I. J. Computer Network and Information Security, **2015, 5, 61-73**
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.05.08

Cumulative Techniques for Overcoming Security Threats in Manets

Ajay Koul
SMVD University School of CSE, Katra,182320, India
Email: ajay.kaul@smvdu.ac.in

Mamta Sharma
SMVD University School of CSE, Katra,182320, India
Email: mmtbch6@gmail.com

***Abstract*—**In day-to-day communications we may need to establish temporary (ad hoc) connections anytime, anywhere. Data transfer through this ad hoc wireless network is required when it is hard to establish the large infrastructure. In MANETs there are many challenges in terms of deploying security especially when the confidentiality of the data is compromised. If the data is highly confidential, then providing security especially in the malicious environment is really a challenging task. Many researchers have however proposed solutions for internal as well as external attacks. But unfortunately everyone has some tradeoffs. Some methods are designed only for specific attacks. Some provide solutions for many attacks but depend on the factors like delay, high resource utilization etc. In this paper, we have in sighted into various security providing techniques that have cumulated from many years. We have attempted to present the current approaches for developing secured systems. These methods have used simple techniques to enhance the security and to reduce the complexity. There are many surveys done before on the security issues and methods. However to our information no one has surveyed the current emerging secured methods which may be more effective than the mostly used ones.

***Index Terms*—**MANETs, Topology control, KDC, Security.

I. Introduction

Mobile Ad Hoc Networks (MANETS) are recognized for setting up an inexpensive and temporary wireless communication systems without any premeditation. MANETs can be operating with heterogeneous devices. The unpredictable topologies in MANETs and its assorted nature are very challenging because it requires more responsiveness and maintenance time to time. Rather than an idealistic and theoretical approach, MANETs need pragmatic and flexible approach to become operative in the severest or any kind of environment. To make it work in well-organized way, the discovery of shortest and least congested routes in the varying topologies need to figure out first. But here lies another problem that MANET uses the wireless shared medium and where there is a shared medium there are chances of interference, snooping and annihilation of information as well as the network's physical entities.

So it raised the need for data's confidentiality and integrity before exchanging it in the network and also the system's physical security. There are many other immense challenges and security requirements which we need to contemplate before deploying MANETs.

Many researchers proposed their solutions [1], [2] which provide excellent security but they require very complex computations and consume a lot of resources like memory, bandwidth etc. They have reduced the effect of various attacks but still they are insufficient and become compromised in some attacks [3], [4]. Other solutions [8], [24], [34], [35] are better in terms of providing some extent of quality of services (low memory utilization, low bandwidth, low power etc.) but they are also promising with certain type of attacks [24], [25]. This has become a big tradeoff between choosing those secured methods that consume a huge amount of resources (large memory, high bandwidth utilization and heavy processors for high computations), and those methods that consume fewer resources but are susceptible to various attacks. In this paper, we have explored different approaches of those secured methods which use a large number of resources and computations (encryption/ decryption/ digital signatures etc.) and those which uses simple methods (trust/ observation/ reputation etc.). Then we surveyed most common types of attacks and different solutions proposed for their alleviation. Following we have summarized the secure methods, their assertions, assumptions, metrics, positive and negative aspects. We have tried to extract out the expedient information from the reviewed papers and then finally we have presented our outlooks on the various research areas that can be defined and explored based on the problems we will discuss. From this survey paper, researchers who are interested in the area of security aspects of MANETs will have the distinct notion about security issues and different approaches which can be used for providing better security. Further study can be initiated from a clear perspective of choosing which methods are appropriate according to the area of interest.

II. Exploration Of Best Proposed Approaches

The use of frequently changing wireless links in MANETs makes it susceptible to attack. So, the first step before sharing information is to discover the most secured routes which can be only accessed by the authorized users. Many protocols proposed claim their approaches to be most secured. Security routing protocols can be cryptographic based, trust based, observation based, reputation based and others. In cryptographic based techniques [1], [5], [19], asymmetric and symmetric keys are distributed among nodes to protect the messages from being tampering and losing their integrity. But encryption/decryption schemes are not suitable for resource-constrained devices.

The key distribution schemes reduce overall efficiency in terms of memory, processing computations, power etc. Protocols using only cryptographic mechanisms may run out of resources and fall under the resource consumption attack. In trust and observation based schemes [38], [41], nodes and their neighbors are observed. The information to and from the observed nodes are stored in tables for further observations. These tables are periodically updated to avoid the stale information. In reputation based schemes [8], [43] ranks or reputation values to each node are already given. There is a predefined threshold value according to which reputation of each node is increased or decreased. There are certain hybrid approaches [30], [32] in which combination of the above schemes can be used. Table 1. shows the list of different techniques on security enhancement that have been emerged from the year 2000 to 2012 and which routing approaches are followed i.e. reactive or proactive. Table 2 shows security mechanisms used to protect MANETs, improvements over basic routing protocols and the mechanisms that have been followed. Watchdog and Pathrater, ARIADNE and TSR, proposed in 2000, 2002 and 2012 respectively, are reactive approaches based on underlying dynamic source routing (DSR) protocol. These schemes have tried to implement security in the existing routing protocol by using reputation mechanisms. Similarly, SAR and FrAODV, proposed in 2002 and 2011 have tried to secure Ad hoc On-Demand Distance Vector (AODV) routing protocol. SAR has used hybrid scheme i.e. combination of asymmetric and symmetric cryptography whereas FrAODV has used trust based mechanism. ARAN and SRAC can work with both routing protocols i.e. AODV and DSR. ARAN has used asymmetric cryptography whereas SRAC is using hybrid as well as trust based approach. Detecting forged routing messages in ad hoc networks scheme, proposed in 2008, is a proactive approach. This scheme has used Optimized Link State Routing Protocol (OLSR) as its underlying routing protocol and it has developed a mechanism to detect intrusions earlier. E-ARAN is a recently proposed proactive approach based on Observation-based Cooperation Enforcement in ad hoc network (OCEAN).

Table 1. Different Secured methods

Secure Methods reviewed	Year of publishing	Routing Approach	Routing Protocol Base
Watchdog & Pathrater	2000	Reactive	DSR
SAR	2002	Reactive	AODV
ARAN	2002	Reactive	AODV/DSR
ARIADNE	2002	Reactive	DSR
Detecting forged routing messages in ad hoc networks	2008	Proactive	OLSR
Detection of the node-capture attack in mobile wireless sensor networks	2008	Proactive	-----
SRAC	2009	Reactive	AODV/DSR
High Performance Firewalls in MANETs	2010	Proactive	AODV/OLSR
FrAODV	2011	Reactive	AODV
TSR	2012	Reactive	DSR
E-ARAN	2012	Proactive	OCEAN

This scheme has used Optimized Link State Routing Protocol (OLSR) as its underlying routing protocol and it has developed a mechanism to detect intrusions earlier. E-ARAN is a recently proposed proactive approach based on Observation-based Cooperation Enforcement in ad hoc network (OCEAN). This scheme has focused specially on detecting selfish behavior of nodes. It is following reputation based approach. Likewise we are exploring few more techniques which are based on observations; double layer approach (transport layer and network layer) and some source prefix filtering constraints.

