Survey on MANET Routing Protocols for Secure Data Transmission

A.Kavitha[1], Dr.V.S.Meenakshi[2]

[1]Research Scholar, Chikkanna Government Arts College, Bharathiar University, Tamil Nadu, (India)
[2]Research Supervisor, PG and Research Department of Computer Science, Chikkanna Government Arts College, Bharathiar University, Tamil Nadu, (India)

ABSTRACT

MANET is a Ad Hoc network in which a large number of nodes are connected wirelessly. It is used in different areas like military, disaster recovery etc. The nodes present in this network are openness and decentralized. MANET is frequently changing its topologies to transfer the data quickly, because nodes in this network are moving always (mobility) and data transfer has been done by finding the efficient routing path between source and destination. Due to the mobility there is a lot of chance to involve malicious node and the network will become more vulnerable to attacks like gray hole and black hole attack etc. These types of attacks affect the MANET routing path and it hence it is necessary to secure routing. To overcome the security problem, single or multilayer security algorithm is needed to link with protocol. In this paper, a survey is made of various kinds of existing protocols and algorithms involved are discussed.

Keywords*: *MANET, Routing Protocol, Security Attacks, Authentication.

I. INTRODUCTION

Over the past few years Wireless ad-hoc network become most important field due to the popularity of mobile devices and wireless network. A MANET can be operated as standalone fashion or connected to internet or external network. Fig.1 shows the structure of MANET.

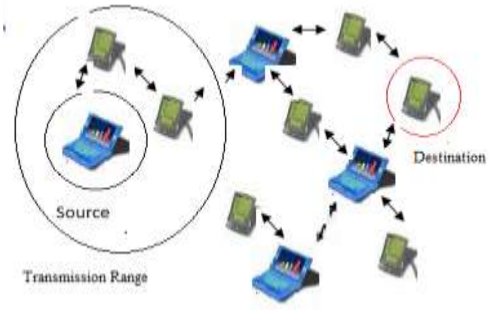

Fig.1 Structure of MANET

The nodes in MANET act as both router and as a host. The mobile nodes are free to move randomly and network topology changes frequently. Wireless network is divided into 2 parts as infrastructure network and ad-hoc networks.

i. Infrastructure network

An infrastructure network act as a bridge which was connected in the form of wired network and wireless network. The base stations are fixed and the mobile network move during communication. If any node goes out of range from any base station, it goes into the range of other base station. Fig.2 shows infrastructure network

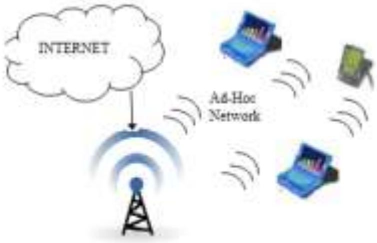

Fig.2 Infrastructure Network

ii. Ad-hoc Networks (Infrastructureless)

No fixed base station and mobile nodes can move while communicating. All the nodes present in this network act as routers. Infrastructureless network also called Ad-hoc network which forms temporary networks. In this type of network nodes are portable devices such as mobile phones and laptops. Fig. 3 shows an ad-hoc network

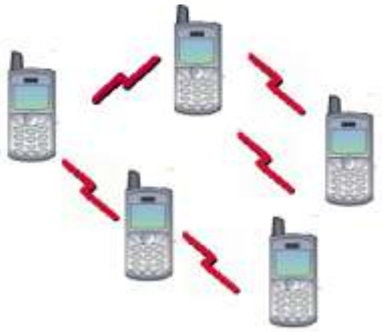

Fig.3 Infrastructureless Networks

MANET is divided into two different types.

- ✓ Single hope network
- ✓ Multi-hope network

Single Hop Network

In single hop network all nodes are in a same radio range that directly send and receive message from one another.

Multi Hop Network

In multi hop network if the desired node is far away from its radio range, so message communication between the nodes can be done through the intermediate node. But in intermediate or neighbouring nodes may occur several security problems such as, it extracts useful information packets, cannot forward packets to the next node or may modify the contents of packets during the data transmission session over the network. These type of nodes are known as misbehaviour nodes or misbehaving nodes.

User authentication and preventing unauthorized users from accessing resources are difficult in MANET. Due to these reasons MANET is particularly vulnerable to various types of attacks such as inside attack, outside attack, active and passive attacks.

