SECURE ROUTING PROPOSALS IN MANETS: A REVIEW

Amit Kumar[1], Vijay K. Katiyar[2] and Kamal Kumar[3]

[1,2]Department of Computer Engineering, M. M. University, Ambala, Haryana, India
[3]Centre for Information Technology (CIT), UPES, Dehradun, Uttarakhand, India

ABSTRACT

MANET has been around for more than two decades. Ad hoc network deployment, ability to cater emergent requirements on-the-spot and providing infrastructure less utility makes Ad hoc networks a play field for testing dynamics and applications. Wireless medium as medium for communication and lack of centralized control renders MANETs a favorable victim of hackers and intruders. Other features like change in the topology due to node's movements, battery depletion at nodes and coverage hampering due to obstacles in random terrains etc. adds to miseries of Ad hoc networks. With lots of proposals in recent times to cater the routing and security requirements in Ad hoc, this works presents a review of historic and current perspective in secure routing schemes in recent times.

KEYWORDS

Routing, Security Issues, Security Goals, Secure Routing in MANETs, Historic Perspective.

1. INTRODUCTION

Wide spread wireless digitization has become the need of hour. Evolution of MANETs on the horizon of wireless and infrastructure networking solutions offered a platform for materializing wireless digitization dreams. MANETs are peer to peer networks without any central control. MANETs are networks with self-configurability and self-organization. These characteristics of MANETs make them a preferred network, whenever and wherever a quick and temporary network deployment is required. Mere easier deployment is not that all. The highly Ad-hoc nature, depleting energy of nodes, mobility of nodes and physical obstacles of a terrain, affects the topology of the MANETs every now and then. This mandates the availability of self-configurable feature in MANETs. The deployment of MANETs in Military applications, border fencing, traffic monitoring, and production line control etc. deals with sensitive data. Data is relayed through intermediate nodes. The air is used as transmission medium. This mode of operations makes MANETs as targets for intruders and attackers. The security challenges in MANETs are stringent than that of wired networks. The limited capabilities of nodes, mobility, dynamic topology and lack of central control make it even difficult to provide a single security solution [1]. The native requirements of security like confidentiality, integrity, authentication, non-repudiation, availability, freshness etc. are difficult to achieve through single solution. The very nature of MANETs doesn't even allow the security solutions for wired networks to be used. To patch the security gaps in MANETs researchers around [2] the globe has proposed many solutions that not only try to customize wired network solutions to MANETs but also presented few MANETs specific solutions. Solutions proposed address different security requirements and offer defence against some of known security attacks. In this paper we present the challenges, open issues, current and historic perspective in security of the MANETs.

DOI:10.5121/ijfcst.2016.6102

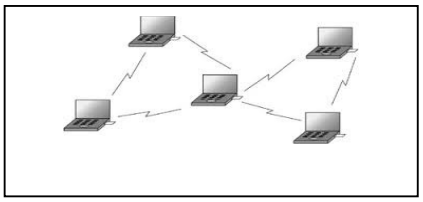

Figure 1 Mobile Ad hoc Network

In Section 2 we present classification of routing protocols. Section 3 & 4 discuss various security issues and security goals respectively. Section 5 introduces security approaches in MANETs. Section 6 explains different secure routing protocols in MANETs. We conclude this paper in Section 7.

2. ROUTING PROTOCOL IN MANETS

Routing Schemes in MANETs are classified into Reactive, Proactive and Hybrid category on the basis of mode of operation. Further classification is due to network structure and classes identified are Flat, Hierarchical and Location or Geography based routing schemes. Another Classification is due to Routing strategy and schemes in this class can be studied under QoS based and Multipath Routing schemes. Figure 2, presents a classification of routing protocols in MANETs.

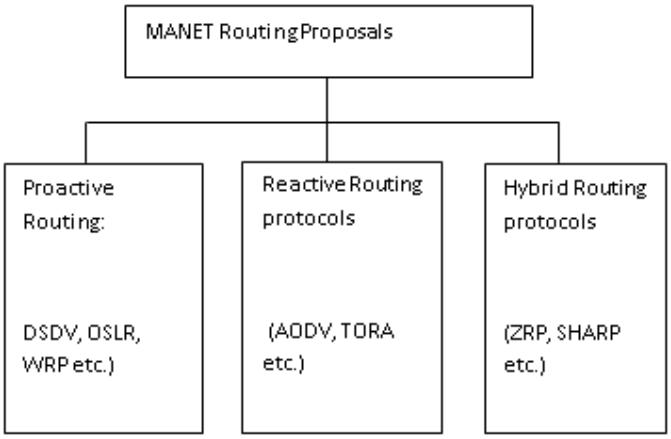

Figure 2 Classification of routing protocols in Ad hoc Networks

2.1 Proactive Routing Protocols

Proactive class of routing schemes stores the routing information gathered from neighbouring nodes through periodic or event based updates. Information received via updates is maintained as routing tables.

The change in the topology due to node movement, energy drain or physical obstacles or physical security attacks initiate next round of updates. Each node may maintain partial or total network topology and thus time and energy spent in convergence of routing information in nodes consume a lot of time and energy. There are times when nodes in the network may possess unstable routing information. Routing protocols like DSDV (Destination Sequenced Distance Vector) [3], OLSR

(Optimized Link State Routing) [4], WRP (Wireless Routing Protocol) etc. are representative protocols in this category.

