ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

A Survey on Contemporary MANET Security: Approaches for Securing the MANET

Rajan Patel [#1], Pariza Kamboj [*2]

[#]Ph.D. Scholar, Faculty of Technology, RK University, Rajkot-360020 and Department of Computer Engineering, Sankalchand Patel College of Engineering, Visnagar-384315, India.

[*]Department of Computer Engineering, Sarvajanik College of Engineering and Technology, Surat-395001, India.

[1] rajan_g_patel@yahoo.com,

[2]parizak@gmail.com

***Abstract*— The wireless mobile nodes are capable to build spontaneously temporary wireless network in absence of infrastructure like AP, Router etc. and they act as a wireless router. Due to this, wireless mobile nodes are capable for forwarding messages to other nodes. MANET (Mobile Adhoc Network) is a one of the wireless network and forms a temporary connection across the mobile nodes without central infrastructure to exchange the information. Due to the characteristics of MANET, it is vulnerable to active and passive attacks from internal and external attacker. This will lead to various security challenges. There is a requirement to secure the MANET from threats and vulnerability. Many security mechanisms are established to secure and protect the MANET. This article is intended to provide contemporary MANET security with perspective of routing protocol security and data security with key management, and monitoring the MANET during routing and/or data transmission using IDS (Intrusion Detection System). This article presents the various attacks face by MANET and its security goals. The article explored various security solutions for routing protocols, data security using cryptography as a first line of defence, key management for securing communication. It also explored various IDS schemes as a second line of defence in MANET.**

Keyword- Cryptography, Data security, attack, IDS, Routing protocol, Secret sharing

I. INTRODUCTION

Wireless Adhoc Network is a temporary connection across the nodes without central infrastructure for exchanging the information. Both Bluetooth (IEEE 802.15.1) [1] and IEEE 802.11[2] are the main wireless ad hoc network technology [3]. MANET is a self-organized and less infrastructure temporary wireless network where the contents are transferred from node to node. In this environment, all nodes are equally works as a router. The MANET's characteristics are wireless link as a shared medium, dynamic topology, node mobility, limited energy, limited resources, distributed operations, fewer infrastructures, self organized, all nodes are not trusted, multipath route etc. MANET has unique challenges due to its characteristics. Hence, MANET is vulnerable toward a great variety of attacks [4] due to its challenges. However, MANET is flexible, scalable, relatively cheap and easily deployable at any place and time because of its characteristics. On the other side, the MANET is vulnerable to availability, integrity, privacy, indeed, eavesdropping and interception. It is also vulnerable to node suppression, node replication and node impersonation due to self organized topology. Secure routing, security of content transfer, quality of service (QoS) and service discovery are the main security goals in adhoc networking [3].

MANET can be used in tactical networks like military communication and operations, emergency services like disaster recovery and rescue operation, commercial sector like networks of visitors at airports and PAN (Personal Area Network), enterprise networking like networks at construction sites, education network like virtual classrooms, entertainment network like multi user games, sensor network like animal movement, context aware services and coverage extension like linking up with the Internet, intranets etc.

In this paper, we focus on contemporary MANET security. This paper is organized as follows. Section 2 describes the MANET attacks and security goal. Section 3 describes the approaches for securing the MANET routing protocol along with comparison. Section 4 explains the various techniques for MANET data security using cryptography and key management as first line of defence. Section 5, describes the Intrusion Detection System (IDS) as the second line of defence for securing the MANET. Finally, we concluded in the last section.

II. MANET SECURITY

The main security goals/requirements are availability, integrity, confidentiality, authentication and non-repudiation. As oppose to this, the main goal of attacker is to violate the security goal through resource consumption, routing disruption and packet leashes. Attacks in MANET are classified based on the status of attacker, behaviour of attack, and the purpose of the attack.

The status of the attacker could be either; internal (insider) in case of malicious node present within the network or external (outsider) in case the malicious nodes do not belong to the network. The behavior of attacks could be either active attack like prevention of message flow between the nodes or passive attack like unauthorized listening to the network traffic for traffic analysis or accumulating data from it. Further, active attacks can be classified into four categories: dropping attacks, modification attacks, fabrication attacks and timing attacks. Based upon the purpose of attack, attacks can be categorized into three categories [5]: the purpose of illegal/invalid access like impersonation and masquerade, purpose of stealing like eavesdropping, snooping and interception, and purpose of targeting content or resource to make an active operation like a reply, Denial of Service (DOS) and packet drop (black hole, gray hole). MANET is comprised of layers such as physical layer, data link layer, network layer, transport layer and application layer. Table 1 shows the various possible attacks at different layers of MANET.

TABLE I
Attacks at different layers of MANET

<table>
<tr><th>MANET Layer</th><th colspan="2">Attacks</th></tr>
<tr><td>Application</td><td colspan="2">Repudiation, Malicious code, Data corruption, Viruses and Worms</td></tr>
<tr><td>Transport</td><td colspan="2">Session hijacking, SYN Flooding</td></tr>
<tr><td rowspan="2">Network</td><td colspan="2">Blackhole, Grayhole, Wormhole, Sinkhole, Byzantine, Sybil, Resource Consumption attack (Vampire), Rushing, Replay attacks, Hello flooding</td></tr>
<tr><td>Attack on Routing table
-overflow,
-Poisoning,
-Replication</td><td>Attack on routing packet
-Packet interception,
-Packet dropping,
-Packet reply,
-Packet modification,
-Packet forgery</td></tr>
<tr><td>Datalink
(MAC Layer)</td><td colspan="2">Sinkhole, Location discloser, Information discloser, Misdirection attack, Traffic analysis, Link spoofing, Link Withholding</td></tr>
<tr><td>Physical</td><td colspan="2">Jamming, Tampering</td></tr>
<tr><td>Multilayer Attack</td><td colspan="2">DOS, DDOS</td></tr>
</table>

The MANET can be secured using cryptography, secure routing mechanisms and IDS or may use the combination of these approaches. Cryptographic method and IDS can protect the MANET before information (control) and/or after information (data) forwarded while secure routing mechanism can protect the control (routing) information and discover dynamically reliable routes [6] which can be either proactive or reactive [7].

III. SECURE MANET ROUTING PROTOCOLS

Position based, proactive, reactive, topology based and hybrid are the strategies of MANET routing protocol. The routing protocols are classified based on acquired routing information such as proactive information or reactive information, fundamental differences among nodes such as uniform (every node plays equal role or equal important is given to all node: flat) or nonuniform (cluster/zone: hierarchical), path construction metric such as stable link or hop count (major protocol uses [8]), topology based routing information in which the routing protocol gives complete list of intermediate nodes, destination based in which the routing protocol gives list of only next hop and location based in which mobile nodes access geographical information. To secure the routing protocol, majority of protocols use the cryptography. The node who wishes to participate in the routing process must trusted nodes. Authentication based technique can be used to discover the trusted nodes. These trusted elements work according to defined rules of protocol. Authentication can be implemented using symmetric, public key or digital signature. Routing information is significantly control information rather than the data. Hence, it cannot be encrypted (mutable filed) which is still remain useful. Secure routing protocol provides the reliable and accurate path in the presence of untrusted network or malicious attackers [9].

ALARM (Anonymous Location-Aided Routing in MANET) [10] is an anonymous secure location based routing protocol. ALARM finds node's current location by flooding the LAM (Location Announcement Message) throughout the MANET. It then constructs topology utilizing the node's location. It is based on advanced cryptographic group signatures, a public key signature which provides both security and privacy. ALARM provides authentication, integrity, anonymity, and un-traceability. It also provides protection from passive and active attacks as well from internal and external attacks.