Applications

MANET was used for mainly for Military application but in now a day's mostly new usage likes search and rescue mission, information collection, and virtual classes. It is mostly used in several areas for secure data transmission. Some of the typical applications are,

i. Technical Networks :

To communicate between soldiers and automated battlefields

ii. Emergency Services

Search and rescue operations

Disaster recovery- earthquakes, Hurricanes

iii. Educational

Virtual classrooms or conference rooms and Set up ad-hoc communication during conferences, meeting or lectures

iv. Home and Entertainment

Home/Office wireless networking

Personal Area network

Outdoor internet access

II. CLASSIFICATION OF MANET ROUTING PROTOCOLS

Routing is the process of transmitting information or packets from source node to destination node. As Ad-Hoc network changes its topology very frequently and thus making packet routing difficult. Routing protocol has significant role in MANET. It controls the flow of data in networks and also decides the efficient path to reach the destination. Routing protocols are the key to MANET success. The routing protocols can be classified based on routing strategy and network structure. Routing protocols can be categorized as:

- ✓ Table -driven or proactive routing protocol
- ✓ On-demand or reactive routing protocol
- ✓ Hybrid routing protocol.

The classifications of these three protocols are shown in Fig.4

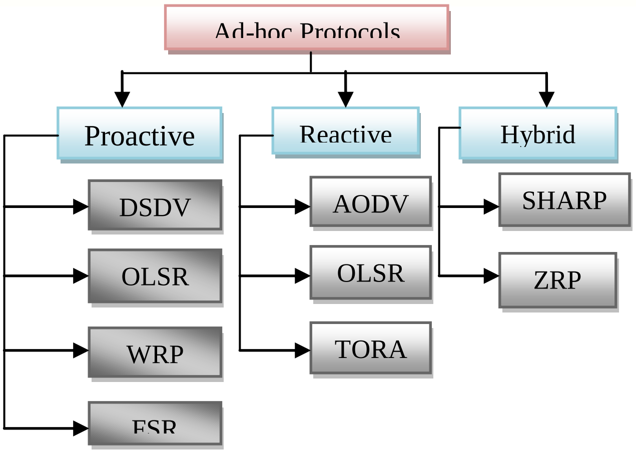

Fig.4 Classification of MANET routing protocols

i. Proactive Routing Protocols (Table Driven)

These protocols update the routing table within certain time. e.g. Destination Sequenced Distance Vector Routing (DSDV), Optimized Link State Routing (OLSR), Cluster-based Gateway Switch Routing (CGSR),Wireless Routing Protocol(WRP), etc.

a. Destination Sequenced Distance Vector Routing (DSDV)

DSDV is a proactive routing protocol based on Bellman-Ford algorithm which evaluates the minimum number of nodes to reach the destination. It is derived from routing information protocol (RIP) and adds new attribute sequence number. Each node maintains a routing table which stores next hop and a sequence number that is create by destination itself. In this protocol routing table updates are transmitted periodically.

b. Optimized Link State Routing (OLSR)

OLSR is a table driven protocol and an optimization of classical link state protocol. In OLSR each node selects a set of Multipoint Relays (MPR) from the set of neighbors with which it has symmetrical links for that it requires bidirectional links. Each node has the knowledge as to for which node it acts as a MPR as they periodically announce this information in their control messages. Therefore overhead minimizes as only MPR retransmit the control messages. In OLSR, MPR nodes declare link state information in the network for the nodes to which it acts as a MPR used to provide the shortest route path to all the destinations. MPR nodes are also responsible for formation of routes from source to the destination.

c. Wireless Routing Protocol (WRP)

Each node maintains four tables i.e. distance table, routing table, link-cost table and, message retransmission list for the purpose of routing. In WRP, only update messages are propagated to the neighbors of a node.

ii. Reactive Routing Protocols (On-Demand)

These protocols do not periodically update the routing table. It generates the routing table whenever the needs to transmit data. It is a high security protocol. This protocol finds the efficient route through route request. e.g. Ad-hoc On-demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), and Temporally Ordered Routing Algorithm (TORA).

a. Ad-hoc On-demand Distance Vector Routing (AODV)

AODV routing protocol works purely on demand basis. When a source node needs to communicate with another node, it starts route discovery process by broadcasting a route request message to its neighbor including the last known sequence number for that destination. Each node that forwards the route request also creates a reverse route for itself back to the source node.

b. Dynamic Source Routing (DSR)

Dynamic Source Routing protocol (DSR) is designed for multi-hop wireless ad hoc networks. DSR is a type of reactive routing protocols. This protocol consists of two main mechanisms "Route Discovery" and "Route Maintenance". In this source node initiate route discovery and floods Route Request (RREQ) in the network. The route request uses a sequence number and path it traversed. The sequence number is used to identify the request and it is used to avoid looping. Route discovery is used to discover the routes from source node to destination.