2.2 Reactive Routing Protocols

Proactive routing schemes suffer performance limitation due to frequent route updates due dynamic topology changes. To overcome these limitations and frequent topology changes, routes may be computed only when it is actually required. Reactive routing schemes follow the suit of temporal update and prevent the instances of unstable network state. DSR (Dynamic Source Routing) [5], AODV [1] (Ad hoc On demand Distance Vector) and TORA (Temporary Ordered Routing Protocol) [6] etc. are the representative routing schemes in this category.

2.3 Hybrid Routing Protocols

Often single feature routing protocols suffers from limitation due to its very mode of operations. Combining the best of two or more classes of protocols often covers the limitation of other class. Hybrid routing protocols combines the features of both reactive and proactive routing protocols and attempt to overcome the limitations of each class of protocols through some customizations in basic operation modes of constituting members. ZRP (Zone Routing Protocol), SHARP (Sharp Hybrid Adaptive Routing Protocol, DHAR (Dual-Hybrid Adaptive Routing) & ADV (Adaptive Distance Vector Routing), TORA etc. are the representative proposal in this categories.

3. SECURITY ISSUES IN MANETS

MANETs are most challenging networks. Due to its very nature of using hostile environments and air-as-medium, MANETs are exposed to different types of active and passive attacks. Active attacks are performed by adversaries who are sufficiently equipped with sophisticated tools. They can not only change the data relayed through networks but also corrupt network's functioning by altering routing, topology and link related updates. Actives attacks like DoS, DDoS, Impersonation, Worm-hole attack, Black-hole attack, Byzantine attacks etc. Other possible attacks are launched by adversaries with limited capabilities. Such attacks can be classified into passive attacks, like eves-dropping, overhearing etc. Some basic constraints [7], [8], [9] and open challenges security aspects in MANETs may be describes as below:

Distributed management: Due to peer-to-peer nature of nodes and Ad hoc installation of MANETs, no centralized control can be established. Distributed nature of MANETs affects the authentication of new nodes, maintaining different generations of nodes, secure distribution of data and keying information, loose control on topology changes etc. are all affected due to lack of centralized control.

Limited resource: Due to Ad hoc and temporal deployment in resource constrained and difficult surrounding, Ad hoc networks suffer from lack of power resources, bandwidth and computational limitations. Due to limited resources Ad hoc networks are paly ground for attackers and developers. Resource limitation has greatly affected the solution space in Ad hoc networks.

Cooperativeness: Due to peer to peer architecture and lack of any centralized control has changed MANETs from client-server to cooperative networks. The cooperation seeks trust among nodes during exchange of any data or routing. Any deviation from cooperative behavior and turning into selfish or compromised nodes establishes the requirements of customized security solutions and forced cooperation among nodes in MANETs.

Dynamic topology: Mobility of nodes, depletion of energy in nodes, nodes revocation due to action against malicious and selfish nodes, physical obstacles and physical node compromise resulted into dynamic nature of wireless network topology requires adaptive security solutions.

4. SECURITY GOALS IN MANETS

Similar to other networks, Ad hoc networks require that security policy and implementation should be a step forward towards realization of certain security goals. Theses may be highlighted as below:

- Authentication
- Integrity
- Confidentiality
- Non-repudiation
- Availability
- Data Freshness

Most of the goals are common with other networks except freshness. Data Freshness is important in Ad hoc networks as Ad hoc networks lacks centralized control. Lack of centralized control and poor synchronization has exposed such networks to collusions at the part of malicious or selfish nodes. This is why data freshness in Ad hoc security policy has found its place in security goals of MANETs.

5. SECURITY APPROACHES IN MANETS

There are different security threats in MANETs at each layer of protocol and to counter them various approaches are used. These approaches fulfil security requirements at each layer of a protocol in MANETs. In MANETs' security provisioning is made available through or using either of the key management, Intrusion Detection System (IDS) or secure routing.

5.1 Key Management Schemes

Key management involves, key distribution, key refreshing and key revocation. Through various keys for encryption, decryption and Message Authentication Codes (MAC) generation, node's authentication and data freshness, security breaches can be identified well in time, before such breach leads to large scale attacks. Use of symmetric or asymmetric keys cryptography in Ad hoc is exercised in various proposals. Further to it, network key, group key or pair wise keys are used to address network level, group level or node-to-node interaction respectively.

When single key is used across the network for securing the information exchange, it is classified as network key. When group of mobile nodes in MANETs are assigned a single key this is called group key. Generation, distribution and revocation of group keys are all distributed processes by its very nature as group keying is managed by a group of logical or physical neighbour nodes [10]. Various proposals have further classified group keying as centralized, distributed and decentralized.

5.2 Intrusion Detection System (IDS)

Another approach for attack detection only is called Intrusion Detection System (IDS). IDS [11], [12] can be classified as either Rule Based or Signature Based and Anomaly Detection Based. Rule based IDS detect the intrusion by comparing the signatures against signature data base. The freshness of signature data base and missing entries against new attacks can't be classified as

intrusion. Anomaly based detection system is able to detect any deviation from normal behaviour by comparing traffic patterns, energy consumptions or delays in acknowledgement etc. [13], [14], [15] and [16]. Several solutions reviewed in this paper can be simultaneously classified in IDS category as well as secure routing. A proposal in [17] is used to detect anomaly by computing the deviation from normal behaviour in terms of forwarding behaviour. Authors in [18] proposed a IDS for reactive routing schemes.

6. SECURE ROUTING

6.1 Secure Routing: Historic Perspective

With security gaining as QoS parameter in Ad hoc networks, secure routing is gaining as playground for security provisioning in Ad hoc networks. Secure routing is either achieved through fixing pre-existing routing schemes or by proposing security aware routing proposals. This section presents historic and current perspective in secure routing solutions proposed in MANETs.