AASR (Authenticated Anonymous Secure Routing) [11] protocol defends the network from the security attacks. AASR uses group signature for authenticating the route request packets at each node. Authors used key encryption onion mechanism to record discovered route and designed a mechanism to encrypt a secret message for verification of route request and route reply link.

RSRP (Robust Secure Routing Protocol) [12] uses the asymmetric cryptography, RSA with CRT (Chinese Remainder Theorem) which quickly performs the decryption process in modular exponentiation. Shamir's secret sharing principle of RSA is applied to discover probable routes. This scheme discovers trustworthy and stable routes based on battery power, mobility and trust value. The probable routes are malicious free and disjoint. This protocol also reduces the key generation complexity by using RSA along with CRT instead of simple RSA. Hence, the routing becomes less expensive and secure. RSRP shows good performance compared to non secure routing protocols like AODV and DSR as well as secure routing protocols ZRP and SEAD.

HASR (Hash-based Anonymous Secure Routing) [13] uses collision resistant one-way hash function and pseudo name generation mechanism similar to AODV. HASR does not apply cryptography on data or key. Hence it requires less computation time and network bandwidth for performing routing functions. HASR provides anonymity and security for communication. HASR protects from replay attack, spoofing attack, route maintenance attack, and DoS attack.

SAODV (Secure AODV) [14], [15] uses public key cryptography for securing the AODV routing protocol. SAODV uses hash chains and digital signature to authenticate the routing information. It uses digitally signed Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. Node-by-node, this digital signature is validated cryptographically. Digital signatures are appended to routing messages. SAODV provides authentication and integrity security services. Key distribution is complicated for establishing a new node in the network. A-SAODV (Adaptive SAODV) [16] is an asymmetric key cryptography protocol based on SAODV which optimize the performance of SAODV. A-SAODV uses a separate thread function for cryptography operation to reduce processing time by applying a parallelism. It uses two threads: one thread for cryptography operation and second for other functions like processing of routing message, management of routing table, generation of the message etc. These threads are referring a FIFO queue for messages that need to verify digitally. Double signature is optional in A-SAODV. In SAODV, nodes may become overloaded as they need to compute double cryptography signatures.

FPNT (Fuzzy Petri Net)-OLSR [17] is an integration of trust based routing mechanism for securing the routing and data forwarding process as well. It utilizes trust based routing mechanism and selects a path based on maximum trust value among all possible paths. FPNT gives better performance compared to OLSR in terms of delivery ratio, average latency and overhead. This algorithm evaluates the trustworthiness of the nodes based on fuzzy rules. Load, packet forwarding rate, average forwarding delay, protocol deviation flags are considered as trust parameters for evaluating the trust of nodes using fuzzy petri net. IBE-RA-OLSR [18] is based on RA-OLSR (Radio Aware OLSR) and Identity Based Encryption (IBE) to provide security to OLSR. IBE-RA-OLSR scheme overcomes the vulnerabilities of RA-OLSR and demonstrates that it does not introduce more overhead compared to the original RA-OLSR protocol. IBE signature secures Hello and Topology Control (TC) messages of OLSR and removes the authenticity verification of public keys. RBC (Reputation Based Clustering) [19] improves the selection of Multi-Point Relay (MPR) in OLSR. In this, residual energy and connectivity index of nodes are used for selection of MPR and cluster head respectively. An election algorithm is introduced for selecting a cluster head which in turn selects the MPR node in the cluster. Trust value of path is evaluated based on trust of the nodes' reputation in the presence of selfish nodes.

TSR (Trust-based Source Routing protocol) [20] is a source based on-demand trust routing protocol. TSR takes care of all routing protocol's functions such as route discovery and path selection, route update, route maintenance, route handoff, route error while dealing with node mobility. Authors proved that TSR performs better than DSR and TDSR. The trust prediction model derives the trust that is either direct trust or indirect trust. Direct trust is the received information from neighbors and it is easy to obtain. Indirect trust is the information received from other nodes such as recommended trust of third party. Authors assumed that initially every node in the network is authenticated and used direct trust for the algorithm. During the process if trust of a neighbor node goes below a threshold, this node is considered as black node. They also used dynamic trust prediction model based on nodes' historical and future behaviors through extended fuzzy logic rules prediction.

CBSRP (Cluster Based Secure Routing Protocol) [21] provides secure key management and secure routing in MANET. It uses digital signature and one-way hashing function. It is a cluster based secure routing protocol that forms small clusters of four to five nodes. Every cluster has a temporary cluster head and member nodes. Within a cluster, all nodes are authenticated using one-way hashing function while cluster-to-cluster authentication is done using digital signature. CBTRP (Cluster Based Trust aware Routing Protocol) [22] is an on-demand source trust based cluster routing protocol for securing routing process from malicious nodes in MANET. It organizes the whole network into one hop disjoint clusters and elects most trustworthy nodes as cluster heads. The member nodes of clusters forward packets only through the trusted cluster heads. Result exhibit that CBTRP out performs the CBRP.

ZRP is hybrid ad-hoc routing protocol that combines properties of both proactive and reactive protocols. SZRP (Secure Zone Routing Protocol) [23] provides security for the Zone Routing Protocol (ZRP) based on digital signature and encryption techniques. SZRP uses both the symmetric and asymmetric key encryption techniques. It provides the integrity, confidentiality and end to end authentication. SZRP effectively works in presence of internal and external attacks. Considering that Certificate Authority (CA) is safe from internal and external attacks generated in the network, it gives good performance on the cost of acceptable overhead. In another work, authors have proposed security of ZRP based on the trust calculations [24]. It provides additional security using trust of nodes which is calculated based upon the performance of nodes such as misbehave, drop data packet etc. Trust value is increased upon successful transmission and decreased upon failure delivery of data. In [25], authors have extended ZRP with trust protocol along with the key hash function SHA256 for authentication and integrity.

In [26], authors have presented a trust based security for OLSR routing protocol. Authors presented trust-based analysis using trust specification language of OLSR. Trust based reasoning allows each node to evaluate the behavior of other nodes. This work offers prevention of OLSR vulnerabilities by isolating the misbehaved nodes in the network.

FL-SAODV (Fuzzy Logic Secure AODV) [27] routing protocol uses fuzzy logic for securing AODV routing protocol. FL-SAODV assumes that each neighbor node has a secret key. First, it establishes the security association with neighbor nodes. Then, message digest authenticates the packet. This strategy rely upon the knowledge of secret key and node's behavior like bandwidth consumption, number of neighbor nodes etc. Security level of a node is determined by fuzzy reasoning system using the analysis and knowledge.

QTABR (Q-learning based Trust ABR) [28] identifies a secure routing path. Associativity Based Routing (ABR) purely depends on associativity with neighbor nodes which is a measure of connectivity among nodes. Participating node must satisfy node's observed associativity for performing routing process. Authors proposed Q-learning technique to score the trust of neighbor nodes in trust evaluation table. QTABR exhibits reduced route selection time and increased end to end packet delivery in comparison of ABR protocol.

SDSDV (Secure Destination Sequenced Distance Vector) [29] protocol uses two one-way hash chains. Routing table of DSDV contains hop count and recent sequence number. These two fields play a vital role for DSDV. Malicious node can easily disturb the routing protocol by modifying either hop count or sequence number. With the help of two one-way hash chain mechanism, hop count and destination sequence number (metric values) are protected from malicious nodes. Two additional fields are added in the packet, ALteration (AL) and ACcumulation (AC). Contents of AL field alter from node to node and contents of AC field accumulates related information of all nodes on a route.

