IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Survey On Secure Mechanisms For Routing In Mobile Ad Hoc Networks: Trends And Future Directions

[1] Mrs. P. Vidhya Devi, [2] Dr. B. L. Shivakumar,
[1] Assistant Professor, [2] Principal,
[1, 2] Department of Artificial Intelligence & Data Science,
[1, 2] Sri Ramakrishna College of Arts & Science, Coimbatore, Tamilnadu, India.

Abstract – A mobile ad-hoc network (MAN) is a multi-hop wireless network made up of mobile nodes with constrained memory, computing power, and battery life. Because the nodes act as both end devices and routers, MANET routing is different from that in standard broadcasting networks. A few routing protocols have been proposed lately for conceivable organization of Mobile Ad hoc Networks (MANETs) in military, government and business applications. In this paper, survey on these protocols with a specific spotlight on security viewpoints and protocols contrast as far as routing philosophies and the information used to pursue routing choices. Secure ad hoc networks need to meet five security prerequisites: confidentiality, integrity, authentication, non-repudiation and availability. The examinations of the solid versions of the proposed protocols are surveyed about concerning the above security requirements.

Keywords: Mobile Ad hoc network, Routing protocols, Security, Wireless systems, Mobile routing;

I. INTRODUCTION

Mobile Ad Hoc Network (likewise called MANET) MANETs are self-determining, self-maintained, and self-healing, taking into account outer network adaptability. It is a network of mobile routers associated by remote connections - the association of which shapes an impromptu topology. The routers are allowed to move arbitrarily and arrange themselves aimlessly; in this manner, the network's remote topology would change quickly and unsure. This kind of network might work in an independent manner, or would be associated with the bigger Web [2]. Nodes in these networks will both create client and application traffic and do network control and routing protocols. Quickly evolving connectivity, network allocations, most extreme error rates, collision conflicts, and bandwidth and power constraints together posture new issues in network control especially in the plan of more significant level protocols, for example, routing and in executing applications with Nature of Service prerequisites. Mobile applications

present additional challenges for network networks as changes to the network topology are swift and widespread [6]. In a mobile ad hoc network, nodes move readily; thusly the network might encounter quick and flighty topology changes. Since the nodes in a MANET regularly have restricted scope of transmission, a few nodes can't discuss straightforwardly with one another. Thus, routing tracks in mobile ad hoc networks possibly contain various hops, and each hub in mobile ad hoc networks has the obligation to perform like a router. Not at all like gadgets in traditional Remote LAN arrangements, all nodes are mobile and the topology of the network is changing progressively in an Ad Hoc Networks, which carries huge and extraordinary challenges to the security of Ad Hoc Networks [11].

II. TYPES OF ATTACKS

In this research, we concentrate on the MANET routing protocols' security features. via particular for military applications, the security of communication via ad hoc wireless networks is crucial. MANETs are more susceptible to digital/cyber attacks than wired networks because they lack a central coordinating mechanism and a shared wireless channel. These attacks can be divided into two categories: passive attacks and active attacks. Attacks that are passive do not affect a connection's ability to function. An opponent seeks to disrupt a network and read the information being transmitted without altering it. The condition of confidentiality is broken if it's also possible for the adversary to interpret the data that was taken. Passive attacks are challenging to identify since the network continues to function normally when they are active. Encryption is typically employed to defend against these assaults. Active attacks try to disrupt the normal operation of the network or modify or destroy the data of a transmission. External assaults are active attacks that originate from outside networks. Attacks are referred to as internal attacks if nodes from the adhoc network are involved [2,3,12,14].

Here's a table listing some examples of active ad hoc network attacks:

Attack Type	Description
Wormhole Attack	A malicious node creates a virtual link to disrupt routing
Blackhole Attack	A node falsely claims to have the shortest route
Grayhole Attack	A node selectively drops or modifies packets
Sybil Attack	A node creates multiple fake identities to control the network
Flooding Attack	A node floods the network with excessive control messages
Jamming Attack	A node transmits interference signals to disrupt communication
Hello Flood Attack	A node overwhelms the network with frequent hello messages
Resource Exhaustion	A node depletes network resources to render it unusable
Routing Misbehavior	A node deliberately provides incorrect routing information
MAC Spoofing	A node impersonates another node by faking its MAC address

