tables.

Disadvantages

- They are not suitable for large networks
- Overhead is high
- Cost of maintaining the network is high, if network topology changes frequently [9].

3.1.2 Reactive (On-Demand) Routing Protocol:

The reactive routing approach does not maintain a continuous route between all pairs of network nodes and thus it is different from the traditional internet routing. Here routes are established as and when required. The route table has to be checked by the source node when it has to send the data packets to some destination which makes the route discovery on-demand. The introduction of route acquisition latency is the disadvantage to reactive approaches. Some finite latency has to be present when a route is required by the source node. But in a proactive approach, whenever the routes are needed they are present which speeds up the data session. Dynamic Source Routing (DSR) protocol, Ad hoc on-demand Distance Vector (AODV) protocol, Ad hoc On-demand Multiple Distance Vector (AOMDV) protocol etc are the protocols included in the Reactive routing protocol [7].

Advantages

- Low routing overhead
- Periodic updates not required

Disadvantages

- Latency is high in the network
- Not suitable for large networks
- Low storage capacity [9].

3.1.3 Hybrid Routing Protocol:

The combination of both proactive and reactive protocols is known as hybrid routing protocol. The disadvantages of proactive and reactive protocols like large overhead and latency are effectively overcome in these protocols. The number of nodes in the network is divided into zones in this protocol. Inside the routing zones, a proactive approach is used and in between the routing zones, a reactive approach is used. ZRP, SHRP are the examples of hybrid routing protocols.

Advantages

- Suitable for large networks
- Requires less overhead as compare to proactive routing protocols
- Latency is low as compare to reactive routing protocol

Disadvantages

- Increases complexity in the network [9].

3.2 DESTINATION SEQUENCED DISTANCE VECTOR (DSDV) PROTOCOL

The conventional Bellman-Ford routing algorithm has been modified and a proactive routing protocol has been established known as destination sequenced distance vector (DSDV) routing protocol. At each of the node, a new attribute, sequence number is added by the protocol. The node transmits the packets to other nodes in the network, with the help of the routing table maintained at each node. This protocol is mainly used for the data exchange along changing and arbitrary paths of interconnection. The interconnections are not close to any base station.

3.2.1 Protocol Overview and Activities:

In order to transmit packets and for connectivity to different stations in the network, routing table is maintained in each node in the network. The available destinations and the number of hops required to reach the destination in the routing table are listed in this table. The destination station provides a sequence number which is used for tagging the routing entry. The station transmits and updated its routing table at regular intervals in order to maintain the consistency. With the information of broadcasted packets, the accessible stations and the number of hops required to reach the particular station can be determined. The packets may be transmitted containing the layer2 or layer 3 addresses. When the nodes move within the network, the packets are transmitted periodically and the routing information is advertised by broadcasting or multicasting the packets. The routing table of the each mobile station has to be advertised by the DSDV protocol. Frequent update of the advertisement is essential, since the entries in the table changes very quickly. There should exist a possibility that the nodes should be able to locate its neighbors in the network by assigning shortest number of hops for a route to a destination. The new sequence number and the following information are maintained by the data broadcasted in each node.

- The destination address
- The number of hops required to reach the destination and
- The new sequence number, originally stamped by the destination

The hardware addresses, network address of the mobile host are also transmitted along with the routing tables. The transmitter created the sequence number and they are stored in the routing tables. Thus the forwarding decisions are made based on the new destination sequence number. All the hosts are updated with the new sequence number in order to decide on how to maintain the routing entry for that originating mobile host. Metric is incremented after receiving the route information and it transmits the information by broadcasting. Incoming packet has to travel one more hop before reaching the destination which is the reason for incrementing the metric before transmission. One more factor which is important here is the time between broadcasting the routing information. When the mobile host receives the new information, it will be retransmitted soon which causes most rapid possible dissemination of routing information among all the cooperating mobile hosts. When the mobile host moves from place to place within the network, it causes broken links. Layer2 protocol which is also known as infinity is used to detect the broken link. A metric is assigned as a infinity metric when the route is broken which determines that there is no hop and the sequence number is updated. Even sequence numbers are those which are originating from the mobile hosts and odd sequence numbers are those which are generated to indicate infinity metrics.