A. Watchdog And Pathrater

In [8], S. Marti et al. explain that Watchdog recognizes misbehaving nodes and a Pathrater supports the routing protocols to avoid these nodes. It is supposed that all routing nodes do not misbehave. When a node forwards the packet, Watchdog promiscuously listens in the network and confirms that the next node in the path also forwards the packet. If the next node does not forward the packet, then it is confirmed as misbehaving. By using this information, Pathrater selects which route is best to deliver the packets. They have implemented the watchdog by maintaining a buffer of newly sent packets and compare each listened packet with the packet stored

Table 2. Security Mechanisms used to protect MANETs

Secure methods Explored	Approaches followed	Security methods used
Watchdog & Pathrater	Reputation based	Nodes are watched promiscuously by Watchdog and a buffer of recently sent packets is maintained to compare with each overheard packet. If a packet remained for longer than timeout, increments a failure tally for the node responsible and if tally exceeds a threshold, the node is declared to be misbehaving and the source is notified.
Watchdog & Pathrater	Reputation based	Nodes are watched promiscuously by Watchdog and a buffer of recently sent packets is maintained to compare with each overheard packet. If a packet remained for longer than timeout, increments a failure tally for the node responsible and if tally exceeds a threshold, the node is declared to be misbehaving and the source is notified.
SAR	Hybrid approach	Keys generation using different trust levels, use digital signatures.
ARAN	Asymmetric cryptography	Trusted certificate server is used to generate and distribute cryptographic certificates. Digital signatures are also used to validate them. Each node knows a priori the public key of the trusted certification authority and obtains exactly one certificate after securely verifying its identity to the server.
ARIADNE	Symmetric cryptography	Clock synchronization, a shared secret between each pair of nodes, an authentic TESLA key for each node in the network is distributed by KDA, uses digital signature to sign routing messages and an authentic route discovery chain element for each node.
Detecting forged routing messages in ad hoc networks	Intrusion detection system	Used where cryptographic based solutions don't work. Alert messages are flooded on detecting a suspect. Suspect is declared as an intruder when other nodes also raise alerts. N is the no. of nodes that can raise alerts. N is taken as 2.
Detection of the node-capture attack in mobile wireless sensor networks	Observation based	Based on tracking of other nodes and re-meet of two nodes within the time set. If they don't meet or time-out expires, an alarm is flooded to announce that node's absence. (MIT) is taken as parameter to suppress fake alarms and to avoid false positives.
SRAC	Hybrid approach & trust based	Each node has an initial pair of public/private keys embedded into each node at the initialization phase or created by a self-organized public key management system. Based on evaluating redundant routing messages received at the target by their TQI (trustworthiness-QoS index) values.
High Performance Firewalls in MANETs	Source prefix filtering constraints	Source prefix filtering constraints are implemented in the route reply packets of the underlying routing protocol used which is used to control route propagation and packet forwarding.
FrAODV	Trust based	IP and MAC addresses are used to identify friend. Friend list is created in the initialization phase or distributed offline. Routing messages are only received by friend nodes by evaluating their friendship values.
TSR	Double layer approach	Observes contention window abnormalities in transport layer and react accordingly in network layer. Control packets are authenticated via security mechanisms [1] [2].
E-ARAN	Reputation based	Based on observation of neighbor nodes, a faulty list is maintained to store all those faulty nodes whose threshold falls below -40 (already preset) and each node stores a route ranker table to choose the high reputed route. Selfish nodes if drops the packets then their reputation go down and the route established by them may not be selected.

in the buffer to see if there is a match. There is certain failure threshold, if it is excesses, then the node is determined to be misbehaving and source is notified about it. Pathrater calculates the negative value path metric to indicate the presence of suspected nodes in the path. The nodes having negative ratings are suspended for some time until their ratings are increased to non-negative values. Pathrater uses Send extra Route Request (SRR) to find a new routes if the well-known route holds only misbehaving nodes. But the overhead of using this extra SRR rises when percentage of misbehaving nodes rises. Their result shows that for 40% misbehaving nodes in the high mobility setup, the overhead rises from 12% to 24% when SRR is activated in the Pathrater and all the simulations were done based on CBR data sources with no reliability requirements.

B. SAR

In [32], S. Yi et al. explain that security mechanism is made into the route request packets. Sender sends route request packets with some metric based on its security and authenticity. On receiving this packet, Intermediate nodes check this packet's security level. If they find it authentic, they forward or reply accordingly otherwise drop it. After discovering the secured route by testing the required security metric on each intermediate node, route reply message is sent back by the receiver node. In this protocol, packets are encrypted using a symmetric encryption/decryption key which is generated with respect to different trust levels. Nodes can only read the route request packets or route reply packets of their trust level. Moreover the floating packets of higher or lower trust level are supposed to be dropped if they are interrupted by a malicious node because node filters packets that belong to its trust level. So this mechanism of broadcasting the routing packets by confirming their trust levels can help in the discovery of attacks by eavesdroppers. It also offers some cryptographic techniques like digital signatures and encryption to check alteration. This protocol finds the assured secured route between two nodes.

C. ARAN

In [19], K. Sanzgiri et al. proposed the use of a trusted

certificate server T to generate cryptographic certificates for each node that wants to enter into the network and a public key which is known to all legal nodes. Keys are created and exchanged through an existing relationship between T and each node. Before arriving in to the network, each node must request a certificate from server T. Each node obtains exactly one certificate after securely verifying their identity to T. All nodes must retain fresh certificates with the trusted server. Using this certification, source verifies that the intended target was reached. In this process, when a node gets route discovery message, it sets up a reverse track back to the source by recording the neighbor's id from which it received the route discovery message. The destination then uncast the route reply message through that reverse track back to the source. Each node in the track checks the previous node's signature, updates its routing table with the address of the node that send it RDP packet, signs the original contents of the message, removes its certificate and signature and attaches its own certificate and then forward the message. This is done to prevent alterations in the route discovery packets in transit. Figure 1 shows its route discovery mechanism

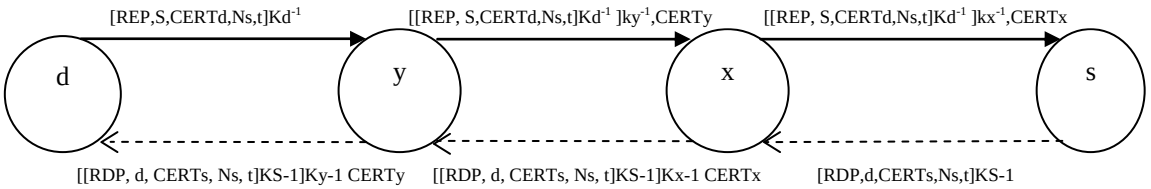

Fig. 1. Route discovery mechanism in ARAN. RDP is broadcasted route discovery packet and REP is unicasted route reply packet. d is destination node, s is source node, x and y are intermediate nodes. CERTs is certificate belonging to source node s, Ns is nonce issued by node s, t is timestamp and [RDP,d,CERTs,Ns,t]Ks^{-1} is the signature generated by private key s to validate the certificate attached.