6.1.1 Authenticated Routing for Ad hoc Networks (ARAN)

ARAN uses the concept of certificates from trusted server for the authentication of nodes [19]. Primarily Route discovery requests are verified using Digital Signature Authentication and equivalent of end-to-end authentication.

Route Discovery is message is propagated through broadcast but replies from destinations are unicast. The process of DSA is applied not only during route discovery but also during route reply. ARAN has certificate revocation procedure in place. The certificates are assumed to serve for limited time and should be renewed with trusted certificate server. Each route discovery message is signed using private key and contains a nonce (monotonically increasing), current time-stamp, and IP. Nodes keeps track of nonce and time-stamp for each node from which they receive route discovery message. A message with same nonce but different time stamp is acceptable. Nodes refrain from forwarding duplicate RDP from same source IP. Nodes on route from source to destination verify and re-sign RDP with its own private key. This same process is phase two and ensures end-to-end authentication. Third phase is optional in the sense that a costly procedure is adopted to ensure shortest path between source and destination.

6.1.2 Secure Efficient Ad hoc Distance Vector Routing (SEAD)

SEAD [20] is proposed to secure the proactive or table driven Ad hoc routing protocol called DSDV [21]. DSDV principally works on the principle of sequence number of update assigned by source and hop count field. Sequence number helps nodes to keep the track of duplicate packets and hop count is used to prevent the infinite looping of packets in the network. The incorporation of DSDV in Bellman's-Ford algorithms adds to miseries of DSDV as distributed version of all-pair-shortest-path algorithm is computationally very costly. It takes lot of time and communication overhead to maintain consistent state across the nodes in whole network. The manipulation of sequence number of update packets and hop count leads to erroneous functioning of DSDV. SEAD provides security by preventing unauthenticated nodes from updating mutable field in the packets. Nodes are compulsorily assumed to obtain cryptographic information like Authentication key and adopt Secure Key Exchange methods like Diffie-Hellman etc.

6.1.3 Secure Routing Protocol (SRP)

SRP is generic security extension module and can be used to extend any reactive Ad hoc routing protocol which uses route request broadcasting approach while querying for route on demand

basis [22]. Only DSR is considered in the proposal for most suitable extension. SAR uses symmetric key cryptography for achievement of authentication between neighbouring nodes. Keying material is presumed to be pre-distributed among nodes. The existence of certification authority is assumed for secure key distribution. Symmetric keying approach is faster as compared to asymmetric keying approach, but to ensure high degree of connectivity, each node needs to maintain sufficiently large number of keys. Reducing on number of keys may either hamper the connectivity. Considering either group-key concept or network wide secure keys leads to chances of network-segment or network wide compromise in case of single node compromise. Proposal fails to consider the performance against leading active attacks.

6.1.4 Ariadne

Ariadne is a security extension to reactive routing protocols in Ad hoc networks. Ariadne [23] is available for DSR protocol. Instead of using the concept of hop-by-hop approach, Ariadne preferred to offer semantic security by opting end-to-end security between pair of nodes called source and destination. The Message Authentication Code (MAC) is used to authenticate senders and receivers for point to point messages. Another provision made by Ariadne is to secure broadcast messages like RREQ. Broadcast Authentication scheme called TESLA is exploited to achieve authentication of broadcast messages. The incorporation of TESLA leads to stringent requirements on clock synchronization. This is very weird assumption which is difficult to achieve. Besides these Ariadne offers a new approach to ensure the validity of route error messages in the route maintenance phase. Some leading attacks like wormhole attack, feedback loop and honest node manipulation, detection of compromised node etc. are the open challenges for Ariadne to consider.

6.1.5 Secure Ad hoc On-demand Distance Vector Routing (SAODV)

SAODV [24] is customized AODV for security provisioning. One way hash chaining and Digital Signature Authentication is used to enhance security of AODV. As each packet contains mutable and non-mutable fields, non-mutable fields are encrypted using digital signature while mutable fields like hop-count are secured using hash-chaining. Hash chaining is irreversible in nature. Every route request packet is associated with new hash chain. SAODV assumes the existence of trusted certification authority CA, for issuing certificate. SAODV works on asymmetric key based digital signature, public keys of nodes are sent along with each route request packet being sent. The limitation in SAODV is that hop-by-hop authentication leads to increase not only computational overhead but also increases communication overhead. Another limitation is the assumption of CA, which by its very nature very defunct assumption. The failure of SAODV against feedback loop attack and manipulation of honest nodes on the route replies by compromised or malicious nodes is not considered in the proposal.

6.1.6 Secure Link State Routing Protocol (SLSP)

Authors in [25] proposed a mechanism to securely discover the neighbouring nodes and secure the dissemination of topology of the network known to them. Nodes in SLSP are aware of local topology within the range of R hops. Nodes in SLSP broadcast their public key in their zone of R-hops. Nodes sign the Link State Updates and Link Information and broadcast. Each new node entering in the zone broadcast its public key. Only nodes in the zone are validated for their broadcasts and thus nodes maintain only few keys. The consistent information on a particular links by nodes incident on link established the validity of the link correctness and its acceptance as new information to be further propagated. SLSP binds the IP and MAC of a node. This helps the protocol to avoid the node replication at MAC Level. To accommodate these features a Neighbour Lookup Protocol is added. Binding of multiple IPs with same MAC, overloading the

network with extra traffic, malicious and selfish behaviour can be easily isolated by using MAC-IP bindings. SLSP is able to counter DoS attack by prioritizing the nodes on the basis of rate of querying. Nodes with least querying rate are given highest priority.

