Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Issues in Manet: A Survey on Attacks and Defense Mechanisms

Tarunpreet Bhatia *
Department of Computer Science Engineering
Thapar University, India

A.K. Verma
Department of Computer Science Engineering
Thapar University, India

Abstract— ***Mobile Adhoc NETwork (MANET) is a collection of mobile nodes which can communicate directly with other nodes within its transmission range and use multihop routing for nodes outside its transmission range. The inherent features of MANETs like dynamic topology, limited network resources (bandwidth, memory and battery power) and lack of centralized trusted authority makes it more vulnerable to attacks than wired networks. The security of MANETs has drawn much attention of researchers these days because existing routing protocols did not incorporate security mechanisms. This paper outlines various security issues related to MANETs, attacks that can be launched and defense mechanisms available against these attacks. The focus of this work is on encompassing complete security solution that involves both reactive and proactive mechanisms.***

Keywords— ***Wireless Networks, MANET, Security Issues, Attacks, Defense Mechanisms***

I. Introduction

MANET (Mobile Adhoc NETwork) consists of mobile nodes which can move from one place to another at any speed and at any time. Adhoc network is formed on fly for temporary purpose. Nodes can directly communicate with other nodes within its transmission range over wireless channel and for the nodes outside its range, multihop routing is used. These nodes can both act as terminal or router and communicate with each other in a self organized way to forward the packets destined for nodes outside its transmission range. There is no centralized authority and fixed infrastructure so nodes themselves are responsible for route discovery and route maintenance. Wireless networks are more vulnerable to attacks than their wired counterparts because of inherent features like:

- Dynamic topology: Rapidly changing topology and membership of nodes. Nodes may leave a network at any time or new nodes can enter network so they cannot be trusted for critical network functions of packet forwarding and routing.
- No centralized authority: In wired networks dedicated nodes and trusted certification authority exists and an attacker has to access the physical medium to launch attack whereas in wireless no centralized authority exists to provide keys for authentication and integrity and an attacker can easily sniff on-going traffic.
- Limited Resources: Mobile nodes have limited resources like battery power, memory, computational power and bandwidth so cryptographic solutions are expensive.

The security framework for MANET must ensure following services:

- Confidentiality refers to hiding of information from unintended receivers.
- Integrity refers to delivery of message to the intended recipient as such without any modification or alteration.
- Authentication refers to assurance and identification of the origin of information.
- Availability states that services and resources must be provided to authorized nodes at all the time.
- Non repudiation ensures that nodes cannot deny later on for sending or receiving message.

II. Classification of Attacks

Nodes in MANET can be broken, malicious or selfish. Broken nodes become non functional due to some link failure so cannot forward the traffic that they earlier agree to forward. Malicious nodes aimed at disrupting the network by dropping the packets or launching denial of service attacks. Selfish nodes hinder the routing by dropping packets in order to conserve their energy and bandwidth. MANET found applications in military, disaster relief operations etc as it is easy to deploy. In order to encourage its use in future, it is important to ensure secure and reliable routing in MANET. Before providing security, we need to know attacks related to such networks. Security aspects were not considered when adhoc protocols were designed. Later researchers tried to incorporate security mechanisms on existing routing protocols. So this paper focuses on attacks and security mechanisms employed to safeguard against these attacks. Fig 1 gives classification of various attacks.

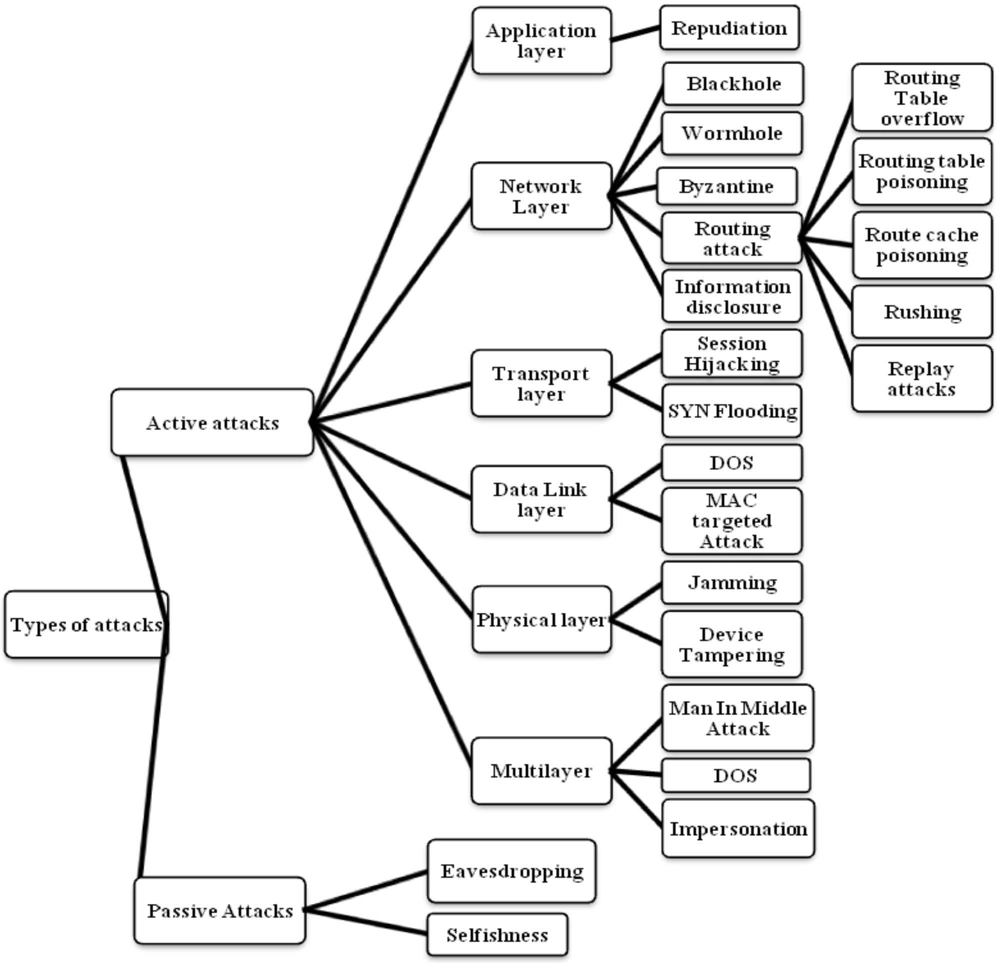

Fig 1 Classification of Attacks

Attacks can be classified into two broad categories.