D. ARIADNE

Y.C. HU et al. in [1] propose ARIADNE. In this protocol, each mobile node has a public/private key pair which is certified from a certificate authority. Every pair of source/destination has a shared secret key. TESLA is used as an authentication protocol. To use TESLA for authentication, each sender chooses a random initial key and generates a one-way key chain by computing a one-way hash function again and again. To authenticate any received value on the one-way chain, an equation is applied to verify if the computed value matches an earlier known authentic key on the chain. Each sender predetermines a time schedule at which it discloses each key of its one-way key chain, in the reverse order from their creation. It is assumed that each node can obtain an authentic TESLA key from the distribution center. Legitimate keys are bootstrapped between pairs of nodes. Route discovery process is initiated by key distribution centre with a special reserved address as target. This address is not the address of any real node. It then uses each returned path to send legitimate keys to each node in the network. This process repeats when a node requests a shared key with any other node and also to KDC, in route reply that node sends the list of nodes for which it requests keys. TESLA relies on an ability of receiver to decide which keys a sender may have previously disclosed based on loose time synchronization between nodes. Before sending the packet, the sender adds a message authentication code (MAC) computed using key. Since the receiver knows the sender's clock may be faster by Δ, packet is discarded if the key has already been published or unless it is received at least Δ before the scheduled key release time. When it is verified that the packet's key is not yet published, receiver buffers the packet and waits for the sender to publish key.

E. Detecting forged routing messages in ad hoc networks

In [33], A. Fourati et al. proposed Intrusion detection system based on OLSR (optimized link state routing) protocol. This protocol tries to thwart attack which is made by legitimate nodes present in the network. It also works where cryptographic based solution doesn't work. It can be implemented on all nodes in the network. Nodes continuously evaluate the semantics of routing message and then act accordingly. When an intruder is spotted, alerts are signaled and they are banned. It checks before taking its decision- is untrusted node an intruder or not? And accordingly implies a low false positive rate. It focuses on detection of generation of fake topology control (TC) messages because they can create confusions in the whole network if disseminated. When a node receives a TC message, according to its local topology statistics, it checks if the initiator of this TC message is 1-hop distance from the common announced MPR selector node or if the common announced MPR selector node had actually nominated the TC originator node as MPR and then assigns one of the three statuses (normal, suspected or intruder) to its originator. After updating its topology table, receiver then forwards its TC message.

F. Detection of the node-capture attack in mobile WSN

M. Conti et al. in [34] provided two methods to detect the node capture: Simple Distributed Detection (SDD) which uses local information on nodes and Cooperative Distribution Detection (CDD) which uses the local nodes cooperation. These two methods are based on the simple observation that if a node (e.g. node A) does not re-meet another node (e.g. node B) within a specific time then it is possible that node B has been captured. This protocol uses random way-point mobility model [35] and

specifically trusts on the honest node re-meeting time to collect overall information about the presence of other nodes in network. The SDD is an event based method. Each node set the corresponding meeting time to the value of its internal clock and starts the corresponding time-out that expires after λ seconds. When two nodes meet, they execute the method, SDD-Meeting. In this method, When a node (e.g. node A) meets another node (e.g. node B), node A invokes the trace method to check if it is to track node B i.e. if node B belongs to the set of nodes having node A. If yes, then node A updates its last meeting with node B and resets the alarm for node B. If on node A time-out expires for node B, then the SDD-Timeout method is invoked and node A floods an alarm in the network which revokes that node and it is considered to be captured. When a node receives a message, SDD-Receive method is invoked. It checks if that message is an alarm and for whom it is raised. E.g. Node A checks when the last alarm for node B is received. If it is received before the Maximum Interval Time (MIT), then the counter for node B is reset to 1 and if received after MIT, then the counter is incremented by 1. It is to avoid false positive alarms. In CDD, nodes share information only when cooperative nodes are present within the same range of communication. It uses the same method trace used for SDD. If two nodes e.g. node A and node B are tracing the third node e.g. node C, then the two nodes compare their meeting time with third node when they last met.

G. SRAC

In [30], Ming Yu et al. proposed protocol that uses redundant copies of routing messages to spot internal attacks. Pair wise secret keys are used between source and destination and intermediate nodes along the established path to protect route discovery messages. Also based on the observations, the node builds the trust on its neighboring nodes by creating a local Certificate Repository (CR). It is assumed that each node in the network is initialized with a unique address and pair of public/private keys embedded into it. Also they can form a self-organized Public Key Infrastructure (PKI) by relating the current CR and present maintenance methods for public key management. When a node starts a route discovery process, it chooses a random number, signs it with its private key and uses key hash function to protect the route discovery message. Finally, the signature and key hash value is appended to the route discovery message which is sent to its neighbors hop by hop until it gets reached to target. To choose a more optimal path, if two nodes show same level of trust, then hop counts are measured, if hop counts are also same then their performance is checked. When receiver (intermediate) gets route request message, it computes the trustworthiness quality index (TQI) and appends it to the route request message along with QoS information before forwarding to next hop. It continues until the message is received by target. Before building a trusted route, target node either sets a certain time to wait or a certain number of route request messages to be received. Target uses its local CR and voting algorithms and then evaluates the received set of copies from different node IDs via different paths because message arrived is decrypted by different intermediate nodes by using different shared keys. Then they are compared by their TQI index values. The index with the minimum cost is preferred. After the path is created, nodes (intermediate) keep observing the best connecting hops in the active paths. Nodes not meeting the specified requirements are removed from the path.

H. High Performance Firewalls in MANETs

In [39], H. Zhao et al. focus on attack which tries to drain the battery of nodes in the network. This scheme is based on ROFL (Routing as the Firewall Layer) mechanism [40] and sets some constraints on the network nodes and the services provided to these nodes. When a service is advertisement to some particular network, only nodes of that particular network can access that service. They cannot access services which are not advertised for them. Before passing any service announcement to a node, the node is first been checked that whether it is authorized to access or not. To stop the advertised service, the routing metric M is set to infinity, and then this infinity route is advertised. Destination address provides services to only those nodes that come under the list of approved source prefixes. Immediately, the packet is dropped if it is forwarded from a source address which is not listed in the source prefix filtering (SPF) constraints of a corresponding route. This packet filtering is applied by layering it on top of routing. Underlying routing protocol provides the pattern (i.e. unicast, multicast or broadcast) for distributing routing information. Once a path between source and destination node is created by underlying routing protocol, each node in that path refers to its local routing table to match the routing announcement and if the same matched announcement is found, then its source prefix constraint is extracted i.e. data packet's header contents (source, destination address and destination port number) and checked before the receiver takes its forwarding decision. If it is forwarded from an authorized node, then it is passed to upper layer otherwise it is discarded. To implement this scheme in AODV, only route reply packet's information of AODV is replaced with service specific announcement (SPF constraints, destination port address, service port address etc.). And then this route announcement is distributed into the network on getting route request and in case of OLSR, these announcements are distributed by flooding Topology Control (TC) messages into the network.