These are just a few examples of active ad hoc network attacks, highlighting the various techniques that attackers may employ to compromise network security and disrupt communication in ad hoc networks. Here's a table listing some examples of passive attacks in Mobile Ad Hoc Networks (MANETs):

Attack Type	Description
Eavesdropping	Passive interception of network communications for information gathering
Traffic Analysis	Analyzing patterns and characteristics of network traffic to gain insights and infer sensitive information
Node Tracking	Monitoring and tracking the movement patterns of nodes in the MANET
Network Monitoring	Passive observation of network activities, topology changes, and routing updates
Rogue Node Detection	Passive identification of unauthorized or malicious nodes in the network
Identity Theft	Passively collecting information to impersonate legitimate nodes in the network
Traffic Correlation	Correlating network traffic to reveal relationships and infer sensitive information
DoS Detection	Passive detection of Denial-of-Service attacks targeting the MANET

III. VARIOUS SECURE MECHANISMS FOR ROUTING IN MANET

1. L. Mao (2008) et.al proposed Towards Provably Secure On-Demand Distance Vector Routing in MANET. Mobile Ad hoc Networks (MANET) is as of now an exceptionally dynamic region of the academic and modern research for its predictable broad applications. Be that as it may, it is powerless against many attacks. Particularly, the routing protocols in MANET bear various types of attacks. Lately, many secure routing protocols have been proposed, among which the protocols based on AODV are more alluring. The security of routing protocols in MANET is normally analyzed by casual means like visual examination and network recreation. There is no conventional meaning of the expression "secure routing" and no numerically thorough method for demonstrating a proposed routing protocol secure. In this way, many "secure" protocols are subsequently found to have flaws. As of late, there have been endeavors to foster conventional means to demonstrate routing protocols secure. In this paper, we analyzed a conventional model, based on the reproduction paradigm, which is custom fitted to the security examination of on-demand distance vector routing protocols in MANET. We showed the ill-advised manipulations, for example, mergence of the adjacent adversarial nodes, the ill-advised meaning of the right system state in the model, and the blemish in the proof for ARAN. An attack to ARAN is introduced, which shows that ARAN isn't provably secure even in their model. So it is extremely perplexing to plan and analyze secure routing protocols in MANET, which needs formal techniques. In our future work, we intend to analyze and think about a few sorts of conventional examination techniques for cryptographic

protocol, and foster programmed devices, e.g., based on model checking, to analyze security of the routing protocols in MANET [1].

2. S. J. Soni (2013) et.al proposed Enhancing security features & performance of AODV protocol under attack for MANET. MANET is a collection of independent mobile clients that impart over moderately bandwidth and power compelled wireless links. These networks are constructed, work and maintained by its own in light of the fact that every node performs double job of host and router. Overall, these nodes have a restricted transmission range thus every node search for the help of its adjoining nodes in sending packets. To lay out routes between two nodes which are away from one another than a solitary bounce, extraordinary routing protocols are already planned. This novel component is dependable to route the message despite dynamic topology of network. The Adhoc On-demand Distance Vector (AODV) routing protocol was at first developed disregarding security in mind. So it can't defend against any sort of security attack. However, there are many security mechanisms accessible that make AODV secure. Nonetheless, by doing more research around here, one significant imperfection in any of the current secure routing protocols was found. That is security mechanisms that are accessible consume seriously handling power and required complex key-management system. Here, we present an original security mechanism that integrates digital signature and hash chain to safeguard the AODV routing protocol that is fit for defending itself against both vindictive and unauthenticated nodes with negligible execution contrast. The proposed security system was additionally recreated in the Network Simulator 2 (NS2) to show minor execution contrast getting through an onslaught [2].