6.1.7 On-demand Secure Routing Protocol Resilient to Byzantine Failures (OSRP)

Byzantine attacks hamper the normal functioning of the routing protocols by altering routing information, dropping and modifying etc. [26]. Such nodes are classified as Malicious and routes containing such nodes are given more weight than others provided that route selection is oriented towards least weight route selection. Byzantine behaviour is reflected by authenticated nodes. The detection of faults is after *log (n)* faults where *n* represents number of nodes in the route. To implement the detection of node originating the fault, source node uses binary search until the fault location is confirmed to single link. The probe in-fact is query to be acknowledged by each node on the legitimate routes. Failing to acknowledge on successive binary search instances helps to identify the link with problem.

6.1.8 Watchdog and Pathrater

Watchdog and Pathrater [2] are the proposal for almost intrusion detection and identification of non-cooperating nodes. Non-cooperating nodes may be either selfish or compromised nodes. Compromised nodes may selectively drop the messages or selfish node may drop due to overloading in broadcast environment. The path-rater module rates the paths among the nodes on the basis of message forwarding behavior of the nodes on the path. The proposal was considered for extending DSR, but both Pathrater and Watchdog can be used to extend any routing protocol in ad-hoc wireless networks environment.

6.1.9 Cooperation of Nodes: Fairness InDynamic Ad hoc NeTworks (CONFIDANT)

CONFIDANT is security fortification of DSR by promoting nodes for cooperation. Non-cooperative nodes are isolated from network activities. This motivates each node to cooperate actively in the routing activities. The routing decision and trust relationships are decided on the basis of nodes experience, observations, routing and forwarding behaviour of nodes [27]. Nodes in CONFIDANT maintain a finite state machine with four major components, called Monitor, Reputation Manager, Trust Manager and Path Manager. Monitor closely maintains neighbourhood watch and reports any deviation from model behaviour. Trust Manager Component sends ALARM messages about node's experience about malicious activities of other nodes. ALARM received by node is treated as per sender node's trust level. Trust is given importance at the time of deciding in routing decisions. Reputation Manager maintains the trust levels as per node's experience, observation and routing behaviour.

6.1.10 Security-aware Ad hoc Routing (SAR)

SAR [28] extends QoS set by including security in routing. Instead of several other parameters like distance, delay or security is used to rate any routing scheme. Proposal can be safely applied to any proactive, reactive or hybrid routing schemes.

6.1.11 Security Protocol for Reliable Data Delivery (SPREAD)

In [29] authors proposed reliability aware secure and multi-path routing schemes with desired optimality criteria. The proposal caters multiple objectives. The confidentiality of secure messages is ensured by using multiple shares of a message routed through multiple optimal paths across the hostile and insecure network. To obtain shares the optimality criteria of routes is

considered. The loss or compromise of one or more shares of a secret message doesn't expose the contents as unless all the shares are joined together. The multi-path routing scheme is also proposed as part of work.

6.1.12 Miscellaneous Historic Solutions:

Techniques for Intrusion Resistant Ad hoc Routing Algorithms (TIARA) [30] identified and presented a collection of design rules that can be applied to overcome the impact of malicious nodes and ensure acceptable level of operation of network under DoS attack. A proposal called BISS in [31] improvised existing routing schemes wit incomplete Security Associations (SAs) by using MACs and digital signatures. Similar to Ariadne BISS affects only RREQ. In [32], [33], [34] authors endorse IPSec as default solution for Ad hoc networks for providing confidentiality, authentication and integrity. IPSec suffers from computational overhead due to several encryptions and verification steps. Secure Message Transmission (SMT) [31] ensures to achieve multiple security goals by using Information Dispersal Algorithm (IDA) [35]. Each message was divided into statistically related fragments containing limited redundancy. To address the integrity and confidentiality of each fragment, MAC was also routed along with through multiple paths. MAC also ensured the authentication of the source. Another proposal in [36] proposed to use multiple paths between a pair of senders and receivers. Multiple paths are used to segment the message into pieces and route across network via multiple paths. The process certainly enhances the confidentiality by making it useless to capture any piece unless all the pieces are joined together. This requires a highly infected network with omnipresent adversary to break into messages. Authors in [37] proposed Jigsaw Puzzle scheme for Ad hoc networks and ensure confidentiality and integrity. A proposal in [38] uses Jigsaw Puzzle [37] to obtain pieces of the message to be routed across the network through multiple paths. No information can be retrieved from any captured piece unless all the pieces are joined together.

6.2 Secure Routing: Current Perspective

This section presents the current research directions in secure routing in MANETs. Many promising proposal proposed in recent times have been reviewed and discussed below.

6.2.1 Secure Route Discovery Protocol (SRDP): In [39] authors proposed Secure Route Discovery Protocol (SRDP) for minimizing communication overhead and computation overhead. SRDP relies on MAC and Digital Signatures. Novelty of the SRDP is aggregation of signatures and multi-signatures. Authors proposed a new adversary model with feedback loop and considered attacks which manipulates honest nodes between a pair of compromised nodes and may insert a node between a pair of compromised nodes. Such attacks results into manipulated routes in the RREP in DSR. SRDP considered only active adversaries. A concept of putative routes is introduced in the proposal where source nodes are able to verify the presence of each honest node on the route and each honest node has the same view of the topology. Instead of using authentication tags during RREQ, intermediate nodes in SRDP keeps a hash of prefix of the route on RREQ. It helps the nodes to identify the duplicate RREQ. Backward authentication is ensured through attaching a MAC or Signature of route on the RREP. It can be any time compared with the cached information to identify any discrepancy.