A. Passive Attacks

The attacker just snoops the network without disrupting the network operation. These attacks compromise the confidentiality of the data and tell which nodes are working in promiscuous mode.

1) *Eavesdropping:* It is reading or snooping of messages by an unintended receiver. In MANET, the nodes share a wireless medium so nodes can easily overhear communication of the nodes within its transmission range. This attack can be prevented by using encryption.
2) *Selfishness*: A selfish node in order to save its battery life and resources does not participate in routing either by dropping the packets or not forwarding them.

B. Active Attacks

Attacks in which attacker disrupts the normal operation of the network by fabricating messages, dropping or modifying packets, replaying packets or tunnelling them to other part of the network. Basically, the content of message is modified. These can be internal attacks (caused by compromised nodes within the network) and external attacks (caused by the nodes outside the network). Active attacks can be further classified corresponding to different layers in MANET:

1) *Application Layer Attacks*

- *Repudiation*: It is an act of refusal in participating in all or part of the communication. For example, repudiation attack on a commercial system in which a selfish node can refuse conducting credit card purchase, or any on-line bank transaction.
- *Malicious Attack*: In this attack, a malicious node disrupts the normal operation of other nodes in the network by attacking the operating system. Malicious node sends virus, worm or Trojan horse to a victim node. A virus is a computer program that attaches itself to legitimate program causing damage to nodes and keeps spreading around the network. A Trojan horse silently sits behind legitimate program and allows an attacker to get some confidential information about a node or the network.

2) *Transport Layer Attacks*

- *Session Hijacking*: In this attack, an attacker gets access to the session state of a particular user by stealing session ID which is used to get into a system and snoops the data. Since most of the times authentication only occurs at the beginning of session, this allows an attacker to gain access to a node. Hijacking is done only after the victim node has established the connection. At first attacker predicts the correct sequence number and then spoofs victim's IP address. Meanwhile to take over the session attacker has to launch DoS attack against the victim. The victim node hangs and attacker communicates as if it is a legitimate system.

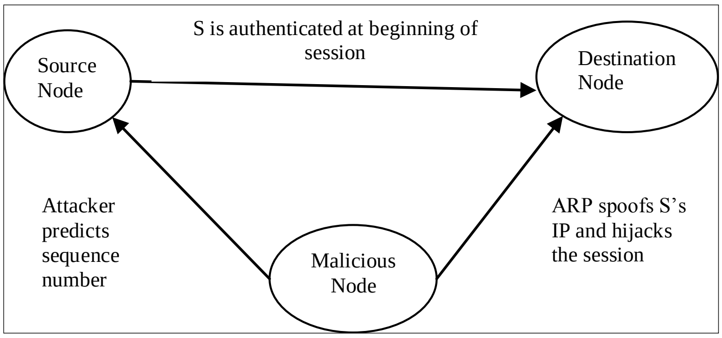
S is authenticated at beginning of session
Source Node
Destination Node
Attacker predicts sequence number
ARP spoofs S's IP and hijacks the session
Malicious Node

Fig 2 Session Hijacking Attack

- *SYN Flooding*: On the internet, nodes communicate using TCP/IP protocol so they need to establish connection using three-way handshake. A malicious node sends a huge number of SYN packets to a victim node. The victim node sends back SYN+ACK packets and keeps the entry for the incomplete connection request. The attacker never sends ACK so a large amount of memory of victim node is consumed for storing pending requests and node may come to a halt even. Another way of launching this attack is spoofing the return address of SYN packets with non-existent node so SYN+ACK packets never reach any node fooling the victim node.

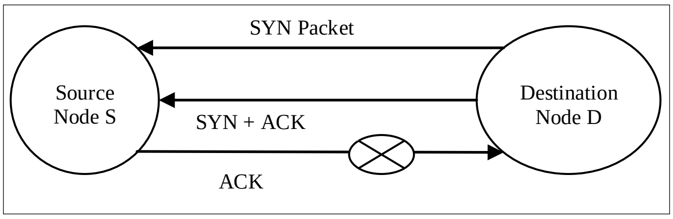

Fig 3 SYN Flooding Attack

3) *Network Layer Attacks*

- *Wormhole Attack*: In wormhole attack, two colluding nodes are involved and one node tunnels the packet to another node in the same network over a high speed private wired link or wireless link [1]. These packets are then resent from that location into the network. This tunnel between two malicious nodes is known as wormhole. This attack can easily be launched against communications that resort to authenticity and confidentiality. For example, consider an attack against AODV in Fig 4, an ad-hoc on demand reactive protocol, in which A1 and A2 are two colluding attackers. Source node S wants to communicate with destination node D so it initiates route discovery and broadcasts route request (RREQ) to its neighbours A1 and X. A1 receives RREQ from S and tunnels it to A2 after encapsulating it. A2 further forwards it to Z from where it reaches D. Since this RREQ passes through high speed private channel, this RREQ will reach destination D first. So the route S, A1, A2, D is chosen. The entire traffic pass through attackers and path with incorrect and low metric is chosen instead of paths with correct metric.

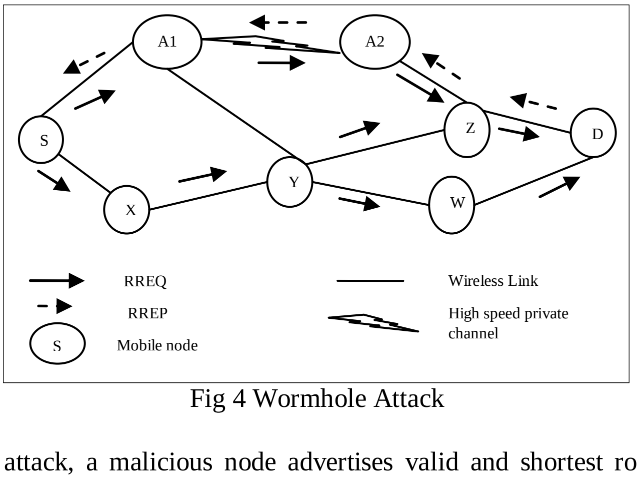

Fig 4 Wormhole Attack

- *Blackhole Attack*: In this attack, a malicious node advertises valid and shortest route to a victim node and thereafter secretly drops data and control packets as they pass through it. In order to have shortest route, blackhole node creates forged packet by modifying hop count and sequence number of the routing protocol message such as AODV. For example, source node S wants to communicate with destination node D. It broadcasts RREQ (route request) messages to its neighbours. An attacker M forges a reply packet by modifying hop count claiming that it has shorter route to D or by incrementing destination sequence number than the authentic value last advertised by D indicating it has fresher route to D refer Fig 5. This leads to the establishment of a fake route through the attacker when maliciously fabricated reply reaches S first than legitimate reply [2]. So, attacker node can eavesdrop or drop the packets. Malicious node is known as blackhole since it consumes data packets forwarded to it and never forwards them.