3. S. Lu (2009) et.al proposed SAODV: A MANET Routing Protocol that cans Withstand Black Hole Attack. Ad hoc On-demand Distance Vector routing (AODV) is the plan of AODV, in any case, gave little consideration to security considerations, thus resulting in the weakness of such MANET to the black hole attack. Based on AODV, this paper proposes and executes AODV experiencing black hole attack, in particular BAODV routing protocol. The network performance of MANET utilizing BAODV is extremely more regrettable than utilizing AODV. Based on BAODV, the article likewise proposes and executes a secure routing protocol SAODV; it straightforwardly checks the objective node by utilizing the exchange of irregular numbers. As per the examination and investigation of SAODV's security and productivity in segment 5, SAODV can successfully forestall black hole attack in MANET, and furthermore keep a high routing effectiveness. So SAODV is a secure and effective routing protocol in MANET. Its security is superior to Aodv's, and its routing effectiveness isn't more awful than Aodv's. Despite the fact that SAODV can expand MANET's security, it carries a weight to the network, for example, the source node necessities to capacity got RREP and SRREP in each routing discovery phase, and to do important estimation. The objective node additionally needs to capacity got SRREQ in each routing discovery phase, and to do pertinent computation. The future research ought to all the more likely balance in the wellbeing and effectiveness, to accomplish a safer routing protocol, whose proficiency is better, and simultaneously, the network performance of MANET can likewise be gotten to the next level [3].

4. S. Yadav (2017) et.al proposed Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme. MANET is exceptionally famous and arisen as another field of research to gives the answer for the majority true issues. Ad hoc network gadgets have simple circuit, less cost, little size batteries, little memory and handling power and so on. With expanding its applicability in different fields including military, personal organization, home network, internet of thing, climate monitoring, VANETs, WSNs, emergency alleviation operation like earthquakes and catastrophe help operation, the prerequisite of plans are additionally expanded to make network secure from different attacks. Forcing security in MANET is exceptionally difficult and hotly debated issue of research science most recent two decades in light of its wide applicability in applications like safeguard. Number of endeavors has been made toward this path. In any case, accessible security algorithms, strategies, models and structure may not totally tackle this issue. Roused from different existing security strategies and exception detection, in this paper novel simple however effective anomaly detection plot based security algorithm is proposed to safeguard the Ad hoc on demand distance vector (AODV) receptive routing protocol from Black hole attack in mobile ad hoc climate. Recreation results got from network simulator apparatus clear the effortlessness, power and adequacy of the proposed algorithm over the original AODV protocol and existing techniques [4].

5. V. K. Saurabh (2017) et.al proposed Cluster-based technique for detection and prevention of black-hole attack in MANETs. Secure routing in the field of mobile ad hoc network (MANET) is one of the most thriving areas of research. A MANET involves different mobile nodes which are associated by wireless links and every mobile node acts as a host as well as a router to layout and guarantees a route. Devising a trustworthy security protocol for ad hoc routing is a moving undertaking because of the remarkable network qualities, for example, absence of focal authority, fast node mobility, incessant topology changes, insecure operational climate, and bound accessibility of assets. Because of low configuration and fast deployment, MANETs are appropriate for emergency circumstances like cataclysmic events or military applications. Accordingly, data transfer between two nodes ought to fundamentally include security. A clustering heading in AODV routing protocol for the detection and counteraction of black-hole attack in MANET has been advanced. Each individual from the unit will ping once to the group head, to identify the elite distinction between the number of data packets got and sent by the particular node. Assuming the shortcoming is seen, every one of the nodes will cloud the infectious nodes from the network. The reading of the system performance has been finished regarding packet delivery ratio (PDR), end to end delay (ETD) throughput and Energy reenactment surmisings are recorded utilizing ns2 simulator [5].

6. A. B. Chehida (2013) et.al proposed A Reputation-Based Clustering Mechanism for MANET Routing Security. A Mobile Ad hoc NETwork (MANET) is an assortment of mobile nodes having no decent topology and cooperating with one another. A MANET is constituted of wireless and battery powered mobile nodes forming a brief network. It is by and large utilized in an environment where it is hard to track down or to settle down a network infrastructure. The more significant MANET qualities can be summed up as follow: dynamic topology, absence of central administration, restricted transmission scope of nodes and

absence of infrastructure. Because of these qualities and particularly in light of the fact that every node needs to go about as both host and router, old style routing protocols can't be utilized in such environment. Consequently, a few explicit ones have been proposed for MANET. Because of these particularities, old style routing protocols can't be utilized and a few explicit ones have been proposed. In this paper we propose a clever standing based clustering mechanism to find malicious nodes and segregate them. To diminish network overhead and to manage network geography dynamicity, the proposed instrument depends on a particular grouping environment. The clustering upkeep complexity is as far as concerns it's decreased by the utilization of a standing based delegation process permitting the bunch head to designate its honours to a picked group part in the event of removal or absence of energy. Five modules constitute this mechanism: a monitoring module to recognize malicious nodes, a standing module to refresh notoriety values, an isolation module to dispose of malicious nodes, a character recognition module to survey makes sources and a delegation module aware of give group head rights delegation [6].