6.2.2 Exhaustive Topology Evaluation: In [40] authors proposed new automated approach for evaluation of secure routing protocols. Most of the routing protocols till date consider the standard network topology and few standard message exchange scenarios. Most evaluation techniques lack exhaustive and automated evaluations. A new model based approach was proposed in [40] that evaluates the given routing protocols for all potential network topologies and attacks. The optimizations have been applied by using equivalence classes for classifying

reducing the number of possible topologies to be considered for analysis. The results of the proposal are motivational.

6.2.2 Modified DSR (MDSR): In [41] authors proposed a Modified DSR (MDSR) routing protocols that note only detect intrusion, but also classifies the nodes as malicious nodes and finally ensure that malicious nodes no longer considered as part of the routes. Each time new node which is suspected to be malicious is confirmed for its suspicious behavior it is added to black list of each node. MDSR considers a special kind of black hole attack called Selective Black Hole attack. MDSR uses Intrusion Detection System (IDS) nodes placed across the network and remain in promiscuous mode. These nodes come into action only when these nodes are first informed of malicious nodes by destination nodes. MDSR consider four new kind of packets called Query REQest (QREQ), Query REPly (QREP), Malicious Node REQest (MNREQ) and ALARM. Destination nodes initiates suspicious node detection with QREQ which is replied through QREP.

Table 1 Parametric Analysis of Secure Routing Protocols

Reference	Keys	RREQ	RREP	Node Authentication	Reactive/ Proactive /Hybrid	Attacks Identify
Sanzgiri, K. et.[19]	1. PKI	Yes	Yes	Yes	Reactive	1. Malicious
Hu, Y. C. et.[20]	1. PKI	--	--	Yes	Proactive	1. Modification
Papadimitratos, P. et [22]	1. Symmetric key	Yes	No	Yes	Reactive	
Hu, Y. C. et.[23]		Yes	No	Yes	Reactive	1. Wormhole 2. Feedback loop 3. Honest node manipulation, 4.Detection of compromised node
Zapata et [24]	1. PKI	Yes	Yes	Yes	Reactive	1. Modification 2. Fabrication
Mouftah, H. et.[25]	1. PKI	Yes	No	Yes	Reactive	1. DoS
Awerbuch, B. et.[26]	1. Fault Detection Based	Yes	Yes	Yes	Reactive	1. Byzantine 2. Malicious Nodes
Marti, S. et.[2]	1. Reputation Based	Yes	No	Yes	Reactive	1. Malicious Nodes 2. Selfish Nodes
Buchegger, S. et.[27]	1. Trust and Reputation Based	Yes	Yes	Yes	Reactive	1. Selfish Nodes
Lou, W. et. [29]	1. Multiple Shares via Multipath	----	----	-----	Reactive	1. Modification 2. Fabrication
Ramanujan, R.et. [30]	1. Intrusion Detection Modelling	Yes	No	Yes	Reactive	1. DoS 2. Malicious Nodes
Kim, J. et. [39]	1. PKC	Yes	Yes	Yes	Reactive	1. Feedback Loop 2. Honest Node Manipulation
Andel, T. R. et al. [40]	--------	Yes	Yes	Yes	Reactive	
Mohanapriya, M. Et. [41]	1. IDS based Modelling 2. PKI	Yes	Yes	----	Reactive	1. Malicious Nodes 2. Black hole
Adnane, A. et. [42]	1. Trust based on	-----	-----	----	Reactive	1. Malicious Node 2. Selfish Node

	Trust Language					3. Identity Spoofing 4. Black hole
Qazi, S., Raad et. [43]	1. Round Trip Time based	-----	-----	-----	Reactive	1.Wormhole attack
Kargl, F. et. [44]	1. Asymmetric key	Yes	Yes	Yes	Reactive	1. Information Leakage 2. Malicious Nodes 3. Selfish Nodes
Choudhury, D. R. et. [45]	------	------	------	------	Reactive	1. Black hole
Das, D. et.[46]	------	------	------	------	Reactive	1. Selfish Nodes
Dholey, M. K. et.[47]	1. PKI 2.Group key	------	Yes	Yes	Reactive	1. Malicious
Raza, I. et.[48]	1. Trust Based	RREQ	RREP	Yes	Reactive	1.Impersonation 2. Collusion 3. Black hole 4. Malicious
Von Mulert, J. et.[49]	1.Simulation analysis	------	------ -	-------	Reactive	1. Misbehaviour 2. Resources limitation effects 3. Black-hole 4. Wormhole

QREQ is for a node two hop away, and helps each node in concluding whether intermediate node can be put into suspicious category provided Probably Malicious (PM) scores of node reached a threshold level. Once a node is suspected as malicious, IDS nodes placed near to PM node switch into promiscuous state. Source is asked to send another series of data packets. If malicious node still drops the packets, IDS nodes circulates this information to all the nodes through nearby IDS nodes. The performance degradation due to increase in Communication overhead was reported 8% compared to DSR. The MDSR was evaluated for end-to-end and packet drop ratio and overhead (bits/sec).