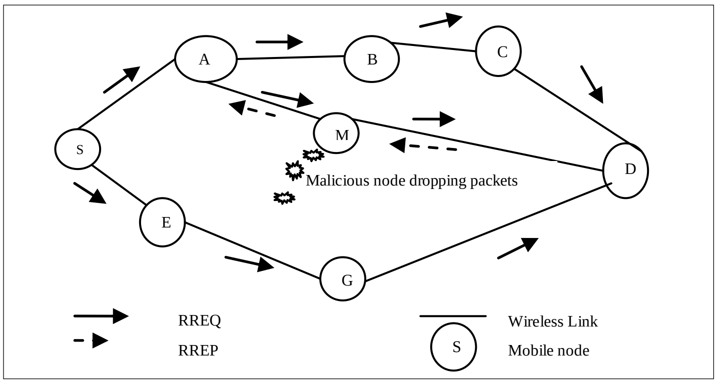

Fig 5 Blackhole Attack

- *Byzantine Attack*: This attack involves multiple attackers that work in collusion to degrade the network performance such as creating loops, selectively dropping packets, choosing non optimal paths for packet forwarding. In Fig 6, attacker A1 forwards routing packets of S normally to A2 but second attacker A2 drops or forges these routing packets. In [3] collusion attack in OSLR protocol is discussed and it has been shown that pair of colluding attackers can disrupt 100 % of data packets.

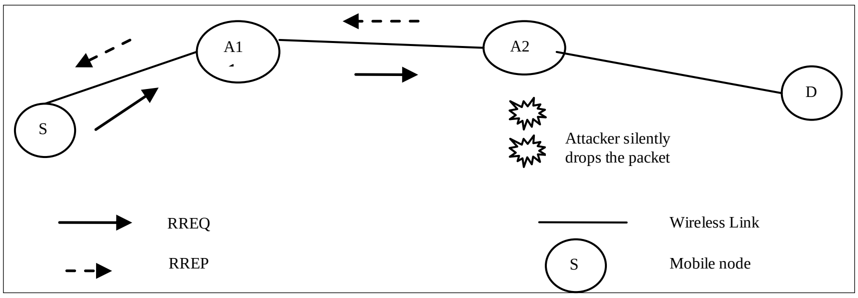

Fig 6 Byzantine Attack

- *Information Disclosure*: A compromised node may violate the confidentiality principle of security and disclose important information like private and public keys, status of nodes, passwords, optimal route to authorized nodes, geographic location of nodes and other control data in packet headers to unauthorized nodes present in the network. The location information revealed give better understanding of the network topology. Routing packets are then sent with inadequate hop-limit and ICMP error messages returned by the intermediate nodes are recorded [4]. So it gives blueprint of the network i.e. which nodes are situated in close proximity to the target node.
- *Routing Table Overflow*: This attack prevents creation of new legitimate routes by overflowing the routing table with routes to nonexistent nodes. This exploits the limited memory capacity of mobile nodes. A malicious node initiates route discovery to non-existent nodes so that limited memory of mobile node gets consumed by having such entries in their routing table which in turn prevents the creation of new routes to authorized nodes in the network. The proactive ad hoc protocols are more prone to this attack because in such networks, routes to all the nodes are already stored before they are needed, in contrast to reactive protocols in which information is discovered when needed.
- *Routing Table Poisoning*: In this attack, malicious node sends fabricated routing update and error messages or modified legitimate updates to authorized nodes in the network. It may result in forwarding packets along sub optimal routes, congestion in the network, formation of loops or blackmail attack in which an attacker sends false route error messages against benign node in order to report benign node as malicious and thus launching denial of service attack against it. In on demand ad hoc protocols, like AODV and DSR, there is separate route maintenance phase to deal with broken routes as nodes move or fail. Let a node S has route to node D via nodes X, Y and Z. A malicious node M can send RERR message to Y spoofing node Z, indicating that link between Z and D is broken so Y deletes corresponding entry for D from its routing table and forwards it to X. So M can successfully prevent traffic between S and D.