7. A. S. Khubalkar (2013) et.al proposed Security enabled DSR for establishing symmetric key and security in MANETS. Nodes participating in the network don't rely on a decent infrastructure, however utilize each other to convey outside their own transmission range. The nodes might join and leave the network at erratic moments. Being mobile, they may likewise move, which additionally results in changes in the network topology. In this manner it suggests that the routing protocol utilized in a MANET should be intended for such an environment. Such networks are extremely helpful in military and other strategic applications, for example, emergency rescue or exploration missions, where static wireless infrastructure is inaccessible or untrustworthy. Business applications are likewise probable where there is a requirement for omnipresent communication services without the present or utilization of a proper network infrastructure. The security has become one of the essential worries as MANETS are being utilized generally. To accomplish security objectives like: authentication, trustworthiness, non-renouncement, privacy, a mystery key is important to be divided among the sender and the collector. Some famous key exchange protocols have a few demerits in the event of MANETs which are because of primarily the prerequisite of high computational capacity. In this paper proposed security improvements to DSR for giving an on-demand secure routing protocol key between the source and the objective during the route creation itself. For the performance assessment, NS2 simulator has been utilized and correlations are made with the essential DSR protocol [7].

8. B. Vaidya (2008) et.al proposed Secure Framework for Integrated Multipath MANET with Internet. With the rising demand of ubiquitous computing, the interconnection of mobile ad hoc networks (MANETs) to Internet is likewise getting alluring, which is supposed hybrid or associated MANET. In the MANET paradigm, routing is a provoking errand because of mobility and the resulting intrinsic dynamic network topology. In many applications, multipath routing plans are wanted as they give different advantages like balancing load, expanding unwavering quality. The current ad hoc routing security plans are not equipped for giving a secure FA discovery, while the current Mobile IP protocol can't give the security insurance to a multihop registration. Subsequently, for giving global connectivity to hybrid

MANET, an integrated plan is required for a secure FA discovery and a secure Mobile IP registration for mobile node. With the rising demand of ubiquitous computing, the interconnection of mobile ad hoc networks (MANETs) to Internet is likewise getting alluring, which is purported hybrid or associated MANET. In MANET paradigm, routing is a moving errand because of mobility and the resulting intrinsic dynamic network topology. In many applications, multipath routing plan is great than single-way routing because of many advantages. Security issues in hybrid MANET, nonetheless, is as yet testing task. There are two essential issues for giving a secure multihop route discovery: Web connectivity and ad hoc routing. They give security investigation by utilizing Boycott Rationale [8].

9. S. Vinay et.al proposed Multipath Source Routing Protocol for Mobile Adhoc Networks with Performance Effective Analysis. MANET is a developing innovation and Nodes on the MANET's are associated wirelessly. There are two sorts of Wireless Networks. Wireless Adhoc Network (WANET) is an appealing innovation that will determine many applications on new innovation. Manet has the rule of infrastructure and infrastructure less, where static as well as dynamic networks are alluring, there are not much significant restriction's that shield business elasticity. With this venture, we concentrate on minimizing the complete energy consumption and lessening network lifetime of absolute 1-Dimensional queue network where nodes are coordinated and unaltered. As of this result, we take the information from sender Routing algorithm to pack the network complete energy proficiency by taking in consider with the distinctions as a part of every one of the Moderate nodes through their distance to send as well as interface one another and leftover energy of one another. We Carry out Dynamic source routing hypothesis to essentially understand the node when genuine nodes are predetermined which can't be put to the source concerning the ideal transfer distance among sender and recipient. Subsequently the ideal objective is to project a low energy productive dynamic source routing plan that ensures minimum power for minimal price and keeps the sender or beneficiary in comparative with lower occupant energy. A few reproduction results show that the found result makes significant developments in wording low energy consumption as well as saving and network dividend is contrasted and the other existing routing algorithms [9].