6.2.3 Trust based Secure OLSR: In [42] authors proposed a new approach to secure OLSR routing protocol called trust based secure OLSR. OLSR is link state routing protocol with selective broadcast forwarding through forwarders. Considering Trust based approach is justified by very nature of Ad hoc network which functionally depends upon the co-operations with neighbouring nodes. Authors referred trust language specified in [43] and specify trust classes. Trust classes are defined on the basis of role of nodes and context of operation. As Multi Point Relay (MPRs) are functional specification of OLSR, secure version consider trust based forwarding by MPRs. OLSR routing tables maintain single and shortest route towards each node. This is exploited by malicious or compromised nodes to provide false information about the topology of network and disrupt normal functioning of OLSR. To detect any anomaly in the topology being circulated and to identify malicious nodes OLSR messages, TC and Hello, are checked for consistency. Nodes in the proposed secure OLSR has to check its trust relationship with MPRs via MPR's behaviour in generation of TC messages about the topology and forwarding of data packets and TC messages. If the behaviour of nodes resembles to as expected in OLSR then nodes have correct relationship with their MPRs otherwise, an incorrect relationship. This approach classifies nodes with malicious behaviour. Authors called it trust based reasoning. On the basis of trust based reasoning nodes themselves validate their trust relationships with nodes. The simulation of the proposed work was done in Glomosim and various attacks like flooding, hello message, Identity spoofing, Black Hole attacks were considered for analysis.

6.2.4 RTT based Wormhole Detection in Reactive Routing: In [43] authors presented a solution against wormhole attack on the basis round trip time (RTT) for packets. Authors replaced

complex solution with limited usability with a feasible solution. RTT calculations also include the computations on queuing and processing delays across multiple hops in the network. Authors assumed fixed number of malicious nodes M>1. Each packet like RREQ and RREP is divided into two parts, Fixed and Dynamic. Dynamic parts carry information like time stamp and packet size etc. On the basis prevailing data rates RTT is computed and conclude if any wormhole is present. The proposal considered the evaluations against packet encapsulation wormhole, out-of-band, high-power-transmission and packet relay wormholes. This proposal considered multi-rate Ad hoc networks which were not considered earlier. The detection of wormholes in each instance of wormhole type was highly promising.

6.2.5 Secure DSR (SDSR): In [44] authors presented Secure DSR (SDSR) protocol. To address the issues related to malicious behaviour, selfish behaviour and information leakage like attacks SDSR sets several goals like ensuring integrity of routes, freshness of routes, exchange of session keys and authentication of participating nodes. MANET-ID based concept which in-fact RSA key pair that prevent against forging new node Id. SDSR is based on asymmetric key cryptography. The RREQ with several static information and nonce is signed with private key called MANET-ID and across the nodes on source to destination nonce is transformed by each node. During RREP traversal, intermediate nodes may verify the source route and revert the transformations to nonce. For secure data exchange session keys are exchanges using Diffie –Hellman key exchange. The use of nonce transformations prevents against any route modifications. SDSR attempts validation using BAN formalism and proves that SDSR is better approach to secure DSR.

6.2.6 Detection of Black Hole in DSR: In [45] also authors presented a proposal to counter black hole attack. A modification is applied to the source of any RREQ. A table called RREQ_Tab for storing more than one RREP corresponding to a RREQ, a timer M_WAIT_TIME upto which source will receive RREP and arrange them in RREQ_Tab. M_WAIT_TIME is set to half of the RREP_WAIT_TIME. An implementation of the proposal was carried out in ns2. Authors lacked the clarity of the idea and its presentation in the proposal.

6.2.7 Least Cost Total Factor (LCTF) based Reactive Routing: In [46] authors presented a solution to identify the selfish nodes and guarantee of shortest path between source and destination by using game theoretic approach and Least Cost Total Factor (LCTF) respectively. If any route is broken, then proposal guarantee of selection next least cost path between source and destination. Game theoretic approach uses the relationship between players and can predict the decisions of players optimally. This approach is used to predict the behaviour of nodes and classify selfish nodes. The network and all its nodes will benefit only if there is cooperation. This proposal considered non-cooperative game model. Each node has associated Cost Factor (CF) which is calculated on the basis of distance from other nodes, power availability, bandwidth etc. To route a packet via this node other nodes has to pay cost CF to this node. The objective function of this game theoretic approach is maximizing utility or CF payoffs for each node. As only forwarding packets earn benefits and dropping causes payoffs during sending own packets, selfish nodes leads to own bankruptcy, so nodes are by default pushed for cooperation and avoid boycott as selfish nodes. Nodes not forwarding RREQ packets are allowed to repeat selfish behaviour until their potential misbehaviour not reached upper threshold value. Reaching to threshold value helps source to conclude on the selfish behaviour and propagate to blacklist node as selfish node. Using same concept proposal identifies selfish nodes which deny to forward data and acknowledgement packets. The simulation based implementation is not discussed in the proposal and lacks the ground.

6.2.8 Group key based Malicious Node Detection in Reactive Routing: In [47] authors proposed an algorithm to overcome the challenge of malicious node between source and

destination during RREP. Cryptographic material like public key, private key and group key is used to tackle the challenge. The group key is updated when a new node joins the group. Nodes establish a group with the nodes in its neighbourhood. This prevents the intruder from obtaining any information of who is the source and present wrong information to the source. The exchange of the keys is established using Group Diffie-Hellmen key exchange protocol. The ability of the proposal to defend was established through conceptual steps.