c. Temporally Ordered Routing Algorithm (TORA)

TORA uses a parameter height for each node which is a measure of the distance in hops from node to the destination node. The source node uses the height parameter to select the best route toward the destination. It is a loop-free multipath routing to destinations minimizing communication overhead.

iii. Hybrid Routing Protocol (Reactive / Proactive)

These are combination of both Proactive and Reactive Protocols. e.g. Zone Routing Protocol (ZRP) etc.

a. Sharp Hybrid Adaptive Routing Protocol (SHARP)

SHARP automatically finds the balance point between proactive and reactive routing by adjusting the degree to which route information is propagated proactively versus the degree to which it needs to be discovered reactively.

b. Zone Routing Protocol (ZRP)

Each node has a predefined zone centred at itself including other nodes whose distance is in predefined limits in terms of number of hops. Route Discovery is done to communicate with nodes not present in the zone of a node by forwarding query messages selectively only to the nodes in its zone rather than all the nodes in a network.

III. CHALLENGES OF MOBILE AD-HOC NETWORKS

This section describes the various research challenges. The following issues are inadequate in MANET environment.

Security

Security is a essential requirement in mobile adhoc network. It is a big challenge due to the reason of no centralized authority to supervise. There are many types of attacks which can collapse the security of MANET. These attacks can be performed on various layers of the network. The following table1 shows the attacks on MANET at layer wise.

Table 1: Classification of attacks at layer wise in MANET

Layers	Attacks
Application	Malicious code attacks (Viruses, worms), Data Corruption.
Transport	Session Hijacking
Network	Black hole, Warm hole, Sinkhole, Grey hole, Flooding, Sybil attacks.
Data Link	Selfish Misbehaviour of Nodes, Malicious Behaviour of nodes, Denial of Service (DoS), Misdirecting traffic.
Physical	Eaves Dropping, Jamming, Active Interference.

Quality of Service

The dynamic changes of topology in ad-hoc network leads to QOS problem.

Routing Overhead

The wireless ad-hoc networks nodes often change their location within network. There are some stale routes generated in the routing table which leads to the unnecessary routing overhead.

Power Consumption

For most of the light-weight mobile terminals, the communication-related functions should be optimized for low power consumption. Conservation of power and power-aware routing must be taken into consideration.

Packet losses due to transmission errors

Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions, presence of interference, uni-directional links and frequent path breaks due to mobility of nodes.

IV. LITERATURE REVIEW

Jie Liu et al [1] proposed intrusion detection and continuous authentication system using hidden Markov model scheduling algorithms to provide high security for mobile ad-hoc network.

R. Rizwan et al [2] introduced a intelligent secure routing model for MANET. This system is mainly developed to detect the type of attack and chooses the optimum routing protocol according to the network attack.

Shengrong Bu et al [3] developed a multimodal biometric authentication with data fusion for continuous user authentication. In their work two sensors are used for authentication and Dempster–Shafer theory is used for data fusion. The system decides which biosensors should be chosen, depending on the security problem.

Hiteishi Diwanji and J.S. Shah [4] designed an unimodal(fingerprint) based biometric encryption key to achieve authentication in MANET. The author created a 48 bit size key using DES algorithm which provides high secure routing.

B.Thanikaivel, B. Pranisa [5] has proposed fast and secure transmit protocol for fast routing using proactive and reactive mechanism. The central agent and process algorithm is used for detecting malicious node.

Vijaya Bhaskar.Ch, Dr. D.S. R. Murthy [6] designed a genetic based routing approach for reliable routing in MANET. The proposed system has been generating an optimized routing path which improves the data delivery over the network and quality of service.

Menaka Pushpa, Dr. K. Kathiravan [7] proposed multicast activity based technique to identify the attacker node in the multicast group and also analyzed the vulnerabilities of PUMA (Protocol for Unified Multicasting through Announcements) and MAODV (Multicast Ad-hoc On-demand Distance Vector routing) in MANET. This technique is well efficient to detect packet drop attacker with false negative alarm rate.

Elakkiya.M, Dr.Edna Elizabeth.N [8] introduced an opportunistic routing technique to detect flooding attack in MANET. Trust value is calculated for every node for secure routing.

D.Saravanan, T.Sangeetha [9] has used genetic algorithm to enhance the network performance and provides efficient routing to the network. It reduces the routing overhead such as time delay, packet loss.