Advantages of DSDV

- DSDV protocol guarantees loop free paths.
- Count to infinity problem is reduced in DSDV.
- We can avoid extra traffic with incremental updates instead of full dump updates.
- Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Limitations of DSDV

- Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.
- DSDV doesn't support Multi path Routing.
- It is difficult to determine a time delay for the advertisement of routes.
- It is difficult to maintain the routing table's advertisement for larger network. Each and every host in the network should maintain a routing table for advertising. But for larger network this would lead to overhead, which consumes more bandwidth [11].

3.2.2 Ad-Hoc On-Demand Distance Vector (AODV) Routing Protocol:

Ad hoc On-Demand Distance Vector (AODV) created path to destination when required and is also known as reactive routing protocol. Only after certain nodes send route discovery message the routes are built so that it communicates or transmits data with each other. The source node, the destination node, and the intermediate nodes along the active route which deals with data transmission alone store the routing information. Memory overhead is decreased; use of network resources is minimized, and run well in high mobility situation. Three main procedures are involved in the AODV communication, path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packet are shown in the following table.

I. RREQ field

Source_ address	Source_seq uence	Broadca st_Id	Destination _address	Destination_ sequence	Hop_ Count

I. RREP field

Source_ address	Destination_ Address	Destination_ sequence	Hop_Count	Lifetime

The route discovery procedure is issued when the source node wants to establish the communication with the destination node. All the accessible neighbors of the intermediate node receive the RREQ request. The intermediate node checks the request RREQ and if it's the destination node, the request from the source will be forwarded to other neighbor nodes. Each node stores the broadcast identifier before forwarding the packet and previous node number from which the request came. When there is no reply timer is used by the intermediate nodes to delete the entry. Intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from are kept when reply is received. In order to detect whether the node has received the route request message previously or not, the broadcast identifier and the source ID are used. . It prevents redundant request receive in same nodes. The source node selects the message based on the hop counts when more than one reply is received. The routing table is invalidated if the link breaks down due to node mobility. When the link is lost, all the destination will become unreachable and route error message is created which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Route discovery is reinitiated once the source receives the RERR, if it still required the route [10].

3.2.3 Zone Routing Protocol (ZRP):

In mobile ad hoc network, the Zone Routing Protocol (ZRP) is a hybrid routing protocol. The control overhead of proactive routing approaches is reduced and the latency caused by route search operations in reactive routing approaches is decreased in the hybrid protocols. Zone Routing Protocol (ZRP) is a structure of hybrid routing protocol suites, which is prepared with the following modules, first is Intra-zone Routing Protocol, second one is Inter-zone Routing Protocol, and last one is Border cast Resolution Protocol.

ZRP refers to the locally proactive routing component as the Intra-zone Routing Protocol (IARP). Inter-zone Routing Protocol (IERP) is the globally reactive routing component. IERP and IARP are not specific routing protocols. A family of limited-depth, proactive link-state routing protocols includes IARP. Routing information for nodes that are within the routing zone of the node is maintained by IARP. Similarly, IERP is a family of reactive routing protocols which enhances the route discovery and route maintenance services based on local connectivity monitored by IARP [12].

4. SECURITY METHODOLOGIES AND SOLUTIONS FOR ROUTING PROBLEMS IN MANET

Farah Kandah et al. [13] have showed how an adversary can utilize the use of multiple nodes to create a colluding attack in MANET. An adversary can inject full controllable powerful malicious nodes in the network, by hiding their identities from other legitimate nodes in the network. This attack is named as the Colluding Injected Attack (CIA). Severe attack in the network which leads to prevent a specific node from receiving any packet is caused when the injected node works together. Hidden terminal problem leading to collision at an arbitrary node is caused, which in turn results in making the attacked node unable to receive or relay any packet. Also the CIA attack in a neighborhood aims to delude the watchdogs nodes (nodes that used to monitor the behaviors of other nodes in a neighborhood) in wrongly reporting the attacked node (the legitimate node) as behaving maliciously in this neighborhood. Previously proposed detection schemes are unable to mitigate the effect or detect their proposed colluding injected attack (CIA) in MANET, as shown in this work.