6.2.9 Distributed Trust based Secure AODV: In [48] authors proposed to protect AODV against impersonation, collusion and black hole attacks. All these solution are handled using malicious node detection based on reputation of a node. Reputation is other node's opinion about a particular node. Trust level below a threshold is alarming situation and factor out a node from taking part in any route determination in AODV. AODV packet format was not altered and no overhead thus introduced. Nodes behave as a guard nodes as well as normal nodes. Nodes compute trust of other nodes and routes on the basis of their behaviour by over-hearing their transmissions. A simple approach in terms of concept and overhead is proposed in fact.

6.2.10 Security Analysis of AODV and SAODV: In [49] authors presented a review on the strengths and security limitations of AODV and SAODV. SAODV is security extension of AODV using some symmetric key cryptography and end-to-end security provisioning. Authors conducted vulnerability tests of SAODV and identified some unresolved issues like such as MAC layer misbehaviour, resources limitation effects, Black-hole attack, and different types of wormhole attacks etc. This analysis was extended to compare the schemes under self-healing category, trust based schemes, directional antennae based proposals and IDS based approaches. The review presented by authors identified the gaps left in various proposals.

7. CONCLUSION

This paper has discussed security issues, goals along with a detailed review of historic and current perspective in secure routing schemes for MANETs. Table 1 presents the conclusions in tabular form. Each protocol has different operational requirements and provides protection against different attacks by using specific approaches. Secure routing protocols are method of choice over IDS and key management. Historic proposals either stressed to improve the RREP or RREQ. Historic solutions don't consider the extra transmission by nodes which are not going to be the part of the routes, misbehaviour of nodes, and honest node manipulation by malicious nodes. Current solutions consider security provisioning in both, RREP and RREQ. Trust based solutions have also been proposed with reputations of nodes being computed on the basis of forwarding behaviours of nodes. Overhead of security provisioning in existing or new routing protocols adds overhead in terms of communication, storage and computation. Future work on secure routing schemes may consider location specific keying information for reduced storage and communication overheads. Heterogeneity of nodes may be considered for resource harness.

REFERENCES

[1] Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561).

[2] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.

[3] Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM computer communication review* (Vol. 24, No. 4, pp. 234-244). ACM.

[4] Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)* (No. RFC 3626).

[5] Johnson, D. B., Maltz, D. A., Hu, Y. C., & Jetcheva, J. (2003). The dynamic source routing (DSR) protocol for mobile ad hoc networks. *IETF Draft, draft-ietf-manet-dsr-009. txt*.

[6] Park, V., & Corson, M. S. (1997). *Temporally-ordered routing algorithm (TORA) version 1 functional specification* (pp. 2-6). Internet-Draft, draft-ietf-manet-tora-spec-00. txt.
[7] LUNDBERG, J. Security in Ad hoc networks. *2000). http://citeseer. nj. nec. com/400961. html*.
[8] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.
[9] Toner, S., & O'Mahony, D. (2003, January). Self-organising node address management in ad hoc networks. In *Personal Wireless Communications* (pp. 476-483). Springer Berlin Heidelberg.
[10] Wu, B., Wu, J., & Dong, Y. (2009). An efficient group key management scheme for mobile ad hoc networks. *International Journal of Security and Networks*, *4*(1-2), 125-134.
[11] Northcutt, S., & Novak, J. (2002). *Network intrusion detection*. Sams Publishing.
[12] Khan, S., Loo, K. K., & Din, Z. U. (2010). Framework for intrusion detection in IEEE 802.11 wireless mesh networks. *Int. Arab J. Inf. Technol.*, *7*(4), 435-440.
[13] Chen, T., Kuo, G. S., Li, Z. P., & Zhu, G. M. (2007).*Intrusion detection in wireless mesh networks* (pp. 146-169). CRC Press, New York, NY, USA.
[14] Rafsanjani, M. K., Movaghar, A., & Koroupi, F. (2008). Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes. *World Academy of Science, Engineering and Technology*, *20*, 351-355.
[15] Ramanathan, S., & Steenstrup, M. (1996). A survey of routing techniques for mobile communications networks. *Mobile Networks and Applications*, *1*(2), 89-104.
[16] Zeng, Q. A., & Agrawal, D. P. (2002). Introduction to wireless and mobile systems. *CENGAGE Learning*.
[17] Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.
[18] Forouzan, B. A. (2007). *Cryptography & Network Security*. McGraw-Hill, Inc.
[19] Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). Authenticated routing for ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, *23*(3), 598-610.
[20] Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad hoc networks*,*1*(1), 175-192.
[21] Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM computer communication review* (Vol. 24, No. 4, pp. 234-244). ACM.
[22] Papadimitratos, P., Haas, Z. J., & Samar, P. (2002). The Secure Routing Protocol (SRP) for Ad Hoc Networks: IETF Internet Draft draft-papadimitratos-secure-routing-protocol-00. txt.
[23] Hu, Y. C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless networks*, *11*(1-2), 21-38.
[24] Zapata, M. G. (2002). Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), 106-107.
[25] Mouftah, H., & Ho, P. H. (2001, March). SLSP: A new path protection scheme for the optical Internet. In *Optical Fiber Communication Conference* (p. TuO1). Optical Society of America.
[26] Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002, September). An on-demand secure routing protocol resilient to byzantine failures. In *Proceedings of the 1st ACM workshop on Wireless security* (pp. 21-30). ACM.
[27] Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing* (pp. 226-236). ACM.
[28] Yi, S., Naldurg, P., & Kravets, R. (2001, October). Security-aware ad hoc routing for wireless networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing* (pp. 299-302). ACM.
[29] Lou, W., Liu, W., & Fang, Y. (2004, March). SPREAD: Enhancing data confidentiality in mobile ad hoc networks. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies* (Vol. 4, pp. 2404-2413). IEEE.
[30] Ramanujan, R., Ahamad, A., Bonney, J., Hagelstrom, R., & Thurber, K. (2000). Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). In *MILCOM 2000. 21st Century Military Communications Conference Proceedings* (Vol. 2, pp. 660-664). IEEE.
[31] Papadimitratos, P., & Haas, Z. J. (2003). Secure message transmission in mobile ad hoc networks.*Ad Hoc Networks*, *1*(1), 193-209.