T-AOMDV (Trust-Adhoc On-demand Multipath Distance Vector) [30] is a multipath routing protocol based on trust. This scheme applies soft encryption using bitwise XOR for securing message of the sender node. After that, the sender node discovers the secure path through trust model. Path trust is measured based on the trust values assigned to nodes by trust model. Data sensitive level of source node is classified into secret class and confidential class. Sender node then selects a particular path for transmission based on its class and path trust. Authors introduced the secure and reliable policy based trust routing in AOMDV [31]. Trust enhanced Routing Table (TRT) module is included to measure a reliable metric for routes. Secure route is mapped via Security Associations (SAs) with the authenticated (trusted) nodes. In [32], Authors have used RBDR (Rank Base Data Routing) scheme for detection and prevention of packet drop attack in AOMDV routing protocol. It identifies the malicious path using rank base data routing record and avoids the malicious path for preventing from packet drop attack.

TOHIP (TOpology-HIding Protocol) [33] discovered the multipath based on topology hiding concept. TOHIP does not maintain link connectivity in route. Hence, the malicious cannot contact to the network topology based attacks. TOHIP can discover the secure multiple disjoint paths by excluding the malicious nodes in routes. TOHIP has capability to find routes and increase packet delivery ratio in the presence of malicious nodes. TOHIP is secured against black hole attack, sybil attack, rushing attack and wormhole attack.

Table 2 summarizes the related work for securing the routing protocol. Cryptography, game theory, reputation, trust, fuzzy reasoning, etc. are the various mechanisms for securing routing protocol. Among these, some approaches are able to find reliable single or multi-paths, some are able to find only trusted path, some are able to find a secure path in presence of outsider and insider attacks by sharing security keys.

TABLE II
Routing Protocol Security

Secure Routing Protocol	Base Protocol	Acquired Information			FDN		Routing Table Metric	Network Information		Security Mechanism	Addressed Attack(s)
		#1	#2	#3	$1	$2		*1	*2		
ALARM 2011	-	√			√		LAM	√		Group signature	Passive as well active internal and

[10]											external attacks
AASR 2014 [11]	-		√		√		Hop based		√	Group signature, Key encrypted onion routing, Anonymous routing	Defend against potential active attacks without unveiling the nodes' identities
RSRP 2014 [12]	-		√		√		Battery power, mobility and trust value		√	RSA-CRT Cryptography	Passive attacks, Impersonation attacks DoS attacks
HASR 2015 [13]	-		√		√		Hop count		√	Collision-resistant one-way hash function and pseudo-name generation/exchang e mechanism	Replay attack, spoofing attack, route maintenance attack and DoS
SAODV 2014 [14] 2002 [15]	AODV		√		√		Hop count		√	Public key cryptography, Hash chain, Digital Signature	Authentication and integrity
A-SAODV 2008 [16]	AODV		√		√		Hop count		√	Double signature mechanism and reply by only non-overloaded intermediate nodes	Authentication integrity and reduced the overhead of SAODV
FPNT-OLSR 2015 [17]	OLSR	√			√		Hop count	√		Fuzzy Petri-net trust based	Outperforms OLSR in terms of packet delivery ratio, average latency and overhead even in presence of malicious node
IBE-RA-OLSR 2012 [18]	OLSR	√			√		Hop count	√		IBE (Identity Based Encryption)	Reduced overhead compared to RA-OLSR
RBC-OLSR 2012 [19]	OLSR	√				√	Nodes' reputation and Hop count	√		Nodes' reputation, Residual energy level and Connectivity index of the nodes	Selfish nodes' identification
TSR 2014 [20]	-		√		√		Hop count, trust value and path trust	√		Dynamic trust prediction model based on nodes' historical behavior and future behavior via extended fuzzy logic rules prediction	Attack resistance, malicious nodes' identification and their exclusion
CBSRP 2013 [21]	DSR		√			√	Hop count	√		Digital signature, One way hash function	Malicious nodes' identification
CBTRP 2010 [22]			√			√	Trust	√		Distinguish trusted nodes from malicious, one-hop disjoint clusters of network are formed	Intermediary malicious nodes
SZRP 2014 [23]	ZRP			√		√	Hop count	√		Digital signature, Symmetric and Asymmetric encryption	Integrity, confidentiality and end to end authentication in presence of internal and external attacks
2012	ZRP			√		√	Hop count	√		Node trust based	Avoid misbehavior

[24]											nodes
2014 [25]	ZRP			√		√	Hop count	√		ZRP with Trust based and HMAC-SHA256	Avoid misbehavior nodes, authentication and integrity
2013 [26]	OLSR	√			√		Hop count	√		Trust based	Isolate the misbehavior nodes
FL-SAODV 2011 [27]	AODV		√		√		Hop count		√	Fuzzy logic, MD (Message Digest)	Trust calculation and authentication
QTABR 2014 [28]	ABR		√		√		Weighted average of the trust value of the nodes and hop count		√	Q-learning based trust	Misbehaving nodes' identification
SDSDV 2009 [29]	DSDV	√			√		Hop count, AL and AC		√	Two one-way hash chains	Protection from malicious nodes
T-AOMDV 2011 [30]	AOMDV		√		√		Hop count		√	Trust model, Soft encryption using XOR	Malicious nodes' identification
2012 [31]	AOMDV		√		√		Reliability metric, time stamp, session key and hop count		√	Policy-based SAs	Securing Routing messages
RBDR 2015 [32]	AOMDV		√		√		Hop count		√	Rank base data record	Packet drop attack
TOHIP 2014 [33]	-		√		√		Hop count		√	Topology hiding	Black hole attack, Rushing attack, Wormhole attack, Sybil attack

#1: Proactive (Periodic protocols), #2: Reactive (On Demand), #3: Hybrid, FDN: Fundamental Differences of Nodes, $1: Uniform, $2: Non uniform, *1: Topology/Source Routing/Path Addressing, *2: Destination/Table Driven/Hop-by-Hop Routing.

IV. MANET DATA SECURITY

We have discussed the various proposed approaches to secure the routing protocol. But MANET cannot be secured 100% by using only secure routing protocol. Hence, MANET requires first level of defence i.e. cryptography in MANET for securing the data. However, once cryptography involved in MANET, the extra overhead may affect the performance of MANET. Cryptography plays a vital role for MANET security.

IBC (Identity Based Cryptography) [34] is used for key distribution without Key Distribution Center (KDC) or Trusted Third Party (TTP) or Certificate Authority (CA). It is effective in MANET for key management, data security and routing protocol security. Authors demonstrated and compared major strengths and weaknesses of various IBC based schemes. IBC requires a Key Generation Center (KGC) to distribute the private-public pair keys to all the nodes before starting the cryptographic operation. Due to this dependency on KGS, IBC hampers the true nature of ad-hoc networks.

Identity-based RSA (Id-RSA) [35] model is a lightweight authentication and encryption scheme for MANET. Id-RSA model performs fast cryptography operations that enhances network performance. Authors compared this model with RSA Threshold Cryptography (RSA-TC) and ECC based Threshold Cryptography (ECC-TC) with respect to cryptography operation execution time and overhead caused due to security messages. They proved that RSA-TC and ECC-TC increase delay and overhead as compared to Id-RSA. In [36], authors improved Id-RSA by removing certificate authentication scheme which in turn requires less computational cost than Id-RSA.

A novel Device to Device (D2D) authentication mechanism is proposed for security in [37]. This mechanism uses secure initial key establishment using Ciphertext Policy Attribute Based Encryption (CP-ABE).

Communicating devices mutually authenticate each other and derive the link key. This scheme provides protection against Man in the Middle (MIM) and replay attacks.