10. S. B. Sharma (2015) et.al proposed Security issues and their solutions in MANET. A mobile ad hoc network is a dynamic network of mobile hosts that has no centralized administration system. Nodes in this network are self-arranging that speaks with different nodes that are inside the extent of that node as it were. Securing MANET is more troublesome as channel is available to real client and malicious attacker too. Nodes are free move arbitrarily because of which the network topology changes every now and again and thusly the trust among the nodes makes complexity of routing of data. To acquire satisfactory degree of security secure variants of proposed bound together security routing protocols are presented. A mobile ad hoc network is a dynamic network of mobile hosts that has no centralized administration structure. Nodes in this network are self getting sorted out that speaks with different nodes that are inside the extent of that node as it were. Securing MANET is more troublesome as channel is available to authentic client and malicious attacker too. Nodes are allowed to move arbitrarily because of which the network topology changes habitually and thusly the trust among the nodes makes complexity of routing of data. To acquire

adequate degree of security secure renditions of proposed bound together security routing protocols are presented. This report makes sense of different security issues in MANET and makes sense of not many security protocols for safeguarding the environment from malicious nodes. Secure routing protocols for MANETs are typically determined as expansions of existing routing protocols. Security techniques and protocols are grouped under 3 segments: Cryptographic techniques, Trust based techniques, and Positioning techniques [10].

11. A. A. Junnarkar (2018) et.al proposed SQMAA: Security, QoS and Mobility Aware ACO Based Opportunistic Routing Protocol for MANET. In ongoing past, the wireless sensor networks are likewise planned by involving the mobility attributes of MANET in many applications. Since from last decade, there is significant improvement in Manet's deployment and its center part of everyday communications particularly the applications like biological, military applications. The QoS execution of MANET routing protocols is altogether affected by the portability conditions in network. In this research work, we are planning the clever pioneering routing protocol to address the challenges of network security as well as QoS improvement. There two algorithms planned in this paper. First proposed Ant Colony Optimization (ACO) with swarm knowledge approach utilized the RSSI estimations to determine the distance between two mobile nodes to choose effective way for communication. This new routing protocol is named as QoS Mobility Aware ACO (QMAA) Routing Protocol and the QoS mindfully protocol is proposed named as Secure-QMAA (SQMAA). The SQMAA accomplished secure communications while guaranteed QoS performance against existing routing protocols [11].

12. A. Bhardwaj (2014) et.al proposed secure routing in DSR to mitigate black hole attack. A mobile adhoc network contains number of mobile nodes, which assumes an important part in routing. Mobile nodes which are in same radio communication range conveying straightforwardly in any case requires cooperation of different nodes and perform multi-bounce communication. In multi-bounce communication, nodes convey without infrastructure and give connectivity by sending packet to neighbor. For this connectivity node utilizes routing protocol. Network topology in MANET change as often as possible and changes are dispersed among nodes. Nodes might join or leave network and are expected to work with collaboration because of absence of central control in network operation. Mobile adhoc networks (MANETs) comprise of mobile nodes with no decent infrastructure. Dynamic Source Routing (DSR) which is on-demand routing protocol is a generally acknowledged mobile adhoc network routing protocol used to give connectivity to mobile nodes. Nonetheless, DSR and other ondemand routing protocols are powerless against various kinds of security attacks and black hole attack is one of them. In black hole attack, malicious node sends a phony route answer as needs be of route solicitation to source node claiming for an optimal route to the goal. Malicious node drops the information packet which lessens packet delivery ratio. To secure DSR, we propose an arrangement which insists the genuineness of route with the help of confirmation packet. This packet is generated by first moderate jump in the route of route answer. Reproduction results show improvement in packet delivery ratio and throughput [12].