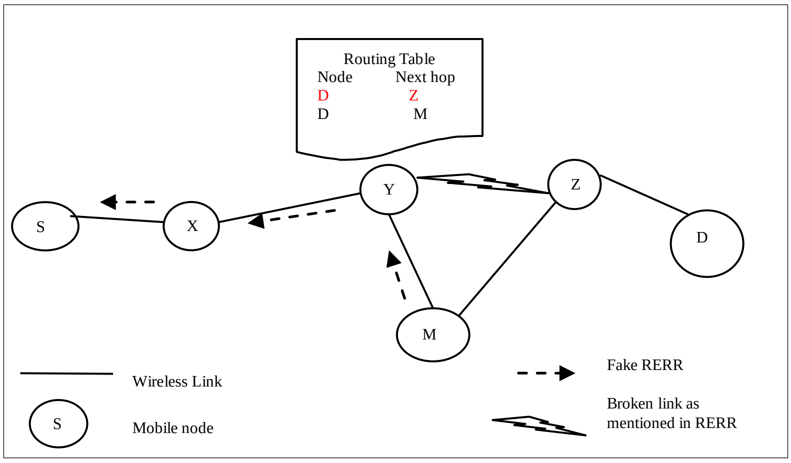

Fig 7 Routing table poisoning

- *Routing Cache Poisoning*: Route cache is maintained by on demand protocols like DSR that stores the routes known to it by overhearing neighborhood transmissions in the recent past. A malicious node can launch DOS attack on any node by simply broadcasting spoofed packets with source routes to D via itself. Any neighboring node overhearing the packet transmission adds the route entry in their route cache [5].
- *Replay Attack*: An attacker instead of modifying packet's contents just replay stale packets in order to exploit battery power, bandwidth and computational constraint of mobile nodes. It leads to congestion in the network and confusion among the routing nodes because of conflicting information, thus delaying packet delivery or preventing them from reaching destination.
- *Rushing Attack*: This attack involves entire network traffic to pass through an attacker. The source node is unable to find any secure route without the attacker. Malicious node after receiving RREQ packet from initiating node reacts immediately and floods the network quickly with these packets before other nodes receiving the same RREQ can react. Nodes receiving legitimate RREQ packets assume them as duplicates and discard them. So every route established has attacker as one of the intermediate nodes.
- *Jellyfish Attack*: It is a selective blackhole attack in which malicious node attacks the network by reordering packets, dropping selective packets or increasing jitter of the packets that pass through it in order to prevent it from being detected and it seems to the network that loss or delay is due to environmental reasons.

4) Data Link Layer Attacks

- *Denial of service*: There is a single wireless channel shared by all the nodes so a malicious node keeps this channel busy by sending false packets to drain node's battery power.
- *MAC targeted Attack*: In MANET, nodes share a wireless medium so medium access control (MAC) protocols are used to coordinate the transmission and to resolve the contention. These attacks disrupt the MAC procedure. For example, an attacker can corrupt the frames by introducing extra bits.

5) Physical Layer Attacks

- *Device Tampering*: Nodes in ad hoc wireless networks are small, compact and hand-held unlike wired devices so can be easily stolen or damaged.
- *Jamming*: The attacker monitors the wireless medium in order to find frequency at which destination node is receiving from sender node. An attacker must have powerful transmitter to sends the signals to the destination at that frequency, thereby interfering with its operations. The most common types of signal jamming are random noise and pulse.

6) Multilayer attacks: These attacks can be launched from several layers instead of a single layer. Examples of multi-layer attacks are jamming, denial of service attacks, impersonation attacks and man-in-the-middle attack.

- *Denial of service attack:* In this, an attacker renders a system unusable, or significantly slows it down for legitimate users by overloading its resources. The goal is that if an attacker can't access the node, it will crash the node. In wired networks, DoS is launched against centralized resource, so it is not available to other legitimate nodes. But in wireless networks there is no single centralized resource so there are many other ways by which it can be launched from several layers. At the physical layer, signal jamming disrupts normal communications. At the link layer, malicious nodes prevent other nodes from channel access. At the network layer, DoS attacks are mounted on routing protocols and disrupt the network performance through routing packets modification, selective dropping or routing table overflow. An example of DoS attack on DSR with modified source route is shown in Fig 8. In DSR, source nodes are explicitly stated in routes in data packets. The routing mechanism lacks integrity checks so DoS attack can be launched by modifying the source routes in packet headers. Assume a path exists from node S to node D and Y and D cannot overhear transmission of each other directly. Let M be a malicious node that wishes to launch DoS attack. S wishes to communicate with D and has an unexpired route in its route cache to D. S transmits a data packet toward D with the source route (S, X, M, Y, Z, D) contained in the packet's header. On receiving the packet from X, M alters the source route by deleting Z from the source route in packet's header. Consequently, when Y receives the modified altered packet, it attempts to forward the packet to D directly. Since Y cannot hear D, the transmission is unsuccessful. At the transport layer, SYN flooding and session hijacking can cause DOS attacks.

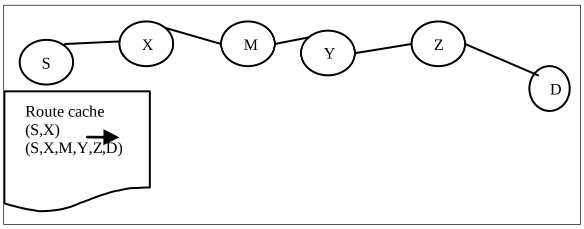

Fig 8 Denial of service Attack

- *Impersonation attacks:* Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further more sophisticated attacks. A malicious node can masquerade itself as an authorized user and give false routing information or change the configuration of the network. Examples of impersonation attack are Sybil attack and trust attack. In Sybil attack, a malicious node or entity has one physical device and forges multiple identities. A faulty node may present multiple identities to an ad-hoc network in order to function as multiple distinct nodes. After becoming part of the network, the adversary overhears communications or acts maliciously. In threshold scheme where a message or key shares are fragmented into different parts and each part takes different path, the attacker may get access to all pieces of fragmented information as it has imposed several different identities.
- *Man-in-the-middle attack:* An attacker sits quietly between the sender and the receiver and makes the actual communicator believe that they are talking to each other but in actual they are talking to the man-in-the-middle who is talking to each of them.

III. DEFENSE MECHANISMS

Fig 9 depicts the classification of defense mechanisms for securing MANET.