Arif Sar et al. [14] have proposed a method applied for preventing and mitigating jamming attacks which is implemented at the MAC layer that consist combination of different coordination mechanisms. Request to Send (RTS) collision problem causes the network throughput may degrade, for that reason RTS/CTS fragmentation thresholds are also involved into this mechanism. The transmissions of the nodes on the common transmission medium are coordinated in the Wireless medium access control (MAC) protocols. The IEEE 802.11 working group proposed two different algorithms for contention resolution. Distributed Coordination Function (DCF) which is completely distributed and the Point Coordination Function (PCF) that has a centralized access protocol are the two mentioned algorithms. The PCF requires a central decision maker such as a base station while DCF uses a carrier sense multiple access/collision avoidance protocol (CSMA/CA) for resolving channel contention among multiple wireless hosts. The malicious or selfish nodes are not forced to follow the normal operational functions of the protocols. The method implemented in this research study is PCF since in the link layer; a selfish or malicious node could interrupt either contention-based MAC protocols. A malicious jammer may also corrupt the frames easily by injecting some bits into the radio channel or launch DoS attack by exploiting the binary exponential backoff scheme. In order to prevent and secure the network from hidden jammer node attacks and prevent collisions on the network, the Request to Send/Clear to Send (RTS/CTS) mechanism is also implemented. The RTS/CTS mechanism is a handshaking process that minimizes the occurrence of collisions when hidden nodes are operating on the network.

Sowmya K.S et al. [15] have considered a fundamental security problem in MANET to protect its basic functionality. This is used to deliver data bits from one node to another. A virtual set of connections between each other is created by the nodes in conveying information to and from and thereby creating a virtual set of connections between each other. Routing protocols play very vital role in the creation and maintenance of these connections. In contrast to wired networks, each node in an Ad-hoc networks acts like a router and forwards packets to other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is a blurry boundary separating the inside network from the outside world. A novel method has been designed to detect blackhole attack: ACO, which isolates that malicious node from the network. They have complemented the reactive system on every node on the network. This agent stores the Destination sequence number of incoming route reply packets in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval. Their solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation.

Kavuri Roshan et al. [16] have proposed a novel period-based defence mechanism (PDM) against data flooding attacks taking enhancing the throughput of burst traffic into account. The basis for the proposed PDM scheme is on periods and uses a blacklist to efficiently prevent the data flooding attack, as a result of which many data packets are forwarded at a high rate for the whole duration.

Kavitha Ammayappa et al. [17] have proposed a new secure route discovery protocol for MANETs that overcomes the vulnerabilities of Ariadne and Endair A, due to hidden channel attacks. It uses 'authentic neighborhood' for route discovery process which potentially protects hidden channels of routing control packets, besides ensuring authenticity and integrity of routing control messages at hop-by-hop level. This authentic neighborhood is augmented by a process of traceability which uses promiscuous mode of a node to detect, diagnose and isolate the adversarial nodes that disrupt the route discovery process. They have observed, from the comparative analysis of the proposed protocol with Ariadne and Endiar A, that the proposed protocol has a balance between security and computational overhead.

Saurabh Upadhyay et al. [18] propose an approach to detect wormhole in MANET by using average time delay to detect anomalies based on statistical information of packets in the networks. Three features of the network are monitored including: the number of incoming packets, the number of outgoing packets and the average route discovery time related to each node, throughput of the network, retransmission attempts and load on the network. The network is having wormhole attacks if any abrupt change of one of these features is reported. The proposed algorithm is light weight and low computation overhead.