A hash chain based public key encryption algorithm has been introduced for MANET in [38]. Authors used montgomery algorithm with hash chain for public key distribution in the scheme. Montgomery is an algorithm that reduces division in modular multiplication compared to RSA. In [39], authors used a credit based cooperation mechanism with hash chains for both routing and data forwarding messages. With this scheme, computational overhead of the node is reduced and security against malicious nodes is provided. In first transaction, only source node uses the digital signature. For further transactions, scheme uses only hash function instead of a digital signature for source node as well for all other intermediate nodes.

In [40], self-certifying ID based cryptography has been adopted instead of digital certificate chains and therefore, storing and managing a public key is not required. Authors employed trust metric to deal with malicious nodes. A node determines the trust and public key of other nodes generated on the basis of identities of the nodes. This scheme significantly reduces communication overhead and computation costs.

Authors surveyed security related issues in modern wireless ad-hoc communications [41]. They provided analysis of the existing networking services and also find out new threats in the existing services. Authors classified two security mechanisms: security by design and trust management for dealing the threats.

A fully and dynamic distributed certificate authority scheme based on Elliptic Curve Cryptography (ECC) has been used for MANET in [42]. This scheme takes less computational overhead and provides same level of security like RSA. They applied polynomial secret sharing and fully distributed CA over an elliptic curve, trust graphs and threshold cryptography.

In [43], combined Real-time Recurrent Neural Network (RRNN) cipher and trust based multipath routing called TR-RRNN has been applied for message security in a multipath environment in MANET. Results have shown that this scheme outperforms the reviewed schemes in security and route formation time.

A secure data transmission is provided along with security services like confidentiality, integrity, authentication, and availability of data using disjoint Secure Multipath Routing (SecMR) protocol for MANET in [44]. Involvement of multipath in SecMR, reduces energy consumption. During route discovery phase, nodes are mutually authenticated and maintain the integrity of routing packet. Symmetric secret key is also exchanged during route discovery phase. The first node slices the message into blocks during data transmission phase. After that, encryption operation is performed on these blocks before distributing over multiple routes.

Authors designed a secure data transfer scheme using threshold secret sharing scheme along with Residue Number System (RNS) [45]. They modified XTR (abbreviated for ECSTR which is an Efficient and Compact Subgroup Trace Representation) cryptosystem for reliable exchange of secret keys. The malefactor cannot learn about transmitted data, if does not know secret key or has less than k-projections (threshold) of a secret key. This scheme provides confidentiality and integrity of the transmitted data.

Authors introduced a novel scheme for hiding identity in MANET [46]. The scheme is implemented at using two popular XOR and DES cryptosystem. This scheme provides prevention from passive eavesdropping due to randomly changed identity of nodes, and impersonation due to hidden identity and ARP spoofing. Authors proved that even in presence of the misbehaving nodes, the scheme gives good results in comparison of traditional AODV in terms of end-to-end delay and packet delivery ratio.

HIBEM (Hierarchical Identity Based Encryption Model) [47] is implemented using hierarchical identity-based integer lattices. HIBEM is secure against key exposed and quantum-computing attacks.

In [48] Elliptical Curve Diffe-Hellman algorithm used to detect unreliable node in MANET. By finding the unreliable node the network is able to transfer the reliable data. The scheme is isolate the unreliable nodes from routing and also increase the network performance.

Table 3 summaries the above MANET data security schemes using utilized service, required security mechanism and addressed attack in MANET.

TABLE III
Data Security

	Service	Security Mechanism	Attack Prevention	Remarks
2006 [34]	Key distribution, data security and routing protocol security	IBC	IBC provides security of data, routing and key management	Survey various proposed schemes for key distribution without KDC or TTP or CA
2011 [35]	Authentication, Confidentiality, Certificateless Public Key	IBC with RSA	Secure against RSA cryptanalysis attacks	Require less overhead and delay compared to RSA-TC and ECC-TC
2015 [36]	Certificateless public key, authentication	Id-RSA with Elliptic Curves	Secure against RSA attacks	Significantly more light weight than Id-RSA.
2014 [37]	Device to Device Authentication, Derive	Ciphertext policy attribute-based encryption (CP-ABE)	Protect against Man in the Middle Attack,	Current D2D protocol cannot be used in multi hop

	link key, Share initial secret information safely		Replay attacks	networks due to inside MIM and replay attack
2011 [38]	Public key encryption algorithm	Montgomery algorithm and hash chain	Resist malicious terminal's replay attack	Montgomery algorithm reduces the division in modular multiplication compared to RSA.
2009 [39]	Stimulate nodes to cooperate in routing and packet forwarding	Credit based cooperation mechanism and hash chain	Defend against cheating nodes	Low workload on nodes compared to digital signature scheme
2015 [40]	Certificate-less trust establishment scheme	Self certifying ID based cryptography	Deal with malicious nodes that are able to falsify public key authenticity	Service like PGP and public key authentication
2014 [41]	Collaborative security in ad-hoc communication	Security by design and trust management mechanism	Prevent the network against Internal attacks	Highlight vulnerability of collaborative schemes to internal attacks and review various security mechanisms proposed for handling these attacks
2013 [42]	Fully distributed certificate authority with authentication and security	Elliptic curve based on trust graphs and threshold cryptography	Protect the network against external attacks	A computational advantage to using ECC with a shorter key length and provide same level of security as of RSA
2011 [43]	Message security in multipath with high level of data integrity and authentication	Real-time Recurrent Neural Network (RRNN) based symmetric cipher and trust based multipath routing	Resistance to routing information disclosed to malicious nodes, misbehaved nodes' identification	Secure and minimal time require for route selection
2015 [44]	Confidentiality, integrity, authentication and availability of data transmission	Multiple paths to ensure security. Mutual authentication of neighbor nodes and maintain integrity. Data transmission use symmetric key encryption for confidentiality	Replay attacks prevention by timer	Reduced energy and space consumption
2015 [45]	Confidentiality and integrity of the transmitted data	Threshold secret sharing constructed with use of the RNS (Residue Number System), reliability of secret keys exchange with the modified public key cryptosystem: XTR.	Protection against malefactor	The malefactor cannot learn about transmitted data, if he does not know secret key or has less than k projections of a secret.
2014 [46]	Identity protection of nodes	XOR and DES encryption	Impersonation and passive eavesdrop, ARP spoof attack	Can be used at Network layer as well as MAC layer also
2011 [47]	Hierarchical identity-based encryption for MANETs (HIBEM)	Hierarchical Identity based on integer lattices	Resistance to key exposure and quantum computing attacks	No bottleneck
2016 [48]	Unreliable node detection	Elliptical Curve Diffe-Hellman	Isolate the unreliable nodes from routing	Improving network performance

V. MANET KEY MANAGEMENT

In MANET, key management is essential for key generation, distribution, maintenance, updation, re-generation among node(s) securely.

An algorithm for keys' exchange is introduced in [49] based on Diffie-Hellman Key Exchange (DHKE). This algorithm confidentially exchanges the keys with zero prior knowledge. Thereafter, the key is used to establish a cryptography channel in MANET.

In [50], authors use Identity Based Broadcast Encryption (IBBE) for group key distribution. In this scheme, no message communication is required for establishing the group key and therefore, communication overhead remain same irrespective of group size. Group key distribution is efficient in terms of computations and communication. In [51], IBC based on Feldman's verifiable secret sharing scheme is used for private key distribution. This eliminate the use of Certificate Server (CS) which is mandatory in case of IBC.

Fully distributed ID based Multiple Secret Keys Management (IMKM) [52] scheme is used for securing clustered ad-hoc networks. The IMKM uses ID based multiple secrets and threshold cryptography to eliminate the need of certificate based authentication public key distribution. This scheme also supports efficient mechanism for key update and key revocation. Authors also developed an IDAGKA (ID-based Authenticated Group Key Agreement) protocol. This protocol supports the authentication process without verifying signatures and it requires only single round of operation.