I. FrAODV

In [41], T. Eissa et al. use friendship mechanism to build trust among nodes. Routes are evaluated based on node's reputation and their identity (IP or MAC addresses). It is assumed that malicious nodes cannot alter the identity of node. List of node's friends is created at the time of its initialization and it also keeps their friendship value. Friendship values can be taken from 0 to 100. Trust on a friend raises as the value raises. Also

friends are identified by their IP or MAC addresses. This protocol uses two algorithms to evaluate and form trusted reverse and forward paths. RvEvaluate algorithm forms reverse path from the target node to the source node. On receiving route request, the target node evaluates its preceding node's friendship value. Request is rejected if the preceding node is not its friend. Intermediate node also evaluates its preceding and next hop's friendship values. If these are friends then it forms reverse route from the current node to the source node otherwise rejects it Whereas FwEvaluate algorithm forms forward paths from the source node to the target node. When a route reply message is received by a node (source), it evaluates its next hop's friendship value. If it is a friend, the request is accepted otherwise rejected. Similarly, intermediate node evaluates the friendship values of its preceding and next hops to form the forward path from the source node to the target node. Evaluation of each node along a path is based upon the friendship's value appended to it. A certain threshold for this friendship (TF) value is set as per scenario, below which the node is seen as unreliable.

J. TSR

In [42], H. N. Saha et al. use double-layer scheme that detects attacks at the transport layer but responds to them at the network layer. It implements four modules. First is watch nodes (LS) module that monitors and detect misbehavior nodes, second is node isolation algorithm (NIA) that isolates the infected nodes from the honest node's list. Third is congestion window surveillance (CWS) module that verifies if the node has fault or compromised because CW size may be increased due to congestion in network. Last is alternate route finder (ARF) module. If CWS sees any abnormalities, it calls ARF to find or build a new path. LS module builds a list that contains each node's first-hop neighbors and neighbors of each first hop's neighbor in the end of neighbor discovery process. This is created to first monitor the presence of any malicious nodes and later isolate them from the network using NIA. This process is assumed to be secure and it is done only once in the whole life span of a node. There is no exchange of packets between the nodes which are not neighbors. The node maintains information of its second-hop neighbor to verify if a received packet forwarded from its one hop neighbor has actually forwarded from its second hop neighbor or not. A watch buffer and a malicious counter are maintained in the each node to monitor the packets exchanged between its neighbors. Each entry in the buffer is time stamped and has a time threshold. Malicious counter monitors the length of sliding window and it increments for the node which is detected as malicious by the watch node. These increments depend upon the type i.e. either the packet is fabricated or dropped by the malicious node. To avoid failures (intentionally or by fault) caused by a legitimate node, a node is declared as a misbehavior node and revoked from its neighbor's list, if its malicious counter exceeds threshold. It is done by announcing an authenticated alert message to each of its neighbors using shared keys to prevent from false announcements. A node cannot produce more than one alert message and if a node receives many alerts about other node then it invokes the CWS module to confirm if that node has some fault or it is malicious. If the node is detected to be malicious, the CWS module then invokes ARF module to find an alternate route (excluding all routes containing malicious nodes that are confirmed by CWS) between sender and receiver.

K. E-ARAN

In [43], A. Jangra et al. proposed protocol that uses reputation based scheme. The protocol observes the behavior of other nodes and rates each node accordingly. Rating is first set to zero, which increments by +1 on every positive action and decrements by -2 on every negative action. Negative threshold is set to -40 below which the node is added to a list of faulty nodes. The source node forwards the data packets to the highest reputation node. Intermediate nodes also forward the data packet to the highest reputation hop till it reaches to the destination node. The destination node acknowledges a signed DACK (data Acknowledgment packet) to the source that modifies its reputation values table by recommending +1 to the first hop of reverse route. Subsequently all the intermediate nodes in the route recommends +1 to their corresponding next hop in the route. Each node stores a Route Ranker Table to store the reputation values of each node based on its direct observations on that node. If two next-hop nodes have the same reputation values then randomly anyone is chosen by the source node and that information is also stored in sent-table. If DACK is not received by source node in specified time set by source's timer, it recommends -2 to the first hop of that route and removes its entry from the sent-table after the time-out expires. Intermediate nodes also recommend -2 to their next hop in the route up to that selfish node who dropped the packet and removes the corresponding entries from their tables on time-out expire. If the reputation value of the next hop falls below -40 (threshold value) then it is temporally suspended from the node's routing table and an error message is sent to the upcoming nodes in its path. Later this suspended node can re-join the network with the reputation value initialized to zero. This process aims to prevent selfish nodes from dropping packets because source nodes only choose the nodes with higher reputation values to forward their data packets and selfish nodes need to maintain their reputation constant in order to receive the packets. On receiving a DACK by an intermediate node, it retrieves its record, and increases the reputation value of the next-hop node that sent the DACK. After it is done, it removes the entry of this data packet from its sent-table.

III. Outlooks On Their Significances

In the previous section we deliberated over the functioning of secure methods. Different metrics have been used for their performance evaluation. Various assumptions are set before claiming their achievements. In Table 3 we summarize the used metrics and given

assumptions to evaluate the security and performance of each of these methods. In Table 4 we will also look upon their strengths and weaknesses and various attacks from which they protect MANETs and for which they fail to prevent. In this section we will signify where these secure methods are lagging behind and where they are effective.

The positive aspects of watchdog and Pathrater [8] are that it can identify misbehavior at the forwarding level and not just the link level. This method works best when both watchdog and Pathrater are coordinating and watchdog performs best on top of a source routing protocol because the packet in transit knows it's previous and next hop address. There are also some negative sides

Table 3. Secured Methods performance Evaluation and Assumptions

Secure methods	**Performance evaluation metrics**	**Their Assumptions**
Watchdog & Pathrater	Node rating (path metric), throughput, overhead, false positives, extra route requests	-
SAR	Processing overhead, path discovery, routing message overheads, overall simulation time & transmitted data	Key distribution and shared secrets mechanism is already present.
ARAN	Packet delivery fraction, routing load, average path length, average end-to-end delay of data packets	Each node knows prior the public key of CA.
ARIADNE	Packet delivery ratio (PDR), Packet Overhead, Byte Overhead, Mean latency, Path optimality	KDC can't be compromised. Disregards physical layer and MAC layer attacks. Network links are bidirectional. A mechanism to setup pair wise shared secret keys and to distribute one authentic public key for each node. Each node can estimate end to end transmission time. All nodes have loose synchronized clocks.
Detecting forged routing messages in Adhoc networks	Comparison of true positives (when intruder is detected) and false positives (when a good node is detected as intruder), no. of nodes and intruders in the network	Nodes authentication & message integrity is provided. Messages can't be altered during transit.
Detection of the node-capture attack in mobile WSN	MIT(maximum interval time) to reduce false positives, no. of false positives	Any long silence is possibly an attack. Only way to tamper with node's memory is to remove it from the network.
SRAC	Total throughput, total overhead, packet latency, packet delivery ratio, trustworthiness-QoS index (represents the combination of trustworthiness and performance cost by each intermediate node along the path).	Each node in the network is initialized with a unique address. Pair of public/private keys is embedded into it. Nodes can form a self-organized Public Key Infrastructure (PKI) by relating the current certificate repository (CR) and present maintenance methods for public key management. Source and destination pair is trusted and during the whole operation, it cannot turn to be malicious.
High Performance Firewalls in MANETs	Amount of data traffic and control traffic, implementation overhead, amount of malicious traffic injected into the network because without its presence, this scheme can't be proved.	Throughput, end-to-end delay etc. depends upon underlying protocol used.
FrAODV	Packet delivery fraction, normalized routing load, friendship message activity, and average time taken by messages to reach the destination from the source.	Malicious nodes can't forge the identity of each node. Malicious nodes present in the network are less in number than the good nodes.
TSR	-	All control packets are authenticated using security mechanism [1], [2]. Src & trgt nodes are trustworthy. Neighbor discovery process is secure. The initial CW size is five and the packet transmission time between two different neighbors of same node is same.
E-ARAN	Average end-to-end delay, throughput	-