The proposed wormhole attack model method works without any extra hardware requirements, the basic idea behind this work is that the wormhole attack reduces the length of hops and the data transmission delay. The steps of proposed algorithm are as follows,

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

G. Indirani et al. [19] have proposed a defense mechanism against malicious attacks in mobile ad hoc networks (MANET). In this technique, multiple paths are established among source and destination for data transmission using swarm intelligence of ant colony optimization. In the selected routes, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using ant agents. Each active node monitors its neighbour nodes within its transmission range and collects the trust value from all monitored nodes. The active nodes adaptively changes as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious. Upon detecting malicious node, the active node sends an alert message to the source node. When the source node wants to forward the data packet to D, it discards the malicious nodes in that path and bypasses the data through other nodes in alternate selected path towards D and performs the certificate revocation process for defending against the malicious nodes.

T. Sakthivel et al. [20] have proposed Path Tracing (PT) algorithm for detection and prevention of wormhole attack as an extension of DSR protocol. The PT algorithm runs on each node in a path during the DSR route discovery process. It calculates per hop distance based on the RTT value and wormhole link using frequency appearance count. Every node in a path has to compute per hop distance of its neighbor with the previous per hop distance to identify the wormhole attack. The corresponding node detects the wormhole if per hop distance exceeds the maximum threshold range. In the routing process, the wormhole link participates in more number than the normal link. This factor is used to detect the wormhole link using a link frequent appearance count.

Reena Karandikar et al. [21] have proposed by providing some addition features to SendReply function and ReceiveReply function of AODV protocol, which has a new valid route. For doing the changes they have made a new function, named as sendSecureReply() and recvSecureReply() where trust based defense mechanism is being used to prevent Mobile Ad hoc network from black hole attack. In the recvAODV function they have made some changes in type of incoming packet. They have changed recvReply (RREP) with recvSecureReply (SREP). After adding secure reply (SREP) they have made changes in send Reply and receive Reply function. There name will be then changed as send SecureReply function and receivesecure Reply function. In this function they have added a new route by adding new pointer to AODV routing table. The new route is actually the entry of that node which comes along the selected route. It is like if the request message is coming from the legitimate node (source) than definitely it is a secure request, but if message is coming from any other node which belongs to the same route, may consist intermediate node, next hop node, companion node or any known node in the existing Ad hoc network. Then the route must be the secure route. But if a request message is coming from an unknown node which has never participated in any communication, then this route will not be the secure route, the request must be coming from a malicious node, selfish node or Black hole node.

Satish Salem Ramaswami et al. [22] have provided a framework for avoiding and eliminating colluding black hole attacks in the Ad hoc on demand Distance Vector (AODV) routing protocol. They have designed a lightweight acknowledgment mechanism that will ensure the proper data packet transmission and reception between the source and destination. The destination will relay the acknowledgement packets to the source through multiple paths only on the reception of a set of special packets. The transmission of the special packets by the source will be a random process so that the malicious node cannot detect the scheme even by eavesdropping.

Ziming Zhao et al. [1] have proposed a risk-aware response mechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation method. Their risk-aware approach is based on the extended D-S evidence model. In order to evaluate their mechanism, they have performed a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR).The major contributions of their paper are summarized as follows:

- They formally proposed an extended D-S evidence model with importance factors and articulate expected properties for Dempster's rule of combination with importance factors (DRCIF). Their Dempster's rule of combination with importance factors is nonassociative and weighted, which has not been addressed in the literature.
- They have proposed an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of their mechanism allows us to systematically cope with MANET routing attacks.
- They have evaluated their response mechanism against representative attack scenarios and experiments. Their results clearly demonstrate the effectiveness and scalability of their risk-aware approach.

Yingbin Liang et al. [23] have proposed to achieve secure communication over MANETs via an approach developed based on information- theoretic security. The idea is to apply the powerful secure coding developed in information-theoretic security to preprocess messages being transmitted through the network to guarantee secure communication in the presence of malicious nodes. The contributions of the paper are summarized below.