13. J. Zhou (2007) et.al proposed SRSN: Secure Routing Based on Sequence Number for MANETs. A mobile ad hoc network (MANET) is an assortment of mobile nodes that are equipped for speaking with one another through wireless connection. Nodes serve as a client or server, yet additionally a router, they communicate data packet by cooperation with different nodes. Be that as it may, because of a few fundamental characteristics, ad hoc network is particularly defenceless against attackers, and routing assumes an important part in the security of whole ad hoc network and isn't minor to tackle. Security of Mobile Ad Hoc Network (MANET) is vital when we deploy MANET as a general rule. This paper proposed one more method SRSN (Secure Routing in light of Arrangement Number) succession number of RREQ packet got together with strong start to finish acknowledgment to perceive misleading route information. SRSN makes a little variant of DSR convention and can safeguard against dark opening assault without growing a lot of utilization of resource and payload. Reproduction results show that SRSN actually can keep up with high packet delivery ratio while there is black hole attack malicious node in network [13].

14. P. Sharma (2014) et.al proposed Enhanced security scheme against Jamming attack in Mobile Ad hoc Network. In mobile ad hoc network security is one of the significant issues in the event of routing. Secure communication is vital for the delivery of genuine information to the beneficiary. In this paper different sort of attacks and their mischief is noticed and we have likewise examined about some plan against various attacks. Jamming attack security plans is fundamental concentration in this research. In this review, we have utilized the AOMDV routing protocol. In this paper, we attempt to determine the impact of jamming attack in the network. Finding the attacker nodes with connection situated protocols could be different work concerning a future report. In our future extent of work, we would hold this methodology in maximizing the performance of a network from jamming attack as far as flooding packets in network when the link are clogged. We have reproduced attack in the ad-hoc networks and track down its belongings. The attacker degrades the general performance of network and gives the untrustworthy routing. The attacker is distinguished and number of unapproved packets conveyed is likewise determined to recognize the number of nodes that degrade the network performance. The re-enactment results like routing load and PDR (Packet Delivery Ratio) of network and every node that gets the data and conveys the data shows that the security conspire has similarly further developed the network performance within the sight of attacker. We have established the environment of multiple attackers and proposed an enhanced security plan to recognize and hinder the attacker in network [14].

15. S. Kumar (2016) et.al proposed a modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol. An Ad-Hoc is a sort of short durational network that doesn't have any managing authority which can make a lot of nodes that can speak with each other with in a proper scope of transmission and it is infrastructure independent. MANET is a less infrastructure network with energetically changing geographies and inconsistent imparting node. As of now the mobile nodes discuss straightforwardly with additional nodes with next to no router and subsequently the favoured functionalities are installed to every node. Since the MANET comprises of mobile nodes with

less configurations of equipment and prerequisites contrasted with a router, consequently protocols and routing utilized are of lightweight functionalities. Each Mobile node is competent for naturally arrange network and making of link with neighbor node for foundation of communication. Routing protocols are utilized to find appropriate route from source to objective and offer help for foundation of communication. AODV routing protocol is a responsive protocol used to identify route according to demand. The total review notice the AODV is great answer for communication in wireless environment yet helpless for different security dangers. Security dangers not just endeavor to compromise the privacy of communication yet additionally degrade the network performance. The total review presumes that gray-hole attack is one of the serious security dangers and it is mandatorily stayed away from the network. Reproduction of proposed arrangement sees that counteraction technique recognize malicious node as well as help to forestall it. Performance perception presumes that proposed technique perform better then, at that point, gray-hole attack in the event of 30 and 40 node scenarios [15].

IV. COMPARISON TABLE

Author's Name	Methodology	Main Merits	Main Demerits	Contributions to MANET Security
L. Mao (2008) et.al	Based on a simulation paradigm	- Conventional model tailored for security analysis of routing protocols in MANETs.	- Complex to design and analyze secure routing protocols in MANETs.	Providing a conventional model for analyzing the security of routing protocols in MANETs
S. J. Soni (2013) et.al	Digital signature and hash chain integration	- Less power consumption in securing AODV routing protocol against malicious and unauthenticated nodes.	- Issues related to sequence numbers in control packets and routing loops.	Introducing a security mechanism that integrates digital signature and hash chain for enhanced security in AODV routing protocol
S. Lu (2009) et.al	Check destination node using random numbers	- SAODV is a secure and efficient routing protocol in MANETs.	- Need for better balance between security and efficiency.	Proposing SAODV, a secure routing protocol that effectively prevents black hole attacks while maintaining routing efficiency