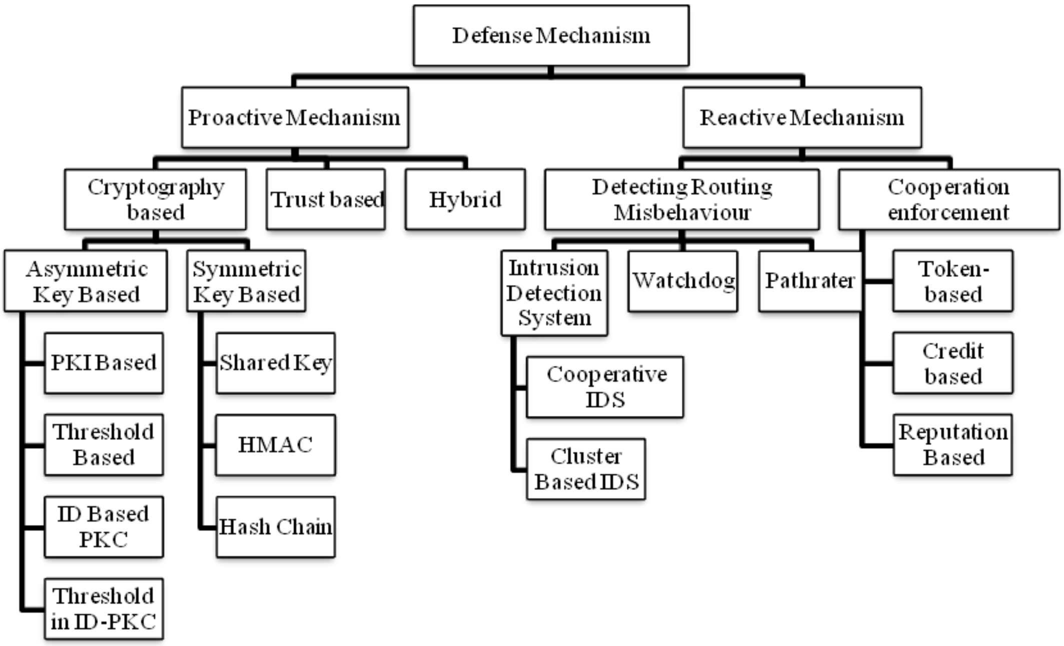

Fig 9 Defense Mechanisms

A. *Proactive Mechanism*

It consists of security-aware routing protocols which prevents occurrence of attacks. These protocols must take the environment features into consideration and form first line of defense as "prevention is better than cure". It includes cryptographic algorithms and trust based mechanism to ensure integrity, authentication and confidentiality of the messages.

1) *Cryptography Based Mechanism:* Traditional cryptography techniques still play a major role in the security of MANET. These techniques require a key distribution and key management mechanism to ensure secure and authenticated communication among the nodes and to prevent the integrity of the messages using digital signature, one way hash chains, symmetric key encryption, asymmetric key encryption, message authenticated

code (MAC), HMAC, identity based cryptography etc. Cryptography mechanisms in MANETs are classified into two broad categories:

Symmetric Key Cryptography: In this cryptography, same key is used for encryption and decryption. If attacker is successful in compromising the symmetric key of a group of certain users, then entire traffic encrypted for that group will be exposed. It cannot be used for integrity and non repudiation checks. Another promising and new research is based on DNA cryptography [6] that follows symmetric key algorithms in order to secure the information by converting it to DNA notation and then translate to mRNA form of data. Source node converts mRNA into proteins and sends over the secure channel along with the keys. Different techniques for implementing symmetric key cryptography are as follows [7]:

- Shared key: Commonly used algorithms are AES and IDEA for generating shared key. They are computationally less intensive as compared to asymmetric algorithms. The disadvantage of shared keys is that each node requires different key pair for communicating with every other node.
- HMAC message authentication code: It is calculated by applying a cryptographic hash function over the message along with a secret key to verify the message. The hash functions used mostly are MD5 or SHA-1 in MANETs as SHA-512 is expensive to compute in terms of resources. It also ensures that the message retains its original content by calculating the message HMAC using a secret key even if it is sent unencrypted. SRP [8] for DSR uses this approach for authentication and integrity.
- Hash chain: It is generated by a repeatedly applying a hash function on an input. Due to the one-way property of hash functions, it is infeasible to find input from output of hash function. In order to authenticate the message, outputs have to be used in reverse order of their generation. To compute any previous key Key_j from Key_i where $I < j$ we use $Key_i = H_{j-I}[Key_i]$. For example, SEAD [9] for DSDV, ARIADNE [10] for DSR uses one-way key chains.

Asymmetric key cryptography: There is a pair of public/private key for each node. Private key is used for encryption and that encrypted text is decrypted by corresponding public key. It has certain merits over symmetric, e.g., key distribution is comparatively easier, compromise of a private key of some user does not expose messages encrypted for other users in that group, authentication and non-repudiation are available. The only demerit is they are computationally expensive. Asymmetric key cryptography approaches are as follows:

- Traditional asymmetric cryptography widely used in the Internet relies on a Public Key Infrastructure (PKI). The success of PKI depends on the reliability, availability and security of a centralized point of control trusted by all i.e. Certificate Authority (CA). In MANETs, a central control point for employing PKIs is not feasible. Another obstacle in MANETs is the heavy overhead of transmission and storage of public key certificates (PKCs). If the CA is compromised, the entire network is exposed. Asymmetric key cryptography is used in ARAN [11], AC-PKI [12].
- Threshold cryptography provides robust security support for MANETs. The CA functions are distributed to several nodes through a threshold secret sharing mechanism because in MANET nodes cannot depend on central entity. This approach is very complicated to implement. Any node can join the network at any time and can act as server sharing load with existing servers. Rivest Shamir Adelman-Threshold Cryptography (RSA – TC) based scheme [13] ensures generation of public and private key pair randomly and private key is shared among several nodes. Encryption is done using public key and decryption using private key. Another public-key cryptosystem getting importance for MANET is Elliptic curve cryptography threshold cryptography (ECC-TC) [14] that can provide security equivalent to RSA with smaller key sizes resulting in faster computations and saving limited MANET resources like memory and bandwidth .
- Identity-based cryptography (IBC) [15] is a special form of public key cryptography. It eliminates the requirement of a CA and PKCs. In this, the identity information like email address is used as public key. Suppose, node A wants to communicate with node B. A knows B’s email address so with this public key messages for that node are encrypted and digital signatures are verified. Trust Authority (TA) generates private key for each node to decrypt and sign messages. IBC, with its fast development in recent years, provides promising solution for MANET security issues. Fang et al. [16] has given the merits of IBC over key based schemes- it is easier to deploy without any centralized infrastructure requirement and resource requirement is much lower like battery power, storage space, and communication bandwidth.
- Threshold in Identity-based Cryptography: In this network, master key pair shares are generated for each node in a distributed way. In <k, n> threshold system, private key corresponding to each node is generated by k nodes jointly. In order to have secure communication among nodes, they need to generate session key using their private key and other node’s public key. V. Daza proposed a protocol [17] in which nodes in MANET themselves are responsible for routing without relying on trusted third party. Each node gets a secret key/public key pair to be used for secure routing. This scheme is extended to threshold cryptography in which secret key SK corresponding to public key is computed by several nodes given by threshold value.

Demerits of using cryptography based solutions-

- Cryptographic algorithms are computation intensive and mobile nodes being resource constrained cannot perform such heavy computations.
- They assume pre-existence of centralized and distributed trusted authority which is not possible in MANET due to dynamic topology.