- They have identified equivalent wiretap models for MANETs with malicious nodes, which facilitate the application of the information-theoretic security approach for securing MANETs, and the corresponding theoretical analysis of fundamental secrecy rate limits.
- The messages transmitted securely between legitimate nodes can be viewed as secret keys, and hence symmetric keys are established between legitimate nodes over MANETs. This solves the open problem of key distribution for MANETs under a two-dimensional (2-D) independent and identically distributed (i.i.d.) mobility model.
- The fundamental limits of the secrecy rate can be characterized in terms of the order of the numbers of legitimate and malicious nodes in networks. These limits apply to all possible secure transmission schemes, including those implemented via cryptographic approaches.
- The information-theoretic approach they have proposed provides *provable* secure transmission (or key distribution) over MANETs.

All the above Attack types, security methodologies and their solutions are summarized in the following table.

Attack Type	Security Methodology	Solution
Balckhole Attack	ACO based security	Isolates the malicious node from the network
Data flooding Attack	Period-based defense mechanism(PDM)	It uses a blacklist to efficiently prevent the data flooding attack
Ariadne and EndairA (Due to channel Attack)	Authentic Neighborhood for route discovery process	This authentic neighborhood is augmented by a process of traceability which uses promiscuous mode of a node to detect, diagnose and isolate the adversarial nodes that disrupt the route discovery process.
Wormhole Attack	Average time delay	Three features of the network are monitored including: the number of incoming packets, the number of outgoing packets and the average route discovery time related to each node, throughput of the network, retransmission attempts and load on the network.
Malicious Attacks	Swarm Intelligence of Ant Colony Optimization	In the selected routes, the nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes using ant agents. Each active node monitors its neighbour nodes within its transmission range and collects the trust value from all monitored nodes. The active nodes adaptively changes as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious.
Wormhole Attack	Path Tracing(PT) Algorithm	. The PT algorithm runs on each node in a path during the DSR route discovery process. It calculates per hop

		distance based on the RTT value and wormhole link using frequency appearance count. Every node in a path has to compute per hop distance of its neighbor with the previous per hop distance to identify the wormhole attack
Colluding black hole Attack	Lightweight acknowledgement mechanism	The lightweight acknowledgement mechanism will ensure the proper data packet transmission and reception between the source and destination. The destination will relay the acknowledgement packets to the source through multiple paths only on the reception of a set of special packets. The transmission of the special packets by the source will be a random process so that the malicious node cannot detect the scheme even by eavesdropping.

5. CONCLUSION

This survey has elaborated the security attacks and routing principles in MANET. Initially the existing security attacks in MANET are analyzed. The attacks fall under two categories that include internal and external attacks. The former attack is due to the malicious nodes within the network and later attack is caused by the nodes which do not belong to the network. Then the secure, efficient dynamic routing techniques under proactive, reactive and hybrid protocol classes which are main issues concerned with ad hoc networks are surveyed. Overall, our survey has concentrated mainly on the existing security attacks and possible routing solution in MANET.

REFERENCES

[1] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn and Ruoyu Wu, "Risk-Aware Mitigation for MANET Routing Attacks", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 2, pp. 250-260, 2012.

[2] Priyanka Goyal, Viniti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", *International Journal of Computational Engineering & Management*, Vol. 11, pp. 32-37, 2011.

[3] Neetu Singh Chouhan and Shweta Yadav "Flooding Attacks Prevention in MANET", *International Journal of Computer Technology and Electronics Engineering*, Vol. 1, No. 3, pp. 68-72, 2011.

[4] Gagandeep, Aashima and Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology*, Vol. 1, No. 5, pp. 269-275, 2012.

[5] Amrit Suman, Praneet Saurabh and Bhupendra Verma, "A B.ehavioral Study of Wormhole Attack in Routing for MANET", *International Journal of Computer Applications*, Vol. 26, No. 10, pp. 42-46, 2011.

[6] Ammar Odeh, Eman AbdelFattah and Muneer Alshowkan, "Performance evaluation of AODV and DSR routing protocols in MANET Networks", *International Journal of Distributed and Parallel Systems*, Vol. 3, No. 4, pp. 13-22, 2012.