S. Yadav (2017) et.al	Anomaly detection scheme	- Proposed outlier detection scheme significantly deals with black hole attacks.	- Need for a security scheme that is fast in limited resource networks.	Introducing a novel outlier detection scheme to secure the AODV routing protocol against black hole attacks
V. K. Saurabh (2017) et.al	Cluster-based approach	- The proposed cluster-based technique shows improved results in detecting and preventing black hole attacks.	- Selection of route based on high objective hop count difference.	Introducing a cluster-based technique for the detection and prevention of black hole attacks in MANETs
Chehida et.al, 2013	- Reputation-based clustering mechanism	- Identification and isolation of malicious nodes in MANETs	- Significant issues for routing interaction and vulnerability to malicious behaviors	- Introduces a reputation-based clustering mechanism to enhance MANET routing security
Khubalkar et.al, 2013	- Security enhancements to DSR routing protocol	- Provides secure key exchange and routing in MANETs	- May implement simultaneous utilization of multiple paths (multicasting) for load sharing	- Proposes security improvements to DSR routing protocol for secure key exchange and routing in MANETs
Vaidya et.al, 2008	- Integrated secure plan for hybrid MANETs	- Robust security against attacks in Internet connection and ad hoc routing	- Conducts simulations to evaluate the performance of the proposed protocol using OPNET Modeller	- Presents a secure framework for the integration of hybrid MANETs with the Internet, addressing security in both Internet connection and ad hoc routing
Vinay et.al, 2010	- Low-energy efficient dynamic source routing protocol	- Minimizes energy consumption and network lifetime in MANETs	- There is no way to transfer packets towards the recipient end	- Introduces a low-energy efficient dynamic source routing protocol for energy optimization in MANETs

Sharma et.al, 2015	- Various security techniques and protocols	- Node authentication, data integrity, and resistance to insider attacks	- Challenging to design a secure protocol providing protection from all types of attacks	- Explores security issues in MANETs and presents security protocols for safeguarding the environment from malicious nodes
Junnarkar et.al, 2018	- Ant Colony Optimization (ACO) with swarm knowledge approach	- Improved QoS and data security against malicious attackers in the network	- Open nature of communication in MANETs poses a security challenge	- Proposes SQMAA protocol that addresses network security and QoS improvement in MANETs
Bhardwaj et.al, 2014	- Verification packet generation in the route answer	- Utilizes unbridled mode, no need for additional database and processing power	- Plain packet for confirmation of malicious node, lacking adequate security features	- Introduces a solution to mitigate black hole attacks in DSR routing protocol through verification packets
Zhou et.al, 2007	- SRSN protocol based on sequence numbers and RREQ packets	- Identifies fake RREQ packets from malicious nodes, defends against black hole attack	- High data delay at the start of the network	- Proposes the SRSN protocol tha uses sequence numbers and end-to-end acknowledgment to comba black hole attacks
Sharma et.al, 2014	- AOMDV routing protocol used	- Improved network performance in the presence of attackers	- Approach focused on maximizing network performance against jamming attack, rather than addressing other security threats	- Presents an enhanced security scheme specifically targeting jamming attacks in AOMDV routing protocol
Kumar et.al, 2016	- Modified approach using AODV routing protocol	- Identification and prevention of gray-hole attacks	- Complexity in detecting partial dropping attacks, potential confusion with malicious nodes	- Proposes a modified approach to detect and eliminate gray-hole attacks in MANETs using the AODV routing protocol

In this paper we discussed secure routing in MANET; in this context have proposed different methodologies and mechanisms to enhance the security of routing in MANETs. These protocols focus on various aspects such as reputation-based clustering, symmetric key establishment, and integration with the Internet, multipath routing, and performance optimization. They have proposed various techniques, such as reputation-based clustering, ACO-based opportunistic routing, sequence number-based routing, and enhanced security schemes. These protocols have shown improvements in packet delivery ratio, throughput, QoS, and data security while mitigating attacks and preserving network performance. The merits of these secure routing protocols include improved packet delivery ratio, throughput, network performance, and protection against malicious activities. They introduce innovative approaches, such as reputation-based clustering, security enhancements to routing protocols, and low-energy efficient routing mechanisms, to mitigate security risks and enhance the overall security of MANETs. However, there are certain demerits associated with these protocols as well. Some of the challenges include the open nature of communication in MANETs, complexity in detecting and preventing attacks, potential delays or disruptions in network operations, and the need for further performance evaluations and simulations.