[32] Atkinson, R., & Kent, S. (1998). Security architecture for the internet protocol.
[33] Raymond, J. F. (2001, January). Traffic analysis: Protocols, attacks, design issues, and open problems. In *Designing Privacy Enhancing Technologies* (pp. 10-29). Springer Berlin Heidelberg.
[34] Sufatrio, K., & Lam, K. Y. (1999). *Scalable Authentication Framework for Mobile IP (SAFE-MIP)*. Internet Draft, draft-riomobileip-safe-mip-00. txt.
[35] Rabin, M. O. (1989). Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM (JACM)*, *36*(2), 335-348.
[36] Raymond, J. F. (2001, January). Traffic analysis: Protocols, attacks, design issues, and open problems. In *Designing Privacy Enhancing Technologies* (pp. 10-29). Springer Berlin Heidelberg.
[37] Vasudevan, R. A., & Sanyal, S. (2011). A novel multipath approach to security in mobile ad hoc networks (MANETs). *arXiv preprint arXiv:1112.2128*.
[38] Rivest, R. L. (1997, January). All-or-nothing encryption and the package transform. In *Fast Software Encryption* (pp. 210-218). Springer Berlin Heidelberg.
[39] Kim, J., & Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. *Ad Hoc Networks*, *7*(6), 1097-1109.
[40] Andel, T. R., Back, G., & Yasinsac, A. (2011). Automating the security analysis process of secure ad hoc routing protocols. *Simulation Modelling Practice and Theory*, *19*(9), 2032-2049.
[41] Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers & Electrical Engineering*, *40*(2), 530-538.
[42] Adnane, A., Bidan, C., & de Sousa Júnior, R. T. (2013). Trust-based security for the OLSR routing protocol. *Computer Communications*, *36*(10), 1159-1171.
[43] Qazi, S., Raad, R., Mu, Y., & Susilo, W. (2013). Securing DSR against wormhole attacks in multirate ad hoc networks. *Journal of Network and Computer Applications*, *36*(2), 582-592.
[44] Kargl, F., Schlott, S., & Weber, M. (2005, January). Secure dynamic source routing. In *null* (p. 320c). IEEE.
[45] Choudhury, D. R., Ragha, L., & Marathe, N. (2015). Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack. *Procedia Computer Science*, *45*, 564-570.
[46] Das, D., Majumder, K., & Dasgupta, A. (2015). Selfish node detection and low cost data transmission in MANET using game theory. *Procedia Computer Science*, *54*, 92-101.
[47] Dholey, M. K., & Biswas, G. P. (2015). Proposal to Provide Security in MANET's DSRRouting Protocol.*Procedia Computer Science*, *48*, 440-446.
[48] Raza, I., & Hussain, S. A. (2008). Identification of malicious nodes in an AODV pure Ad hoc network through guard nodes. *Computer Communications*,*31*(9), 1796-1802.
[49] Von Mulert, J., Welch, I., & Seah, W. K. (2012). Security threats and solutions in MANETs: A case study using AODV and SAODV. *Journal of network and computer applications*, *35*(4), 1249-1259.

AUTHORS

Amit Kumar is presently working as Assistant Professor, in IT department, M. M.University, Mullana, India. He is also looking after IT infrastructure i.e. data center & university network etc. in the capacity of System Analyst. He has obtained his M. Sc. in Computer Science from Kurukshetra University, India, in 2006. He completed his Masters in Technology in IT Engineering from M.M. University, Mullana, India, in 2010. He is a Cisco Certified Network Associate (CCNA-2011). He is a candidate for Ph. D from Computer Sc. & Engineering Department in M.M University. His Interest lies in Networks, Security and Optimization.

Dr. Vijay Kumar Katiyar born in Kanpur, India, on 30th June 1972. He received his Ph.D degree from M. M. University Mullana, Ambala, Haryana and B.E & M.E. degrees from Kumaon University Nainital (U.P) and NIITR, Chandigarh respectively. He has supervised 25 M. Tech and 1 M. Phil candidates. His research interests are in Wireless Sensor Networks, Reliability Theory and Artificial Neural Networks, etc. He has about 18 years of experience in teaching. He has published about 25 research papers in international journals of repute. Presently he is supervising 8 Ph. D and 8 M. Tech candidates.

Dr. Kamal Kumar received his Ph. D in Wireless Sensor Networks, from Thapar University in 2014. He received his M.Tech. as well as B.Tech degree from Kurukshetra University, Kurukshetra, India. Presently he is working as Assistant Professor (Selection Grade) in Centre for Information Technology (CIT) in University of Petroleum and Energy Studies. He has also served as Associate Professor in Computer Engineering Department in M.M. Engineering College, Ambala, India. His research interest lies in WSNs, Adhoc Networks, MANETs, Security Issues in Wireless Networks and Grid Computing. He has published 18 research papers in SCI Journals, Referred Journals and International Conferences. He has served TPC member of many IEEE sponsored International Conferences. He has served as reviewer in SCI Journals.