[7] Punardeep Singh, Harpal Kaur and Satinder Pal Ahuja, "Brief Description of Routing Protocols in MANETS And Performance And Analysis (AODV, AOMDV, TORA)", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 1, 2012.

[8] Anju Gill and Chander Diwaker, "Comparative Analysis of Routing in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, No. 7, 2012.

[9] Rajiv Chechi, Vikas Malik and Ompal Gupta, "Classification of Routing Protocols in MANET & their Pros & Cons: A Review", International Journal of Research in IT & Management, Vol. 2, No. 11, pp. 28-31, 2012.

[10] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", *International Journal of Computer Science, Engineering and Applications*, Vol. 2, No. 1, 2012.

[11] Vijayalakshmi M, Avinash Patel and Linganagouda Kulkarni, "QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network", *International Journal of Communication Network & Security*, Vol. 1, No. 4, pp. 62-70, 2011.

[12] M. Vijaya Lakshmi and S. Venkatachalam, "Comparative analysis of QoS routing protocols in MANETS: Unicast & Multicast", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 2, No. 4, pp. 242-250, 2012.

[13] Farah Kandah, Yashaswi Singh and Chonggang Wang, "Colluding Injected Attack in Mobile Ad-hoc Networks", *IEEE Conference on Computer Communications Workshops INFOCOM*, pp. 235-240, 2011.

[14] Arif Sari and Beran Necat, "Securing Mobile Ad-hoc networks against jamming attacks through unified security mechanism", *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, Vol. 3, No. 3, pp. 79-94, 2012.

[15] Sowmya K.S, Rakesh T and Deepthi P Hudedagaddi "Detection and Prevention of Blackhole Attack in MANET Using ACO", *International Journal of Computer Science and Network Security*, Vol. 12, No. 5, pp. 21-24, 2012.

[16] Kavuri Roshan, K. Reddi Prasad, Niraj Upadhayaya and A. Govardhan, "New-fangled Method against Data Flooding Attacks in MANET", *International Journal of Computer Science & Information Technology*, Vol. 4, No. 3, pp. 25-34, 2012.

[17] Kavitha Ammayappan, Vinjamuri Narsimha Sastry and Atul Negi, "A New Secure Route Discovery Protocol for MANETs to Prevent Hidden Channel Attacks", *International Journal of Network Security*, Vol. 14, No. 3, pp. 121-141, 2012.

[18] Saurabh Upadhyay and Aruna Bajpai, "Avoiding Wormhole Attack in MANET using Statistical Analysis Approach", *International Journal on Cryptography and Information Security*, Vol. 2, No. 1, pp. 15-23, 2012.

[19] G. Indirani and K. Selvakumar, "Swarm based Intrusion Detection and Defense Technique for Malicious Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Applications*, Vol. 50, No. 19, pp. 1-6, 2012.

[20] T. Sakthivel and R. M. Chandrasekaran, "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach", *European Journal of Scientific Research*, Vol. 76, No. 2, pp. 240-252, 2012.

[21] Reena Karandikar, Rashmit Kaur Khanuja and Surendra Shukla, "Proposed solution to prevent black hole attack in MANET", International Journal of Research in IT & Management, Vol. 2, No. 2, pp. 487-496, 2012.

[22] Satish Salem Ramaswami and Shambhu Upadhyaya, "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing", *Proceedings of IEEE Information Assurance Workshop*, pp. 253-260, 2006.

[23] Yingbin Liang, H. Vincent Poor and Lei Ying, "Secrecy Throughput of MANETs under Passive and Active Attacks", *IEEE Transactions on Information Theory*, Vol. 57, No. 10, pp. 6692-6702, 2011.

[24] Shilpa Jaiswal and Sumeet Agrawal, "A Novel Paradigm: Detection & Prevention of Wormhole Attack in Mobile Ad Hoc Networks", *International Journal of Engineering Trends and Technology*, Vol. 3, No. 5, pp. 571-573, 2012.

[25] Tamilselvan L and Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", *Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, pp. 21, 2007.