V. CONCLUSION

In this paper we surveyed different MANET moves toward sort of security based reactive, proactive and hybrid ad hoc routing protocols. The protected versions of every one of the proposed protocols have additionally been surveyed. Traditionally, a solid ad hoc network needs to meet different security necessities, Confidentiality, Integrity, Availability, Authentication and non-repudiation. The proposed secure routing protocols offer advancements in terms of authentication, integrity, confidentiality, and resistance to various attacks. They pave the way for more secure and reliable communication in MANETs, making them suitable for critical applications such as military operations, emergency rescue missions, and ubiquitous computing. Further research and development in secure routing protocols for MANETs are essential to tackle evolving security threats and to ensure the privacy and integrity of data transmission. The continuous improvement of secure routing protocols will contribute to the wider adoption and deployment of MANETs in diverse domains, enabling efficient and secure communication in dynamic and infrastructure-less environments.

REFERENCES

1. L. Mao and J. Ma, "Towards Provably Secure On-Demand Distance Vector Routing in MANET," 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 2008, pp. 417-420, doi: 10.1109/CIS.2008.61.
2. S. J. Soni and S. D. Nayak, "Enhancing security features & performance of AODV protocol under attack for MANET," 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), Vallabh Vidyanagar, India, 2013, pp. 325-328, doi: 10.1109/ISSP.2013.6526928.
3. S. Lu, L. Li, K. -Y. Lam and L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," 2009 International Conference on Computational Intelligence and Security, Beijing, China, 2009, pp. 421-425, doi: 10.1109/CIS.2009.244.
4. S. Yadav, M. C. Trivedi, V. K. Singh and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme," 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), Mathura, India, 2017, pp. 1-4, doi: 10.1109/UPCON.2017.8251012.
5. V. K. Saurabh, R. Sharma, R. Itare and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2017, pp. 489-494, doi: 10.1109/ICECA.2017.8212712.
6. A. B. Chehida, R. Abassi and S. G. El Fatmi, "A Reputation-Based Clustering Mechanism for MANET Routing Security," 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany, 2013, pp. 310-315, doi: 10.1109/ARES.2013.42.
7. A. S. Khubalkar and L. R. Ragha, "Security enabled DSR for establishing symmetric key and security in MANETS," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, India, 2013, pp. 1-5, doi: 10.1109/WOCN.2013.6616208.
8. B. Vaidya, J. -Y. Pyun, S. Pan and N. -Y. Ko, "Secure Framework for Integrated Multipath MANET with Internet," 2008 International Symposium on Applications and the Internet, Turku, Finland, 2008, pp. 83-88, doi: 10.1109/SAINT.2008.111.
9. S. Vinay, S. B. Honnalli and G. Varaprasad, "Multipath Source Routing Protocol for Mobile Adhoc Networks with Performance Effective Analysis," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 41-44, doi: 10.1109/ICICCT.2018.8473258.
10. S. B. Sharma and N. Chauhan, "Security issues and their solutions in MANET," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 289-294, doi: 10.1109/ABLAZE.2015.7155013.
11. A. A. Junnarkar, Y. P. Singh and V. S. Deshpande, "SQMAA: Security, QoS and Mobility Aware ACO Based Opportunistic Routing Protocol for MANET," 2018 4th International Conference for

Convergence in Technology (I2CT), Mangalore, India, 2018, pp. 1-6, doi: 10.1109/I2CT42659.2018.9058022.

12. A. Bhardwaj, "Secure routing in DSR to mitigate black hole attack," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, India, 2014, pp. 985-989, doi: 10.1109/ICCICCT.2014.6993102.
13. J. Zhou, J. Chen and H. Hu, "SRSN: Secure Routing Based on Sequence Number for MANETs," 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 2007, pp. 1569-1572, doi: 10.1109/WICOM.2007.395.
14. P. Sharma and A. Suryawanshi, "Enhanced security scheme against Jamming attack in Mobile Ad hoc Network," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-5, doi: 10.1109/ICAETR.2014.7012891.
15. S. Kumar and N. V. Doohan, "A modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 2016, pp. 1-5, doi: 10.1109/CDAN.2016.7570922.