of this method. Misbehaving node can confines its transmission power such that the true recipient gets too weak signal. This hints the misbehaving node identify the transmission power required to reach each of its neighboring nodes. Watchdog cannot notice multiple colluding nodes if they are dropping packets at a rate lesser than the preconfigured minimum misbehavior threshold. It requires maintaining a lot of state info at each node as it observes its neighbors to confirm that they do not retransmit a packet that they have previously forwarded. If a collision occurs at the receiver, retransmission of packet occurs, which may appear as a replay attack to the node performing as its watchdog. But the question arises here is that how to know nodes are misbehaving due to their own fault or they have been attacked? Because if we increase the negative values of malfunctioning nodes (trusted nodes) then the chances of the attacks by malfunctioning attacker nodes (working with the trusted ones) would also increase. Watchdog on its own does not affect routing judgments, but it

deliveries Pathrater with additional information to fight misbehaving nodes more effectively and Pathrater alone cannot identify a path with misbehaving nodes to decrement its rate. Any route requests triggered by SRR can overflow the network with Route Request and Route Reply packets, which really increase the overhead. False positives occur when the watchdog mechanism reports that a node is misbehaving when actually it is not. Difference between DSR and Pathrater is that the later uses node ratings as path metric and different paths are then matched using this metric reliability. When there is no reliable information then the Pathrater computes the shortest path algorithm.

If there are multiple paths then the path with high metric is selected whereas former picks whatever the shortest path available in the route cache.

SAR [32] permits the use of security as a negotiable metric to improve the importance of the routes. As compared to AODV, this protocol sends less routing control messages. Fewer routes discover but these routes are assured to meet the trust requirements of their sender nodes. If more than one assured route exists, it finds one of the shortest based on number of hops and if all safe routes founded are shortest than the one of the finest suitable is preferred. Again it also has some negative aspects that if nodes do not meet the security requirements then it may drop packets even if the shortest route is available or all links are joined. It picks the first RREP that reaches at the sender. Problem here is that the first RREP comes to the sender may be the false one if there is flooding attack of RREP packets. It does not state anything about how to use the security level as a metric. Route discovery process may lose due to not having appropriate security approval even though there exists a connectivity path to the desired destination. The processing overhead increases on confining flooding mechanism for more optimal and safe routes therefore increasing performance and cost too which is not affordable in low cost networks.

In ARAN [19], there is no assurance that the first route request received travelled along the shortest track from the source. It may be prohibited from travelling on shortest track to reach the destination because of congestion either legitimately or maliciously. There are certain issues in transmitting ERR messages and in key revocation - It is difficult to find whether the node transmitting bulky ERR messages is compromised or simply out of order. ARAN does not differentiate between these two and looks all irregular behavior as the same. If the trusted certificate server broadcasts an announcement for the revocation of a particular node, to the ad hoc group that wants its revocation. Any node receiving this announcement re-broadcasts it to its neighbors so that they reorganize routing to avoid transmission through the untrusted node. Problem here is that in some cases, the untrusted node that is having its certificate withdrawn may be the only connection between two parts of the ad hoc network. In this case, the untrusted node may not forward the announcement of revocation for its certificate, causing partition of the network that persists until the untrusted node is no longer the only connection between the two partitions. If an attacker node has attained certificate then ARAN cannot stop fabrication of routing messages. It is protected as long as certificate authority is not compromised. It has high processing overhead and needs extra memory for the storage of certificates and signatures in the packets. There are also some strong points in ARAN which are worth noticing. Because request discovery messages do not have a hop count and messages are signed at each hop, malicious nodes have no chance to redirect traffic. Error messages are also signed; malicious nodes cannot produce fake error messages. Signed error messages provide non-repudiation which verifies authentication of a source node actually sent error message. A node inserting fabricated messages into the network may be debarred from future route controlling. The route request packet is signed only by the source node with its own private key and route reply packet is signed only by destination node's signature and certificate, this ensures that only the destination can reply to route discovery message. Any modifications in transit would be immediately identified by intermediary nodes along the track, and the modified packet would be consequently discarded. It is effective in finding the shortest routes to the destination in least congested networks. But infeasible in extremely congested networks because the first route discovery packet reached to the destination may have travelled along the long path due to congestion in the network. Congestion may prevent the discovery of shortest routes but ARAN efforts to pick not only shortest route but also least congested route too.

ARIADNE [1] does not consider the case in which an attacker compromises the trusted Key Distribution Centre; if it is compromised then the full network is compromised. It prevents from only one compromised node. An attacker can extend the route by adding extra compromised nodes along the route. This can add delay in the network because nodes like to prefer the shortest route. Route Error message is not processed until the TESLA key gets revealed; this causes delay in knowing that the route is erroneous and in between data packets still continue to be sent along that broken route. In a certain part of network, an attacker intentionally hold Route Requests from a certain node for some period and initiates unnecessary Route discoveries with the chain values from the past discoveries, to make other area nodes believe that it is flooded. Mechanism of key exchange is very complicated. But due to TESLA key's protection, forged route error message cannot be sent. It uses one-way hash function to make sure that no hop is excluded. This is its advantage that any alternation in the node list is detected. If an attacker tries to alter the keys and message authentication code in reply packet, such an alteration is identified due to target MAC field in the reply. Each route request consists of a list of nodes to avoid, and then the message authentication code forming the initial hash chain is computed over that list of nodes.

On spotting suspect in Detecting forged routing messages in ad hoc networks [33], it broadcasts an alert

message to all network nodes except to the suspected node. It then updates its topology table according to the TC message information unless it is verified that the suspected node is an intruder. To decrease the false positives, it applies several checks before declaring a suspected node as an intruder because a node may loses topology information due to collisions and mistakenly alleged a good node as an intruder or attackers may flood fake alert messages to declare good nodes as intruders. A node is declared to be an intruder if at least other n different nodes declared it. In their work, they have chosen n=2, but the performance increases when n rises. But the problem in this method is that the number of nodes n has a certain threshold. On increasing n, number of false negatives also increases. It is assumed that nodes and message authentication, integrity is already provided and messages cannot be altered in transit.