In [53], authors used key distribution scheme using Identity Based Broadcast Encryption (IBBE) in MANET. This scheme provides authentication of the broadcaster, average computation load, efficient communication and scalability. It is secure against Chosen Ciphertext Attack (CCA) also. Encrypted broadcast is forwarded to the receivers where decryption operation takes place at all receivers. Introduced Scheme combines the identity-based cryptosystem with a bilinear map to replace group key setup. Each group member can select the broadcaster and designated receivers for transmission of a confidential message.

An identity-based secret key management scheme is proposed for MANET in [54]. This scheme is implemented using Simpler Threshold version of Schnorr signature (SimpleTSch). It is compared with Certificate based Key Management (CKM) scheme and Identity-based Key Management (IKM) scheme. Comparison shows that the proposed scheme is at par with other ordinary key management schemes in the middle scale network.

On-demand self organized certificate less public key management is presented with enhanced security in [55]. In this scheme, public key verification is performed by Media Access Control (MAC) function instead of RSA certificates. It saves storage space, bandwidth and computation power.

Trusted Party (TP) less threshold key management scheme based on bilinear pairing ECC and singencryption is used in [56]. It provides confidentiality and authentication in MANET. It requires fewer communications which in turn lowers bandwidth consumption.

An authentication scheme based on Diffie-Hellman key agreement algorithm is introduced in [57]. The proposed scheme assists certificate store server to help mobile nodes to achieve identity authentication for issuing user's certificate.

A fully self organized iFUSO identity-based key management scheme is proposed for MANET [58]. iFUSO is an asynchronous network in which only trusted nodes are considered for participation in group initialization. This scheme can revoke the private key of malicious or compromised nodes. Nodes themselves perform all operations without any presence of central server or entity in a fully distributed manner.

The above mentioned schemes are summarized in table 4 based on utilized service and security mechanism used for Key Management.

TABLE IV
Key Management

	Service	Security Mechanism	Remark
2013 [49]	Confidentiality of key exchange during conversation initiation with zero prior knowledge	DHKE	Secure key exchange without CA
2012 [50]	Efficient group key distribution	IBBE	Communication overhead remains unchanged irrespective of group size
2012 [51]	Distributed private key generation for IBC	Based on Feldman's verifiable secret sharing scheme	Eliminates the need of CS in IBC
2010 [52]	Fully distributed IMKM	Combined ID based multiple secrets and threshold cryptography	Eliminates the need of certificate based authentication public key distribution, It is economic, adaptable, scalable, and autonomous key management
2014 [53]	Non interactive key distribution	IBBE with bilinear map	Protects against CCA, average computation load, efficient communication, scalable and dynamic
2012 [54]	Secret key management	Simpler threshold version SimpleTSch	Performs at per with ordinary key management scheme in middle scale network
2014 [55]	Certificate less self organized on demand public key management	MAC function instead of RSA certificates to perform public key verifications	Saves considerable computation power, bandwidth and storage space
2012 [56]	Threshold key management scheme without a trusted party with confidentiality and authenticity	ECC based threshold polynomial and signcryption	Signcryption consumes fewer system resources with lower bandwidth consumption, fewer communication quantity, and can realize signature and encryption simultaneously
2012 [57]	Authentication Scheme	DHKE	The communication can use symmetry

			cryptographic algorithm for lower computation and also save resource of the MANET after node authentication.
2013 [58]	Fully self organized key management system	iFUSO identity based	Mechanism to revoke the private key of malicious or compromised nodes and update the keys of non compromised nodes.

VI. Intrusion Detection System

IDS (Intrusion Detection System) [59] is a software application or tool or device that monitors the activities of machines/networks to report against violation of policy or malicious activities. The IDS collects the behavior or traffic of machines and/or networks for performing the analysis of suspicious activates. Anomaly based, specification based, signature based, reputation based, hybrid etc. are the techniques used for performing the analysis. The information collection can be online or offline. Finally, IDS reports or take an action against affected machines or networks to mitigate the detected effect. Hence the IDS response strategies are either reactive or passive. The reactive IDS (IDPS-Intrusion Detection and Prevention System) is last level of intrusion response system. IDS is the second level of defense in MANET [60], [61]. Only information security is not sufficient to provide complete protection [62] and therefore, IDS need to integrate.

In [63], authors presented the statistical classification based IDS in AODV reactive routing protocol. This scheme locally collects data and merges the collected data for classifying the model. It detects flooding attack, forging attack and packet dropping black hole attack. A specification based IDS placed in host is used for AODV routing protocol in [64]. It addresses RREQ flooding attack, Denial of Service (DoS) attack, black hole attack, wormhole attack and rushing attack. In [66], authors used contamination borders [65] for sinkhole attack detection in AODV reactive routing protocol.

A behavior based cluster IDS engine is used in DSR routing protocol [67]. It detects modification attack, packet dropping black hole attack, impersonation attack and fabrication attack with fewer false alarms.

In MDSR (Modified DSR) [68], an anomaly based IDS uses 2-hop collaborative neighbor scheme for black hole attack detection and removal of selective attack in DSR routing protocol. In selective black hole attack, malicious nodes drop the data packets selectively. MDSR reduces energy consumption and packet loss compared to DSR routing protocol. IDAR (Intrusion Detection & Adaptive Response) [69] is an anomaly based clustered IDS that addresses the rushing attack, Sleep Deprivation (SD) attack, black hole attack and gray hole attack. In this scheme, attacks are identified by using Network Characteristic Matrix (NCM) and Performance Matrix (PM). Thereafter, intruder node is simply isolated or routing is done around it as per no punishment policy in AODV reactive routing protocol. However, the performance of the network is degraded in IDAR. In [70], authors used Genetic Programming (GP) along with Multi Objective Evolutionary Algorithm (MOEA) to find out optimal tradeoffs between security criteria and the power consumption of the nodes. This scheme addresses route request flooding and route disruption attacks utilizing anomaly detection as in AODV reactive routing protocol. DPS (Detection and Prevention System) distributed IDS is employed for black hole detection and prevention in AODV routing protocol in [71]. For the working of DPS, some special nodes are deployed in the network. These nodes analyze the behavior of their neighbors to detect black hole attack and broadcast a message to declare the node malicious. Thereafter, network rejects all types of data from the declared malicious nodes. CDC-ADS (Conceptual Data Collection - Anomaly Detection System) [72] is an anomaly routing detection IDS that enhances the accuracy of anomaly detection in OLSR routing protocol.

ACF-EX (Adaptive Character Frequency-based EXclusive) [73] signature matching scheme improves the process of signature matching. This scheme is evaluated in a distributed network environment and its performance is compared with Snort. ACF-EX performs well by reducing time and packet rate in comparison of Snort. CCIDS (Court like Cluster IDS) [74] is a signature based cluster IDS for protecting against link spoofing and link deletion attacks in OLSR routing protocol. This scheme adopts a court-like structure that provides timely and accurate detection of attacks. Court-like structure works similar to real life for accusation, investigation and defense of the network that is divided into one hop clusters.

The effective K-means clustering data mining technique is introduced to identify malicious nodes responsible for black hole attack in ZRP routing protocol [75]. In [76], watchdog sensor and Bayesian filtering based scheme are used for identifying black hole attack and selfish nodes in peer to peer network. This system monitors traffic of every neighbor nodes and decreases number of false positive due to integration of bayesian filtering inside the watchdog.

In [77], AACK (Adaptive ACKnowledgment) based IDS in distributed environment is introduced to identify the selfish and misbehaving nodes in DSR routing protocol. This scheme not only reduces routing overhead compared to TWOACK scheme, but also increases detection efficiency by applying node detection instead of link detection.