- Cryptographic solutions are ineffective against internal attacks like blackhole and grayhole [18].
- Though cryptography methods prevent certain attacks but at the same time they create opportunities for DoS attacks [19] as nodes in MANET have limited battery and computational power and can be easily kept in shutdown mode.

2) *Trust Based Mechanisms:* The demerits of key based cryptography along with trade-off between security and DoS attacks emerged as a new area of research these days. In this, secure routing protocols use trust as security metric to avoid inclusion of malicious or selfish nodes while establishing routes. Each node determines the trust it has on the other nodes by directly communicating with neighbouring nodes and also combining other nodes' recommendations. On the basis of nodes' trustworthiness, a node can decide whether to exchange routing information with it or not. Mostly trust based schemes [20, 21] use IDS for monitoring neighbourhood traffic but need buffering of packets which may consume computational resources. Another category is light-weight trust based routing in which there is no buffering of packets while monitoring neighbourhood traffic. Trust based routing consider different parameters such as battery power, quality of services, packet forwarding behaviour of neighbouring nodes [22]. The authors of [23] defined trust the node i on its neighbour j as weighted sum of direct trust and indirect trust of all its neighbours on node j. The basic idea behind trust based routing is to add trust level of predecessor node in RREQ before broadcasting RREQ. The path having maximum trust level is then chosen to forward packets. Weight w decides how much preference be given to direct trust as compared to indirect trust.

$$\mathrm{Trust}_i\,(j) = w\,\mathrm{Trust}_{\mathrm{Direct}} + (1\text{-}w)\,\mathrm{Trust}_{\mathrm{Indirect}}$$

A trust-based reactive routing protocol [24] discovers several loop-free paths during a single route discovery in AODV based on hop counts and trust values as metric. This two-dimensional evaluation approach selects the shortest path from several alternatives that meet the security requirements based on trust.

3) *Hybrid Mechanisms:* Cryptographic mechanisms being more expensive and trust based being less secured, so hybrid protocol must be created that combines the advantages of both. In order to secure trust metric in the routing packets, a lightweight security mechanism must be incorporated to get hybrid protocol which is less expensive than cryptographic mechanism and more secure than trust based. Future protocol designs should focus on using combination of trust-based metrics and lightweight security mechanisms.

TABLE I
COMPARISON OF SEVERAL ASYMMETRIC PROACTIVE SCHEMES

Parametres → ***Approaches*** ↓	***Ease of implementation***	***Risks of compromising***	***Key generation***	***Attacks possible***
PKI based	Difficult to implement as compared to ID based sender need to verify public key by trusted third party.	If Certificate Authority is compromised though network is exposed but past encrypted messages are still secure.	Public and private key are generated at the same time by the client or CA.	Vulnerable to internal attacks like blackhole, grey hole and Dos attacks as nodes can easily get legalized keys
Threshold Based	Very complex to implement as several nodes share the responsibility of key management	Multiple CA's share key distribution so attacker has to compromise all to get keys.	Public and private key are generated simultaneously by the set of nodes sharing key	Vulnerable to Sybil attack if large number of nodes share key distribution.

			management responsibility.	
ID Based PKI	Very simple to implement as sender need to know the identity of receiver.	Master secret key used by Trust Authority if stolen can decrypt entire past traffic.	Public key can be generated by the client at any time and private key by TA using master secret key.	Vulnerable to fabrication and key escrow attack (in which keys to decrypt encrypted data can be accessed by authorized third party eg. under law of court.
Threshold in ID-PKI	Computation and communication overhead is more than ID based	There is no single trusted authority that can be compromised so more secure.	Initial master key and private keys for respective nodes are computed by multiple nodes.	TA always generates same private key for a malicious node masquerading as legitimate node.
Trust Based	Less computation overhead as trust is calculated by monitoring neighbourhood using IDS.	This scheme is less secure if trust value is not encrypted.	Keys are optional can be used to secure trust metric so less computation intensive.	Prone to fabrication and modification attack.

B. Reactive Mechanism

Existent proactive techniques cannot defend against all types of attacks so reactive mechanisms act as a second security wall. Security solutions are typically attack oriented i.e. threats are identified first and then existing ad hoc protocols are enhanced or new security aware protocols are designed to thwart those attacks. These protocols behave well in the presence of anticipated attacks but collapse under unidentified and unanticipated attacks [25]. It consists of detecting routing misbehaviour with the help of intrusion detection system and cooperation enforcement reducing selfish node misbehaviour.

1) Detecting Routing Misbehaviour

- *Intrusion detection System:* An Intrusion Detection System (or IDS) detects threats and unwanted manipulations in the network. This technique, which was developed first in the wired network, has also gained some attention for the security of MANETs. Zhang [26] proposed the distributed and cooperative architecture of IDS for MANETS in which each node has built-in IDS agent that participates in the intrusion detection process and response activities by detecting the intrusion behaviour locally and independently. The nodes can also share their investigation results with each other. This cooperation among nodes generally happens when a node detects an anomaly and is unable to figure out the category to which anomaly belongs to. The node that has detected the anomaly requires cooperation from other nodes in searching their security logs to track the possible traces of that anomaly. There are four main functional modules of IDS:
- Local data collection module: It gathers the real-time data from various resources.
- Local detection engine: It examines the local data collected and detects for anomalies in the data.
- Cooperative detection engine is needed in case a node wants to know more about the suspicious intrusion so it propagates gathered information to its neighbors to know their viewpoint.

- Intrusion response module gives the response to the intrusion after it has been confirmed. The response can be reorganizing the network redistribution of the keys, or removing all the malicious or compromised nodes.

  Enhanced Adaptive ACKnowledgment (EAACK) [27] is an intrusion detection system that is capable of detecting malicious nodes in presence of false misbehaviour report. EAACK relies on ACK for end to end acknowledgement scheme, S-ACK to detect misbehaviour in presence of receiver collision and MRA to know whether the destination received the reported missing packet through a different route and digital signature for signing all acknowledge packets and verifying until they are accepted.
- *Watchdog:* In this every node keeps account of all the neighbouring nodes' frequency of dropping packets or sending invalid routing information advertisements. Its implementation is based on inherent feature of MANET i.e. a node can directly overhear transmission of all the nodes within its transmission range. In watchdog [28], every node maintains a buffer of packets which have been recently sent and compares it with every overheard packet. If match occurs, packet is removed from the buffer otherwise failure tally of that node is incremented by the watchdog. When the failure tally exceeds a prespecified threshold value, watchdog sends message to the source node notifying it of misbehaviour by neighbouring node. This scheme has certain demerits because of which it is unable to detect misbehaviour in presence of ambiguity in collisions, collision at receiver side, false misbehaviour, partial dropping of packets at lower rate than threshold value of watchdog and multiple colluding nodes.
- *Pathrater:* Along with watchdog, pathrater is also run by each node. It combines the knowledge of misbehaving nodes given by watchdog with link reliability information to pick the most reliable and secure route. Each node has to maintain the trustworthiness rating of every other known node. Path metric is also calculated by averaging ratings of all the nodes over that path. If several multiple paths exist then the path with highest metric is chosen not with shortest path as in standard DSR.