In detection of the node-capture attack in mobile WSN [34], each node flooding n messages every t seconds to show their existence to other nodes. It is assumed that the message authentication mechanism is already present and a node's memory can only be modified or tampered if it is removed from the network. It requires a fixed threshold of alarms to revoke a node. In simulation, at start, data structure in each node is initialized in a way that it has met all nodes in the set, and without performing attack it is run for 1000 seconds. Due to memory limitation, it is assumed that a maximum of 20 nodes can be traced by each node. Its positive aspects are that the false positive alarms are avoided. It does not require same offset time for the node but accepts skew and drift error [36], [37]. Loose time synchronization can also be considered. Raising MIT doesn't raise number of false positives, but raising alarms reduces number of false positives.

SRAC [30] is not feasible for large network nodes having least resources because if n nodes are present along a path, then it requires generating and allocating (n-1) 2/2 keys to the nodes on the path. Route error messages are not protected. There is large overhead due to encryption/decryption. It is not efficient for low computing nodes because in a large mobile network, links broke more frequently and it has to deal large number of route error messages. It is assumed that a source node and target node cannot be attacked. But it does well in some cases like each node (intermediate) along the route computes the TQI value and passes it to the next hop until it reaches to the target node. The target selects the path by comparing their TQI values and chooses the most efficient with least cost. Only the source node and target node have the authentic keys to decrypt the routing messages. SRAC differs from the basic routing protocol AODV, ARIADNE and ARAN. SRAC holds many paths to the target node whereas AODV holds only one path in its routing table. Therefore, in SRAC, on link breakage, routes are not created again. It just picks up another one. In Ariadne, sender continually sends data packets via broken path until the route error message it has received is verified by TESLA key. In SRAC, there is no such delay caused by waiting error messages to be verified and therefore, it increases the PDR. Path having least cost is chosen which is also the most trusted path having least hop counts, whereas ARAN depends on the first route request message received which may have travelled longest but not congested path.

High Performance Firewalls in MANETs [39] has some implementation overhead. It is costly as it requires service specific entries to be maintained in routing table and transmitting of control traffic in the network. Its performance is evaluated for filtering of malicious activity at destinations only. But the good thing about this method is that routing advertisements are only sent to the nodes which are authorized to access that service and packets for a service are only accepted from nodes to which routing advertisements were sent. This scheme can be implemented by any routing protocol with some minor modifications, while being transparent to upper layers and implements packet filtering by taking advantage of underlying routing mechanisms. It helps to drain battery power of the compromised nodes faster. It is an effective firewall mechanism for highly dynamic networks as it creates boundaries between regions that have different policies, even in changing topology. Therefore, achieves high performance irrespective of the network mobility. It drops unwanted packets very early and further away from the destinations depending on how far ROFL announcements can propagate in the network and saves a lot of battery power. ROFL announcement is stored at each intermediate node because RREP is unicast back to the route initiator along the reverse path that RREQ traversed. Therefore, it doesn't require extra control messages as compared to AODV because client route information is piggy-backed in RREQ messages initiated by the route requestor at the beginning. It reduces control traffic as RREQ packets from unauthorized nodes are dropped silently by neighbors which have seen that ROFL announcement before.

The effectiveness of FrAODV [41] is that as the number of friends increases, the network performance also increases. Routing message load is less. Their results prove that less control packets need to broadcast in the network because it blocks routing messages traffic from the unreliable nodes. It is a simple method based on evaluating friendship values without any use of encryption/decryption mechanism. And it is not costly. But the weak side of this method is that it accepts any new node's MAC address. E.g. A legitimate node lost its connection for sometime but regains after some time period and joins the network. Its MAC address is not changed but it might become compromised in between by some attacker node. In high mobility network, frequent breakage of links causes generation of RERR messages, removal of broken links and again forming new paths which raises high routing messaging activity. Also RERR messages are not protected. An attacker may produce false RERR messages. It can incur delay in high mobility networks if attackers use the support of RERR messages therefore downs the network's performance.

TSR [42] detects network abnormalities at the transport layer with the help of congestion window (CW) and reacts at the network layer with the help of alternate route

finder (ARF). Alert message is authenticated using shared keys and a node cannot produce more than one alert message to prevent from false announcements. Re-routing does not depend upon route error packets. ARF module checks route history to disable the duplicate suppression in re-routing process. But question arises here is that what if attacker compromises a watch node? then compromised watch node may send false alarm for a good node just to divert the traffic to some other longer route and it may happen that attacker doesn't fabricate the authenticity of alert message so that no other node doubts on it. If compromised nodes are present in large number, they can accuse an honest node to be misbehaving by generating fake alert messages against it one by one. TSR enhances the DSR scheme. In DSR, the source node waits for a route error packet to initiate re-routing whereas in TSR, congestion window surveillance (CWS) module first checks the abnormalities in the network. If detected, then it initiates re-routing. This enables the source to initiate re-routing if route error packets are dropped by some malicious node in the false route.

E-ARAN's [43] recommendation process makes it hard for selfish node to create a reputation attack for a certain period. Also its Data acknowledgement (DACK) is signed. But problem with this scheme is that as number of selfish nodes increases, end-to-end delay of data packets also increases because at every hop, each node needs to check its reputation table before forwarding data packets to the highest reputation value next-hop node. Therefore, it also reduces the throughput of the network.

Table 4. Strengths and Weakness of the Secure Methods for MANETS

Secure methods reviewed in this paper	Strengths	Weaknesses	Defends against	Vulnerable to
Watchdog & Pathrater	Identifies misbehavior at the forwarding level. Performs best on top of a source routing protocol.	Cannot notice multiple colluding nodes. Occurring of collision on receiver's side appears as replay attack. Requires maintaining a lot of node's state information.	Black hole, replay but not effective	Routing table related, wormhole, rushing, DoS
SAR	Fewer routes are discovered but they are shortest and safe according to its trust requirements.	Does not state about how to use the security level as a metric. The first RREP comes to the sender may be the false one. Processing overhead increases on confining flooding mechanism for more optimal and safe routes.	Routing table related, rushing, replay, eavesdropping, impersonation, location disclosure, eavesdropping	Black hole, wormhole, DoS
ARAN	RERR messages are also signed. Only the destination can reply to the RREQ messages. Effective in finding the shortest routes in the least congested areas.	It doesn't differentiate whether RERR messages are compromised or simply out-of-order. Certain issues in key revocation too. It is protected as long as CA is not compromised. Needs extra memory for storing certificates. High processing overheads.	Routing table related, rushing, replay, spoofing, impersonation, modification	Byzantine, black hole, wormhole, DoS, fabrication of nodes
ARIADNE	Forged route error message cannot be sent. Uses one-way hash function to make sure that no hop is excluded. Alteration in the keys and MAC in reply packet is easily identified due to target MAC field in the reply.	Prevents from only one compromised node.RERR messages do not processed until the TESLA key gets revealed. Key exchange is very complicated. Attacker can initiate unnecessary route discoveries by holding RREQ from a certain node. Supports nodes with few resources.	Routing table related, black hole, gray hole, replay, spoofing, DoS, impersonation	Wormhole, rushing, eavesdropping, attacker may inject data packets
Detecting forged routing messages in ad hoc networks	On detecting suspect, it broadcasts an alert message to all network nodes except to the suspected node. Applies several checks before declaring a suspected node as an intruder.	Number of nodes (n) that declare a certain node as an intruder has a certain threshold. On increasing n, number of false negatives also increases.	Legitimate attacks by legitimate nodes, generation of false topology control messages	if message authentication mechanism is absent
Detection of the node-capture attack in mobile WSN	Does not require same offset time for node. If a node doesn't respond within re meet time alarms are disseminated. False positive alarms are also avoided.	Each node floods n messages every t seconds to show their existence. Requires a fixed threshold of alarms to revoke a node.	Detects the captured or absent node	if message authentication mechanism is absent
SRAC	Only the source node and target node have authentic keys to decrypt the routing messages. TQI values of each path are compared and then the most efficient with least cost and least hop count is chosen. It holds many paths to the target node. Therefore, on link breakage, routes are not created again. It just picks up another one. Increases the Packet Delivery Ratio.	Not feasible for large network nodes having least resources. Route error messages are not protected. Large overhead due to encryption/decryption.	Byzantine, Sybil, selective forwarding, black hole, rushing, spoofing, unauthorized participation, fabricated routing messages	Wormhole, RERR packets are not protected