MEACA (Mobility and Energy Aware Clustering Algorithm) [78] is used in hierarchical cluster based architecture for improving upon detection accuracy and energy consumption. The Nash equilibrium game theory is proposed in cluster based architecture for addressing sinkhole attack [79]. Bayesian game theory and trust in cluster based architecture is proposed for addressing internal and external intrusions [80]. The Bayesian game theory is used for detecting external intrusions and building the trust relation between nodes by observing the behavior of their neighbor nodes for avoiding internal intrusions.

Table 5 summarize the related work of IDSs for securing the MANET using detection mechanism, used architecture, addressed attack, used routing protocol, way of collecting data for analysis and how the system response to the intrusion.

TABLE V
IDS in MANET

IDS	Detection Mechanism	Architecture	Addressed Attack	Routing Protocol	Collection Approach	Intrusion Response	Remark
2013 [63]	Statistical Classification	Not specified	Flooding attack, Forging attack, Packet dropping attack	AODV	Collect data locally & merge it to adapt the classifier models offline	No	Minimizes cost and also reduces error for classifiers
SIDE 2014 [64]	Specification	Host based	RREQ flooding attack, DoS, Black hole attack, Wormhole attack, Rushing attack	AODV	Collect audit data for some predefined time frame	No	Effectively can detect attacks in real time, SIDE induces least number of control packet overhead compared to other IDSs.
2015 [66]	Contamination borders [65]	peer-to-peer	Sinkhole attack	AODV	Traffic	No	Accuracy is higher but system addresses only sinkhole attack
2008 [67]	Behavior	Clustered	Modification attack, Drop attack, Impersonation attack, Fabrication attack	DSR	Network packets	No	IDS can detect unknown intrusion with fewer false alarms
MDSR 2014 [68]	Anomaly	Not specified	Black hole attack, Gray hole attack	DSR	Traffic online	Removal of selective black hole attack	Less energy loss and data packet loss
IDAR 2014 [69]	Anomaly	Clustered	Rushing attack, SD attack, black hole attack, Gray hole attack	AODV	Traffic online	Responds to black hole and sleep deprivation attacks by isolating the intruder nodes, responds to rushing attack by either isolating or routing around the intruder node (no punishment)	Degradation of network performance
2010 [70]	Anomaly	Not specified	Route request flooding attack, Route disruption attack	AODV	Network packets	No	GP with MOEA used to make optimal tradeoffs between security criteria and power consumption
DPS 2015 [71]	Anomaly	Distributed	Black hole Attack	AODV	Behavior of only neighbor nodes	Broadcasts a warning message to declare a black node for isolating it from the network	Considerably reduces the packet drop ratio with a very low false positive rate
CDC-ADS 2015 [72]	Anomaly	Distributed	Anomaly detection	OLSR	Data are collected based on four	No	Enhance the accuracy of anomaly detection

					aspects of OLSR behavior		
ACF-EX 2013 [73]	Signature (rule based)	Distributed	Known signature attack	-	Network packets	No	Improves the process of signature matching for a signature based NIDS
CCIDS 2010 [74]	Signature	Clustered	Link spoofing, link detection	OLSR	Routing packets	Yes	Uses a court-like structure for timely and accurate detection of attacks, also increases capability in distinguishing malicious accusations
2014 [75]	Data mining	Distributed	Black hole attack	ZRP	Routing packets	Isolate malicious nodes	Uses effective K-means clustering data mining technique
2010 [76]	Watchdog sensor and a Bayesian filtering	Peer to peer	Black hole attack, Selfish nodes' detection	-	Traffic of every neighbor node	No	Decreases number of false positives and higher percentage of attack detection
2010 [77]	Watchdog	Distributed	Selfish nodes' detection	DSR	Acknowledge-ment packets	Inform source node	Reduces routing overhead and increases detection efficiency by applying node detection instead of link detection
2011 [78]	MEACA	Hierarchical cluster	-	-	Mobility and energy of nodes in the cluster	No	Minimizes imposed communication and processing overhead, reduces energy consumption and improves detection accuracy
2015 [79]	Game theory	Clustered	Sinkhole attack	-	-	No	Uses game theory and Nash equilibrium
2010 [80]	Bayesian game theory	Clustered	Internal and external intrusion	-	Behavior of only neighbor nodes	Builds trust relationship between nodes and estimates trust value for each node to prevent internal intrusion	Detects external intrusions using game theory and internal intrusions using established trust level among neighboring nodes

VII. CONCLUSION

As MANET is a wireless adhoc network, it has its own characteristics and features. It is vulnerable to active and passive attacks from internal and external attackers due to its characteristic and features. Single approach is not sufficient to secure MANET. Some security mechanisms can be used to prevent from malicious activity during path discovery process in MANET. To secure the data being transmitted, cryptography may integrate as a first level of defense. The IDS is used to monitor the network as a second line of defense. These solutions are application specific. Cryptographic method and IDS can protect the MANET before forwarded message (control) and/or after forwarded message (data). While secure routing mechanism can protect the control (routing) information and discover dynamically reliable routes. Besides using cryptography as first line of defense, some other security mechanisms like game theory, fuzzy, trust etc. can also be used during route discovery phase and data transmission. Performance of the network may goes down with the inclusion of security mechanisms that is negotiated as a tradeoff for supporting the need of security. There are more and more new applications in the commercial sector that are using MANET recently. Therefore, the success of this technology will largely depend on security of new applications and programs to be developed.

REFERENCES

[1] Bluetooth IEEE 802.15.1Standard,https://standards.ieee.org/findstds/standard/802.15.1-2002.html Date accessed: 10/1/2016
[2] IEEE 802.11 Standard, http://standards.ieee.org/about/get/802/802.11.html Date accessed: 10/1/2016
[3] Rubinstein M G, Moraes I M, Campista M E M, Costa L H M, and Duarte O C M. "A survey on wireless ad hoc networks," In Mobile and Wireless Communication Networks, Springer US, vol. 211, pp. 1-33. 2006.
[4] Mafra P M, Fraga J S, and Santin A O. "Algorithms for a distributed IDS in MANETs," Journal of Computer and System Sciences, vol. 80(3), pp. 554-70, 2014.
[5] Draft Paper Nie P. Security in Ad hoc Network, publishing name:? 2006, pp .1-40.
[6] Vijayakumar K, and Somasundaram K. "Study on reliable and secure routing protocols on MANET," Indian Journal of Science and Technology, vol. 9(14), pp. 1-10, 2016.
[7] Pathan, A. S. K. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2010.
[8] Son T T, Le Minh H, and Sexton G, Aslam N. "A novel encounter-based metric for mobile ad-hoc networks routing," Ad Hoc Networks, vol. 14, pp. 2-14, 2014.