2) *Cooperation Enforcement:* In MANET, some nodes may not cooperate with one another in order to conserve its energy and battery power. These selfish nodes do not directly damage other nodes but drops the packets which can affect network performance severely. Following are the mechanisms to ensure cooperation:

- *Token Based*: The token based scheme [29] extends AODV to detect false routing update messages and packet forwarding misbehaviour. In order to perform network operations of forwarding and routing, each node has to carry a token and its local neighbours monitor to detect any misbehaviour in network operations. Nodes not having valid token are isolated from the network and their neighbours will not interact with them while forwarding packets. This scheme uses asymmetric cryptography- global secret key shared by k neighbours and public key pair. Every legitimate node holds a token signed with the private key that can be later verified by its neighbours. Upon expiration of the token, the node has to get it renewed by multiple neighbours sharing the key. The validity period of token depends on the behaviour of node. A well behaving node has to renew its token less often. But this feature is not effective if node mobility is high. Dynamic changing topology of the network that shares a key for issuing or renewal of tokens leads to high computational overhead. This scheme is vulnerable to spoofing attacks in which a node can request more than one token.
- *Credit Based*: Buttyan and Hubaux [30] proposed credit based scheme known as nuglets in which a node that uses a service must pay the nodes that provide the service. Nuglets or virtual currency are earned by relaying outside traffic and spent by sending its own traffic. The major demerit of this scheme is the need of trusted and temper-resistant hardware to secure the currency. There are two different models - Packet Purse Model in which source loads each packet with nuglets and each forwarding node takes out nuglets for the forwarding service. This model discourages users from flooding the network but source needs to know how many nuglets to be included in the packet and second Packet Trade Model in which destination has to pay at the end for the packet and each intermediate node buys the packet from its previous node on the path. The source node need not to know exact nuglets to be included but this model cannot prevent flooding of the network. In [31] a novel protocol is proposed in which cooperation mechanism is imposed by providing credits to nodes for participating in routing packets. It uses hash chain instead of digital signature for security against deceptive nodes by reducing computational to a large extent.

3) *Reputation Based mechanisms:* CONFIDANT and CORE are examples of reputation based scheme [32]. CORE [33] given by Michiardi stands for "A COllaborative REputation Mechanism". In this, each node keeps track of collaboration of other nodes using a technique called reputation. It prevents DoS attack as there is no incentive for a node that maliciously spread negative information about other nodes. CONFIDANT [34], given by Buchegger and Le Boudec, stands for "Cooperation Of Nodes, fairness In Dynamic Ad-hoc NeTworks". This protocol is an extension to on-demand routing protocols like DSR. It consists of four functional units:

- Monitor for observations
- Reputation System for recording routing and forwarding behavior of other nodes learned from their own experience, overhearing neighborhood traffic and from the trusted second hand observations from the neighbors.
- Trust Manager controls the trust given to received warnings and sends alarm messages if it has detected itself, received report, or observed some malicious behavior of another node.
- Path Manager decides whether to take an action against misbehaving node like isolating it and excluding routes containing it, reranking paths in the cache or sending an alarm for that misbehaved node.

TABLE III
COMPARISON OF SEVERAL REACTIVE SCHEMES

Parameters → *Approaches* ↓	*Protocol employed*	*Merits*	*Demerits*
Cooperative IDS	Source routing protocol like DSR, OLSR, AODV	It consists of local detection engine as well as cooperative detection engine.	Huge consumption of network bandwidth and power. Requires each node to take part in detection so fails in presence of selfish nodes. Based on the assumption that participants are trusted so vulnerable to internal attacks.
Cluster IDS	Source routing protocol like DSR, OLSR.	One node within the cluster has the sole responsibility of monitoring so more efficient scheme.	Need of local history on each node. Complex detection engine at the cluster head is needed.
Watchdog	Source routing protocol like DSR	Each node contributes in detection process. Increased network throughput.	Increased network overhead as buffering of packets is done. Unable to detect misbehavior in presence of ambiguity in collisions, receiver collision, partial dropping of packets [4] etc.
Pathrater	Source routing protocol like DSR	Each node contributes in detection process. Most reliable link is chosen based on trust metric.	Vulnerable to collision problems. Used with source routing protocols only. More network overhead.
CONFIDANT	On demand ad hoc protocols like DSR	Makes cooperation fair. Scalability as performance is unaffected by number of nodes. Generates an alarm when misbehavior is detected.	Based on the assumption that nodes are authenticated so fails if some node has forges its identity.
Nuglets	On demand ad hoc protocols like DSR, AODV	Detect packet forwarding misbehavior and fake routing messages. Prevents flooding of the network if Packet Purse model is used.	Fair approach as malicious nodes can be blocked by the neighbors. Tamper resistant hardware is needed at each node to maintain counters.
Token Based	AODV	Lifetime of token depends on nodes' behavior. Benign nodes are given incentives. Uses asymmetric cryptography algorithms so more secure.	Focuses on network layer security not on physical or link layer. Multiple attackers are possible. Secure path is chosen, confidentiality and integrity of data packet is not considered.

IV. CONCLUSIONS

The research in the field of security of MANETs is still in its infancy. The paper gave broad analysis of the current vulnerabilities, security issues, existing solutions related to MANET security and their pros and cons. Most of the existing protocols and solutions are attack-oriented that is they focus on particular attack and neglect other attacks or collapse in presence of unidentified and unanticipated attacks. The security solution must encompass wider perspective involving both known and unknown attacks. So developing multifence security solution is an area of future research. There is a trade-off between security and network performance. The need of the hour is to integrate security with QoS (Quality-of-Service) so that optimized security solutions are developed for MANET.