High Performance Firewalls in MANETs	Routing advertisements are only sent to the nodes which are authorized to access and packets for a service are only accepted from nodes to which routing advertisements were sent. It can be implemented by any routing protocol. It is an effective firewall mechanism for highly dynamic networks and gives high performance. It drops unwanted packets very early. Reduces control traffic.	Implementation overhead. Costly as it requires service specific entries to be maintained. Its performance is evaluated for filtering of malicious activity at destinations only.	DoS, battery exhaustion	-
FrAODV	It evaluates friendship values without any use of encryption/decryption mechanism. As the number of friend nodes increases, the network performance also increases. Routing message load is less because it blocks routing messages traffic from the unreliable nodes. Not costly. Packet delivery ratio increases when mobility decreases.	Accepts any new node's MAC address. RERR messages are not protected so it may incur delay in high mobility networks. Packet delivery ratio decreases when mobility increases.	Routing traffic from untrusted nodes	Legitimate attacks, RERR packets are not protected, spoofing
TSR	Detect network abnormalities at the transport layer and reacts at the network layer. Alert message is authenticated using shared keys and a node cannot produce more than one alert message to prevent from false announcements. Source node does not wait for a route error packet to initiate re-routing. It disables the duplicate suppression in re-routing process.	Large number of compromised nodes can accuse an honest node to be misbehaving by generating fake alert messages against it one by one.	Black hole, jellyfish, framing, blackmail	Sybil, sinkhole
E-ARAN	Recommendation process makes it hard for selfish node to create a reputation attack for a certain period. Data acknowledgement (DACK) is signed.	As number of selfish nodes increases, end-to-end delay of data packets also increases. Therefore, it also reduces the throughput of the network.	Selfish node	wormhole

IV. Open-Eyed Problems Before Deploying Manets

The success of deploying MANETs and the communication between its nodes highly relies on their collaboration but if this collaboration is compromised due to the presence of compromised nodes in the network then surely it would not be successful. So before forming a network of nodes we need to check out that no illicit node is present in the network and if the network detects it earlier or later, then it must remove that immediately.

Authorized node is not acting faulty or damaged and if it is detected for behaving falsely then either it should be detached from the network or it should be suspended for some time (because it might not be working due to some natural fault). The network's routing information is not spoofing and deceiving by unknown nodes. These unknown nodes are not injecting fabricated routing messages into our established network. To avoid unknown nodes from tampering the data and control packets, various encryption and authentication schemes [1], [5] have proposed and are in use. Though set of unknown nodes in a network is the separate problem but the major threat is from those nodes which are known but they act as loop holes. They are generally not easily recognized. So attacks from these nodes are more threatening. It is imperative to prevent from these attackers because once they capture a node, they can formulate any information e.g. with routing table which stores the information about the neighbor nodes, reputation table which store the ranks or reputation values of other nodes. And if they have an access to encryption and authentication keys, then the whole network is dysfunctional or in the hands of an attacker. Main method to detect and avoid these attacks is to monitor the behavior among the nodes [6], [7], [8], [9] and then thwarting these attacks through the techniques [3], [4]. Also modifications in control messages which are propagating between intermediate nodes are acceptable only by those nodes which are listed in the control message to do that. Shortest routes are chosen only if they are secured. If some secured protocol chooses a secured route that is not shortest but least congested then the messages are not readdressed from its path. The location of the network nodes is not exposed to other network nodes. It reduces the chances of attacks from the compromised nodes as well as unknown nodes outside of the network. Stale information stored in the routing tables also creates misinterpretation about the network topology and may lead a node to redirect its traffic to the same node again and again. No erratic or unpredicted operation should be ignored. Immediate verification must be done

on its detection. If there are multiple unknown nodes detected in the network, it is better to shut down the network and then reorganize the whole network entities because eventually they would destroy the whole network and consumes all its limited resources. Also it would become expensive to again build up the whole network with new resources. So it's better to rearrange the network utilizing the same set of resources. Lastly but not limited to, if the underlying Medium Access Control methods are reevaluated before devising the secured architecture then it may foster the ways of providing better security as well as quality too in MANETs.

V. Research Area Directions Founded On Assorted Requirements, Constraints And Tradeoffs

MANETs as we know is prone to attacks from the intruders. Different security mechanisms have been proposed in the past to provide security in MANETs. In this paper we have tried to compare the advantages and drawbacks of several approaches. The purpose of doing so is to provide a guideline towards development of a secure routing protocol and the conditions that make the environment so prone to attacks. So in future maintaining rate of node's mobility and topologies in the network is required. Also distributing use of batteries and other power resources and eliminating tradeoffs between rate of battery consumption and updating nodes due to frequent topological changes is also required. Some other factors also should be taken into account like distribution and use of available bandwidth, providing physical safety to the network bodies, increasing size of network, signal fading and jittering due to large number of multi hops and setting up of minimum and maximum rate of transmission power, eliminating tradeoffs between packet delivery and time delay, eliminating tradeoffs between bandwidth capacity and congestion and distributing authorized access to every node in the network. The methodology or the protocol which is to be developed should also take care of the other aspects of the network which are very important as far as providing security or avoiding threats are concerned. These are provision of security in all seven layers of OSI, detecting number of malicious nodes and formulating malicious activities in the network, Maintaining traffic rate of control/data packets according to the type of traffic (Constant Bit Rate or Varying) and setting up the minimum-maximum rate, routing load balancing, Medium Access Control methods for channel contention, reducing tradeoffs between application aspects and security aspects, focusing maximum route availabilities and finding shortest route from them and maintaining periodic routing table information proactively and reactively.

VI. Conclusion

In this paper, we discussed on prevailing threats to MANETs and also researched on the various solutions proposed to thwart them. Different solutions to these threats proposed by different authors are also given. But as we cannot discuss all of them here so we started with four standard protocols published in year 2002 then moved to cumulative techniques from the year 2008 to 2012. Recent techniques are focusing on how to implement security in MANETs without using so overloaded and costly cryptographic solutions and how to make security protocols more simple but effective. Table 1 and 2 includes the discussed secured methods, the basic routing protocols they have enhanced and security mechanisms they have used to make the solutions more simplified and effective. It is concluded that the security of our network depends upon our specific demands like military applications demand security rather than performance of the network whereas in corporate they need performance though security is also an issue e.g. in cases where credit card numbers, secure passwords are required to submit. No efficient solution is still proposed to remove this trade-off between security and performance. In Table 3, we have listed various metrics and assumptions set by the discussed methods. Table 4 mentions the strengths and weaknesses. We have concluded with the open problems in MANETs which seriously need to be seen. At last we have also defined research areas more specifically according to the problem areas.