[9] Andel T R. Formal security evaluation of ad hoc routing protocols, ProQuest, 2007.
[10] El Defrawy K, and Tsudik G. "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Transactions on Mobile Computing, vol. 10(9), pp.1345-58, 2011.
[11] Wei L, and Yu M. "AASR: authenticated anonymous secure routing for MANETs in adversarial environments," IEEE Transactions on Vehicular Technology, vol. 63(9), pp.4585-4593, 2011.
[12] Sinha D, Bhattacharya U, and Chaki R. "RSRP: A robust secure routing protocol in MANET," Foundations of Computing and Decision Sciences, vol. 39(2), pp.129-54. 2014.
[13] Lo N W, Chiang M C, and Hsu C Y. "Hash-Based anonymous secure routing protocol in mobile ad hoc networks," IEEE *10th Asia Joint Conference on Information Security (AsiaJCIS),* pp.5-62, 2015.
[14] Lupia A, and De Rango F. "Performance evaluation of secure AODV with trust management under an energy aware perspective," IEEE *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2014),* Monterey, pp. 599-06., 2015.
[15] Zapata M G, and Asokan N. "Securing ad hoc routing protocols," In *Proceedings of the 1st ACM workshop on Wireless security*,NY,pp.1-10. 2002.
[16] Cerri D, and Ghioni A. "Securing AODV: the A-SAODV secure routing prototype," IEEE Communications Magazine, vol. 46(2), pp.120-25, 2008.
[17] Tan S, Li X, and Dong Q. "Trust based routing mechanism for securing OSLR-based MANET," Ad Hoc Networks, 30(C), pp.84-98, 2015.
[18] Ben-Othman J, and Benitez Y I S. "A new method to secure RA-OLSR using IBE," *IEEE Global Communications Conference (GLOBECOM),* Anaheim, CA, pp. 354-58. 2012.
[19] Robert J M, Otrok H, and Chriqi A. "RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks," Computer Communications, vol. 35(4), pp.487-99, 2012.
[20] Xia H, Jia Z, Li X, Ju L, and Sha E H M. "Trust prediction and trust-based source routing in mobile ad hoc networks," Ad Hoc Networks, vol. 11(7), pp.2096-2114, 2013.
[21] Morshed M M, and Islam M R. "CBSRP: cluster based secure routing protocol," *IEEE 3rd International Advance Computing Conference (IACC), Ghaziabad,* pp. 571-76, 2013.
[22] Safa H, Artail H, and Tabet D. "A cluster-based trust-aware routing protocol for mobile ad hoc networks," Wireless Networks, vol. 16(4), pp.969-84, 2010.
[23] Pan N K, and Mishra S. "Secure hybrid routing for MANET resilient to internal and external attacks," In *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India,* Springer International Publishing, vol. 1, pp. 449-58, 2014.
[24] ElRefaie Y, Nassef L, and Saroit I A. "Enhancing security of zone-based routing protocol using trust," *IEEE8th International Conference onInformatics and Systems (INFOS),Cairo,*,pp.32-39, 2012.
[25] Rahman M T, Mahi N, and Julkar M. "Proposal for SZRP protocol with the establishment of the salted SHA-256 Bit HMAC PBKDF2 advance security system in a MANET," *IEEE International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), Dhaka,*,pp.1-5, 2014.
[26] Adnane A, Bidan C, and de Sousa Júnior R T. "Trust-based security for the OLSR routing protocol," Computer Communications, vol. 36(10), pp.1159-1171, 2013.
[27] Zhang Z. "A novel secure routing protocol for MANETs," *InTech*, 2011, pp. 455-66.
[28] VijayaKumar A, and Jeyapal A. "Self-Adaptive trust based ABR protocol for MANETs using Q-Learning," The Scientific World Journal, pp.120-25. 2014.
[29] Wei WJ, Chen HC, and Lin YP. "A secure DSDV routing protocol for ad hoc mobile networks," *IEEE Fifth International Joint Conference onINC, IMS and IDC,* Seoul, pp.2079-2084, 2013.
[30] Huang J W, Woungang I, Chao H C, Obaidat M S, Chi T Y, and Dhurandher S K. "Multi-path trust-based secure AOMDV routing in ad hoc networks," In *IEEE Global Telecommunications Conference (GLOBECOM 2011),*Houston, Tx, USA, pp.1-5, 2011.
[31] Salmanian M, and Li M. "Enabling secure and reliable policy-based routing in MANETs," In *IEEE Military Communications Conference, Orlando, FL,* pp.1-7, 2012.
[32] Sumaiya V, Patel R, and Patel N. "Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET," IEEE *International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore*, pp.1-5, 2015.
[33] Zhang Y, Yan T, Tian J, Hu Q, Wang G, and Li Z. "TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks," Ad hoc networks, vol. 21,pp.109-22, 2014.
[34] Zhang Y, Liu W, Lou W, and Fang Y. "Securing mobile ad hoc networks with certificateless public keys," IEEE Transactions on Dependable and Secure Computing, vol. 3(4), pp.386-99, 2006.
[35] Eissa T, Razak S A, and Ngadi M D. "Towards providing a new lightweight authentication and encryption scheme for MANET," Wireless Networks, vol. 17(4), pp.833-42, 2011.
[36] Kasra-Kermanshahi S, and Salleh M. "An improved certificateless public key authentication scheme for mobile ad hoc networks over Elliptic Curves," In Pattern Analysis, Intelligent Security and the Internet of Things, Springer International Publishing, pp.327-334, 2015.
[37] Kwon H, Hahn C, Kim D, Kang K, and Hur J. "Secure device-to-device authentication in mobile multi-hop networks," In Wireless Algorithms, Systems, and Applications, Springer International Publishing, pp. 267-278, 2014.
[38] Feng W, Qing-wei S, and Ke C. "A mobile ad hoc network public key encryption algorithm based on hash-chain," *Procedia Engineering*, vol. 23, pp. 659-664. 2011.
[39] Janzadeh H, Fayazbakhsh K, Dehghan M, and Fallah M S. "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," Future Generation Computer Systems, vol. 25(8), pp.926-934, 2009.
[40] Hamouid K, and Adi K. "Efficient certificateless web-of-trust model for public-key authentication in MANET," Computer Communications, vol. 63, pp. 24-39, 2015.
[41] Saied Y B, Olivereau A, Zeghlache D, and Laurent M. "A survey of collaborative services and security-related issues in modern wireless Ad-Hoc communications," Journal of Network and Computer Applications, vol. 45, pp.215-27, 2014.
[42] Alomari A. "Fully distributed certificate authority based on polynomial over elliptic curve for MANET," 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Honolulu, HI, pp.96-100. 2013.
[43] Liu C Y, Woungang I, Chao H C, Dhurandher S K, Chi T Y, and Obaidat M S. "Message security in multi-path ad hoc networks using a neural network-based cipher," In *IEEE Global Telecommunications Conference (GLOBECOM 2011),Houston, Tx, USA,* pp.1-5, 2011.