REFERENCES

[1] H. Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Wormhole attacks in wireless networks", *Selected Areas in Communications, IEEE Journal on* , vol. 24, no. 2, pp. 370- 380, 2006.

[2] Usha and Bose, "Understanding Black Hole Attack in Manet", *European Journal of Scientific Research*, vol. 83, no. 3, pp.383-396, 2012.

[3] B. Kannhavong, H. Nakayama, A. Jamalipour, "NIS01-2: A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks", *Global Telecommunications Conference, GLOBECOM '06, IEEE*, 2006, pp.1-5.

[4] R. mishra, S. Sharma, R. Agrawal, "Vulnerabilities and security for ad-hoc networks", *International Conference on Networking and Information Technology, IEEE* 2010, pp. 192-196.

[5] S. Gupte, M. Singhal, "Secure routing in mobile wireless ad hoc networks", *Ad hoc networks, Elsevier*, vol. 1, no. 1, pp. 152-174, 2003.

[6] A.K Verma, M. Dave and R.C. Joshi, "DNA cryptography: a novel paradigm for secure routing in MANET", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 11, no. 4, pp. 393-404, 2008.

[7] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks", to appear in Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, H. Jin and W. Jiang (eds), IGI Global, 2010.

[8] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks", *in Proceedings of CNDS*, 2002.

[9] Y. Hu, A. Perrig, D. B. Johnson, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks", *Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02),IEEE* Press, 2002, pp. 3-13.

[10] Y. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless networks, Springer Science + Business Media, Inc. Manufactured in The Netherlands, 2005, 11, pp. 21 – 38.

[11] B. Dahill, B.N Levine, E. Royer and C. Shields, "ARAN: A secure routing protocol for Ad Hoc Networks", UMass Tech Report 02-32, 2002.

[12] Y. Zhang , W. Liu, W. Lou, Y. Fang, and Y. Kwon, "'AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks", *Proc. IEEE Int'l Conf. Comm* , 2005, pp. 3515-3519.

[13] G. Padmavathi, B. Lavanya, "Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks", *Int. J. Advanced Networking and Applications*, vol. 3, no. 4, pp. 1245-1252, 2012.

[14] A. Liu, and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks*", In Proceedings of the 7th International Conference on Information Processing in Sensor Networks*, SPOTS Track, 2008, pp. 245-256.

[15] S. Zhao, A. Aggarwal, R. Frost and X. Bai., "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks", *IEEE Commun. Surveys and tutorials*, vol. 14, no. 2, pp. 380-400, 2012.

[16] Y. Fang, X. Zhu, and Y. Zhang., "Securing resource-constrained wireless ad hoc networks*", IEEE Wireless Commun*., vol. 16, no. 2, pp. 24–29, 2009.

[17] V. Daza, J. Herranz, P. Morillo, and C. Rafols, "Cryptographic techniques for mobile ad-hoc networks", *Computer Networks, Elsevier*, vol. 51, no. 18, pp. 4938-4950, 2007.

[18] M.N. Lima, H.W. da Silva, A.L. dos Santos, G. Pujolle, "Requirements for survivable routing in MANETs", *Proc. Wireless Pervasive Computing,* (ISWPC 2008), pp. 441–445.

[19] J. Cordasco, S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security", *Elsevier Electron. Notes Theor. Comput. Sci,* vol. 197, pp. 131–140, 2008.

[20] A. Pirzada, A. Datta, C. McDonald, "Incorporating trust and reputation in the DSR protocol for dependable routing", *Elsevier Comput. Commun.*, vol. 29, no. 15, pp. 2806–2821, 2006.

[21] J. Li, C. Lee, "Improve routing trust with promiscuous listening routing security algorithm in mobile ad-hoc networks", *Elsevier Comput. Commun*., vol. 29, no. 8, pp. 1121–1132, 2006.

[22] N. Marchng, R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", *IET Inf. Secur.*, vol. 6, pp. 77-83, 2012.

[23] Z. Liu, S. Lu and J. Yan, "Secure Routing Protocol based Trust for Ad Hoc Networks", *International Conference on Software Engineering, Networking and Parallel/ Distributed Computing, IEEE*, 2007, pp. 279-283.

[24] X. Li, Z. Jia, P. Zhang, R. Zhang and H. Wang, "Trust-based-on-demand multipath routing in mobile ad hoc networks", *IET Information Security,* vol. 4, no. 4, pp. 212 – 232, 2010.

[25] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang., "Security in mobile adhoc networks: challenges and solutions", *IEEE Wirel. Commun*., vol. 11, no. 1, pp. 38–47, 2004.

[26] Y. Zhang, W. Le, Y. Huang, "Intrusion Detection Techniques for Mobile Networks", *Wireless Networks Journal*, vol. 9, no. 5, pp 1 – 16, 2003.

[27] E.M. Shakshuki, K. Nan, T.R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", *Industrial Electronics, IEEE Transactions on* , vol. 60, no. 3, pp.1089-1098, 2013.

[28] C. Obimbo, L. M. Arboleda-Cobo, "An Intrusion Detection System for MANET", *Communications in Information Science and Management Engineering (CISME),* 2012, vol. 2, no. 3, pp.1-5.

[29] H. Yang, X. Meng, and S. Lu., "Self-organized Network Layer Security in Mobile Ad Hoc Networks", ACM MOBICOM Wireless Security Workshop 2002, pp.11-20.

[30] L. Buttyan and J. Hubaux. Nuglets, "A Virtual Currency to Simulate Cooperation in Self-organized Ad Hoc Networks", Technial Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne 2001.

[31] H. Janzadeh, K. Fayazbakhsh, B. Bakhshi, M. Dehghan, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains", *Future Generation Computer Systems, Elsevier,* vol. 25, no. 8 , pp. 926-934, 2009.

[32] S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems", *Communications Magazine, IEEE,* 2005, vol. 43, no. 7, pp. 101–107.

[33] P. Michiardi, R. Molva., “Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks”, *IFIP - Communication and Multimedia Security Conference* 2002, pp. 107-121

[34] S. Buchegger, J.-Y. Le Boudec., “Performance Analysis of the CONFIDANT Protocol”, *In proceedings of MobiHoc, ACM Press*, 2002. pp. 226–236.