References

[1] Y.C. HU, A. Perrig, and D. B. Johnson, "ARIADNE: a secure on-demand routing protocol for ad hoc networks," in *Proc. MOBICOM*, 2002, pp. 12-23.

[2] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *Proc. CNDS*, 2002.

[3] Y.-C. HU, A. Perrig, and D.B. Johnson, "PACKET LEASHES: a defense against wormhole attacks in wireless networks," in *Proc. INFOCOM*, 2003, pp.1976-1986.

[4] Y.-C. HU, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. WISE*, 2003, pp. 30-40.

[5] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," in *Proc. NDSS*, 2003, pp. 263–276.

[6] B. Awerbuch, D. Holser, C. Nita-rotaru, and H. Rubens, "An On demand secure routing protocol resilient to byzantine failures," in *Proc. WISE*, 2002, pp. 21-30.

[7] S. Buchegger and J.Y. Le boudec, "Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proc. PDP*, 2002, pp. 403-410.

[8] S. Marti, T. Giuli, k. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. MOBICOM*, 2000, pp. 255-265.

[9] W. Yu, Y. Sun, and K. J. R. Liu, "Hadof: defense against routing disruptions in mobile ad hoc networks," in *Proc. INFOCOM*, 2005, pp. 1252-1261.

[10] Pradip M. Jawandhiya, Mangesh Ghonge, M.S. Ali and J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks", *IJEST*, 2010, pp. 4063-4071.

[11] L.Tamilselvan, V.Sankaranarayanan, "Prevention of Black hole Attack in MANET," *Proc. AusWireless*, 2007, pp. 21- 26.

[12] S.Lee, B.Han, and M.Shin, "Robust Routing in Wireless Ad Hoc Networks," *ICPP Workshop*, 2002, pp. 73-78.
[13] M.A.Shurman, S.M.Yoo, and S.Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM SE, 2004, pp. 96-97.
[14] S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Black hole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," *IJNS*, 2007, pp. 338-346.
[15] Y.C.Hu, A.Perrig, and D.Johnson, "Wormhole Attacks in Wireless Networks," *IEEE JSAC*, 2006, pp. 370-380.
[16] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," *IEEE WCNC*, 2005, pp.2106-2111.
[17] X.Su, R.V.Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks," *Proc. ICC*, 2007, pp. 1136-1141.
[18] M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," *Proc. MILCOM*, 2006, pp. 1-7.
[19] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proc. ICNP* , 2002, pp. 78–87.
[20] W. Yu, Y. Sun, and K. J. R. Liu, "Hadof: defense against routing disruptions in mobile ad hoc networks," in *Proc. INFOCOM*, 2005, pp. 1252-1261.
[21] Joshua Wright, GCIH, CCNA, 2003, Detecting wireless LAN MAC addresses spoofing, technical document. [Online] Available: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf/.
[22] Gayathri Chandrasekaran, John-Austen Deymious,Vinod Ganapathy, Marco Gruteser, Wade Trappe, "Detecting Identity Spoofs in 802.11e Wireless Networks", In *Proc. GLOBECOM*, 2009, pp.4244-4147.
[23] S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, 2002.
[24] J. F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," in *Proc. Wksp. Design Issues in Anonymity and Unobservability, Berkeley, CA*, 2000, pp. 7-26.
[25] J. Hubaux and E. W. Knightly, "Denial of service resilience in ad hoc networks," in *Proc. MOBICOM*, 2004, pp. 202-215.
[26] Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen and Z.Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," in *Proc. ICC*, 2007, pp. 1247 – 1253.
[27] Kejun Liu, Jing Deng, Member, Pramod K. Varshney and Kashyap Balakrishnan,"An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE TMC, 2007.
[28] C. Kaufman, R. Perlman, and M. Speciner, "Network Security Private Communication in a Public World", Prentice Hall PTR, A division of Pearson Education, Inc., 2002.
[29] Ming Yu , Mengchu Zhou and Wei Su , "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments",in *Proc. IEEE Vehicular Technology Society*, 2009 pp. 449 – 460.
[30] S. Albert Rabara and S.Vijayalakshmi, "Rushing attack mitigation in multicast manet (RAM3)", in *Proc, IJRRCS*, 2010, pp. 131-138.
[31] Xu Su, Dissertation, "Integrated prevention and detection of Byzantine attacks in mobile ad hoc networks", University of Texas at San Antonio, 2009.
[32] S. Yi, P. Naldurg, and R. Kravets, "A Security-Aware Routing Protocol for Wireless Ad hoc Networks", in *Proc. MOBIHOC*, 2002 pp. 286-292.
[33] A. Fourati; K. Al Agha, "Detecting forged routing messages in Adhoc networks", Springer published on nov, 2008, pp.205 – 214.
[34] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks", ACM WiSec, 2008 pages 214-219.
[35] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. "A performance comparison of multi-hop wireless ad hoc network routing protocols" in *Proc. MOBICOM*, 1998, pages 85–97.
[36] S. Ganeriwal, S. Capkun, C. C. Han and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe, 2005, pages 97–106.
[37] K. Sun, P. Ning, and C. Wang, "Fault-tolerant cluster-wise clock synchronization for wireless sensor networks" TDSC, 2005, pg.177–189.
[38] S. Bansal and M.Baker," Observation-based Cooperation Enforcement in ad hoc network", July 2003.
[39] H. Zhao and S. M. Bellovin, "High Performance Firewalls in MANETs" *Proc. MSN*, 2010 pages 154-160.
[40] H. Zhao, C.-K. Chau, and S. M. Bellovin, "ROFL: Routing as the firewall layer," in New Security Paradigms Workshop, September 2008.
[41] T. Eissa; S. A. Razak; R. H. Khokhar; N. Samian, "Trust-Based Routing Mechanism in MANET: Design and Implementation", Springer, Mobile Networks and Applications June 2011.
[42] H. N. Saha, D. Bhattacharyya, A. K. Bandhyopadhyay and P. K. Banerjee, "Two-Level Secure Re-routing (TSR) in Mobile Ad Hoc Networks" *Proc. MNCAPPS*, 2012 Pages 119-122.
[43] A. Jangra, Shalini, N. Goel, "e-ARAN: Enhanced Authenticated Routing for Ad Hoc Networks to handle Selfish Nodes" *Proc. ICAESM*, 2012 pages 144-149.

Authors' Profiles

Ajay Koul received his PhD degree from SMVD University. He is currently working as Assistant Professor in the School of Computer Science at SMVD University Katra, J&K, India. His research interests include wireless network Security, Visual Cryptography and Data Storage

Ms Mamta Bucha has completed her M.Tech From Guru Nanak Dev University Punjab and currently she is working as project fellow in UGC sponsored project at SMVD University in the area Security and QoS in MANETs.