[44] Faisal M, and Mathkoor H. "SDTP: Secure data transmission protocol in ad hoc networks based on link-disjoint multipath routing," IEEE *2nd World Symposium on Web Applications and Networking (WSWAN)* Sousse, pp.1-5, 2015.
[45] Ivanovich C N, Grigor'evich B M, Sergeevna K I, Sergeevich N A, and Igorevna G A. "Development of the protected data transfer protocol for the MANET networks on the basis of Residue number system," Omsk, pp.1-5, 2015.
[46] Mohsen Y M, Hamdy M, and Hashem M. "GPSIH: A generic IP-based scheme for identity hiding in MANETs," IEEE *9th International Conference on Informatics and Systems (INFOS),* Cairo, pp.32-38. 2014.
[47] Li H. "A hierarchical Identity-Based encryption for MANETs," IEEE *International Conference on Computational Problem-Solving (ICCP*), Chengdu, pp.330-333, 2011.
[48] Thangaraj SJJ, and Rengarajan A. "Unreliable node detection by Elliptical Curve Diffe-Hellman algorithm in MANET," Indian Journal of Science and Technology, vol. 9(19), pp. 1-6, 2016.
[49] Stulman A, LahavJ, and Shmueli A. "Spraying Diffie-Hellman for secure key exchange in MANETs," In Security Protocols*, XXI* Springer Berlin Heidelberg, pp.202-212. 2012.
[50] Yang Y. "A communication efficient group key distribution scheme for MANETs," In Network and System Security*,* Springer Berlin Heidelberg, 7645, pp.361-372, 2012.
[51] Chan A C. "Distributed private key generation for identity based cryptosystems in ad hoc networks," Wireless Communications Letters, IEEE, vol. 1(1), pp. 46-48, 2012.
[52] Li L C, and Liu R S. "Securing cluster-based ad hoc networks with distributed authorities," IEEE Transactions on Wireless Communications*,* vol. 9(10), pp. 3072-3081, 2010.
[53] Yang Y. "Broadcast encryption based non-interactive key distribution in MANETs," Journal of Computer and System Sciences, vol. 80(3), pp. 533-545, 2014.
[54] ZHANG Y, and QIAN H F. "An efficient identity-based secret key management scheme for MANETs," The Journal of China Universities of Posts and Telecommunications, vol. 19, pp.127-136, 2012.
[55] Maity S, and Hansdah R C. "Self-organized public key management in MANETs with enhanced security and without certificate-chains," Computer Networks, vol. 65, pp.183-211, 2014.
[56] Meng X, and Li Y. "A novel threshold key management scheme based on bilinear pairing without a trusted party in mobile ad hoc network," *IEEE 14th International Conference on Communication Technology (ICCT), Chengdu,* pp.73-77, 2012.
[57] Xingliang Z, and Shilian X. "A new authentication scheme for Wireless Ad Hoc Network," IEEE International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), pp.312-15, 2012.
[58] da Silva E, and Pessoa Albini L C. "Towards a fully self-organized identity-based key management system for MANETs," *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),*Lyon, pp.717-723, 2013.
[59] Liao H J, Lin C H R, Lin YC, and Tung K Y. "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36(1), pp.16-24, 2013.
[60] Amiri E, Keshavarz H, Heidari H, Mohamadi E, and Moradzadeh H. "Intrusion detection systems in MANET: a review," *Procedia-Social and Behavioral Sciences*, vol. 129,pp .453-459, 2014.
[61] Nishani L, and Biba M. "Machine learning for intrusion detection in MANET: a state-of-the-art survey," Journal of Intelligent Information Systems, vol. 46(2), pp.1-17, 2015.
[62] Nadeem A, and Howarth M P. "A survey of MANET intrusion detection and prevention approaches for network layer attacks," communications surveys and Tutorials, IEEE, vol. 15(4), pp.2027-2045, 2013.
[63] Mitrokotsa A, and Dimitrakakis C. "Intrusion detection in MANET using classification algorithms: the effects of cost and model selection," Ad Hoc Networks, vol. 11(1), pp.226-237, 2013.
[64] Panos C, Xenakis C, Kotzias P, and Stavrakakis I. "A specification-based intrusion detection engine for infrastructure-less networks," Computer Communications, vol. 54, pp.67-83, 2014.
[65] Sánchez-Casado L, Maciá-Fernández G, García-Teodoro P, and Aschenbruck N. "A Novel Collaborative Approach for Sinkhole Detection in MANETs," In Ad-hoc Networks and Wireless*,* vol. 8629, pp.123-136, 2014.
[66] Sánchez-Casado L, Maciá-Fernández G, García-Teodoro P, and Aschenbruck N. "Identification of contamination zones for sinkhole detection in MANETs," Journal of Network and Computer Applications, vol. 54, pp.62-77, 2015.
[67] Ping, Y., Xinghao, J., Yue, W., and Ning, L. "Distributed intrusion detection for mobile ad hoc networks," Journal of Systems Engineering and Electronics, vol. 19(4), pp. 851-859, 2008.
[68] MohanapriyaM, and Krishnamurthi, I. "Modified DSR protocol for detection and removal of selective black hole attack in MANET," Computers & Electrical Engineering, vol. 40(2), pp.530-538, 2014.
[69] Nadeem A, and Howarth M P. "An intrusion detection & adaptive response mechanism for MANETs," Ad Hoc Networks, vol. 13, pp.368-80, 2014.
[70] Şen S, Clark J A, and Tapiador J E. Power-aware intrusion detection in mobile ad hoc networks, In Ad hoc networks*,* Springer Berlin Heidelberg, vol. 28,pp.224-239, 2010.
[71] Imran M, Khan F A, Abbas H, and Iftikhar M. "Detection and prevention of black hole attacks in mobile ad hoc Networks," In Ad-hoc Networks and Wireless, Springer Berlin Heidelberg, vol. 8629, pp.111-122, 2014.
[72] Gohargazi H, Jalili S, and Rahmanimanesh M. "Routing anomaly detection in OLSR–based MANETs," International Journal of Mobile Communications, vol. 13(3), pp.276-98, 2015.
[73] Meng Y, Li W, and Kwok L F. "Towards adaptive character frequency-based exclusive signature matching scheme and its applications in distributed intrusion detection," Computer Networks, vol. 57(17), pp.3630-3640, 2013.
[74] Zhang D, and Yeo C K. "A novel architecture of intrusion detection system," *7th IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV,* pp.1-5, 2010.
[75] Sumit S, Mitra D, and Gupta D. "Proposed intrusion detection on ZRP based MANET by effective k-means clustering method of data mining," IEEE *International Conference on Optimization, Reliability, and Information Technology (ICROIT), Faridabad,* pp.156-160, 2014.
[76] HortelanoJ, Calafate C T, Cano J C, De Leoni M, Manzoni P, and Mecella M. "Black-hole attacks in P2P mobile networks discovered through Bayesian filters," In *On the Move to Meaningful Internet Systems: OTM 2010 Workshops,* Springer Berlin Heidelberg, vol. 6428, pp.543-52, 2010.
[77] Al-RoubaieyA, Sheltami T, Mahmoud A, Shakshuki E, and Mouftah H. "AACK: adaptive acknowledgment intrusion detection for MANET with node detection enhancement," *24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth,WA,* pp.634-40, 2010.
[78] Darra E, Ntantogian C, Xenakis C, and Katsikas S. "A mobility and energy-aware hierarchical intrusion detection system for mobile ad hoc networks," In Trust, Privacy and Security in Digital Business, Springer Berlin Heidelberg, vol. 6863, pp.138-49, 2011.
[79] Bouhaddi M, Radjef M.S, and Adi K. "A game approach for an efficient intrusion detection system in mobile ad hoc networks," In Foundations and Practice of Security Springer International Publishing, vol. 8930, pp.131-46, 2014.

[80] Rafsanjani M K, Aliahmadipour L, and Javidi M M. "An optimal method for detecting internal and external intrusion in MANET," In Communication and Networking Springer Berlin Heidelberg, vol. 120, pp.71-82, 2010.

AUTHOR PROFILE

Rajan Patel is pursuing Doctoral Research in the area of Mobile Ad Hoc Network from RK. University, Rajkot, India. He has received Bachelor's of Engineering degree in Computer Engineering from Saurashtra University, Rajkot, India in 2004 and Masters of Technology degree in Computer Engineering from S.V. National Institute of Technology, Surat, India in 2009. Presently he is working as an Assistant Professor in the department of Computer Engineering, Sankalchand Patel College of Engineering, Visnagar, India. He has more than 12 years of total experience and published more than twenty four research publications in International Journals and conference proceeding including IEEE, Science Direct, Springer etc. He also reviews many research articles in National and International conferences of IEEE and Springer. His primary research area includes Security in Mobile Ad Hoc Network.

Pariza Kamboj is working as a Professor and Head in department of Computer Engineering, Sarvajanik College of Engineering and Technology, Surat, India. She received her B.Tech. and M.Tech. degree with honors in Computer Science and Engg. She has completed her Ph.D. in the domain of Mobile Adhoc Network. She has more than twenty years of experience and more number of research publications in International Journals and International Conferences with diversified areas. She delivered many expert talks and also acted as a reviewer of various national and international conferences and journals. Her areas of interest are Mobile Ad-hoc Network, Computer Networks, Mobile Computing and Pervasive Computing.