Neha Agarwal, Neeraj Manglani [10] has presented a new approach using genetic algorithm for energy efficient routing in mobile ad hoc network. This algorithm provides the best path to transfer data when one path fails. The author compared Proposed GA based routing and traditional flooding based routing.

Sherin Zafar et al [11] suggest optimized genetic stowed biometric approach to overcome the QoS based issues in MANET. The proposed technique is developed with the help of iris biometric and genetic algorithm.

Remya S, Lakshmi K S [12] developed Secured Hierarchical Anonymous Routing Protocol (SHARP) using cluster routing. This system overcomes the anonymity problem between source and destination. This protocol achieves better anonymity protection compared to other anonymous routing protocols.

Ashish Sharma et al [13] used hybrid cryptography technique (DES, RSA) to transfer data with high security in MANET. The authors also presented a comparison of SAODV and AODV routing protocol with different parameters like energy, packet delivery ratio and throughput.

Raj Kamal Kapur, Sunil Kumar Khatri [14] proposed a technique using symmetric and asymmetric cryptography which provides secure transmission of data over a critical requirement of MANET routing. The proposed technique has been simulated using AES algorithm for symmetric crytography, RSA algorithm for asymmetric cryptography and MD5 for Hash algorithm.

Deore Suvarna et al [15] constructed an Enhanced Adaptive Acknowledgement (EAACK) technique for secure data transmission in MANET. The focus of this system is to overcome the problem of misleading misbehaviour, finite transmission power and receiver collision. Cluster algorithm and digital signature are used for secure acknowledgement.

Anjali Anand et al [16] proposed a Distributed Dynamic Model to ensure secure and reliable Routing in Mobile Ad hoc Networks against misbehaving nodes. The performance of the proposed has been evaluated in terms of Packet success ratio, Routing overhead and Throughput. This system compared with existing technique such as LMRSA, LARS, OCEAN, and traditional DSR protocol.

Archana P. Mandhare, Sujata V. Kadam [17] Established Trust Worthy Reliable Path in MANET with the help of SRP (Secure and Reliable) routing protocol which established secure and reliable route for data transmission.

Priyanka Patil et al [18] designed and evaluated ALERT protocol to prevent the anonymity of the MANET. SHA-1 algorithm has been designed to prevent MITM and Dos attacks. Nachammai. M, Dr . N. Radha [19] proposed cooperative bait detection scheme (CBDS) for secure transmission after detecting the malicious node. It identified black hole and gray hole attack. RC$ and MD5 algorithms are used for encryption process.

Garima Jain, Dr.Gajendra singh Rajawat [20] proposed an improved version of AODV with the help of homographic encryption scheme which prevents pollution attack in MANET.

Rasika R. Mali, Sudhir T. Bagade, [21] proposed Secure Acknowledgement (ACK) System for detecting the misbehaving node in MANET. ACK is a truly an acknowledgement based technique.

A.Maheswary, Dr.S.Baskar [22] introduced Letter Shape based algorithm for encrypting the transfer data over network. This technique has been compared with DES, AES and RSA which proves the proposed technique took less time to encrypt the data. It also prevents man in the middle attack.

V.Sesha Bhargavi, S.Viswanadha Raju [23] proposed a trust based secure routing system in MANET to achieve better performance in terms of the packet delivery ratio and throughput. Banoth Rajkumar, Dr.G.Narsimha [24] has presented a Trust based threshold revocation method for enhancing the security of routing in MANET. This is achieved by calculating trust values and distributing secret key to all the nodes. The advantage of this system is misbehaving nodes are eliminated.

S.Harihara Gopalan, Dr.R.Radha Krishnan [25] proposed three methods trust aware model and fuzzy aided and Ant Colony Optimization (ACO) algorithm to find optimal routing for high security.

Suveg Moudgil, Dr. Sanjeev Rana [26] identified three kinds of Dos attack (Spoofing attack, Route flooding and HELLO flooding) on OLSR routing protocol. The main objective of this system is isolate these flooding and spoofing attacks and increases the overall network performance.

Rohit Chourasia, Rajesh Kumar Boghey [27] developed a novel intrusion detection system which identify the misbehaviour of packet dropping and also choose alternate path to transfer data. The performance of the proposed system is calculated in terms of Packet delivery ratio, routing overhead, throughput and average delay.

Sherin Zafar [28] introduced a novel biometric signature based approach to enhance the security of network in MANET. This approach has been implemented in MATLAB. The performance factors of the proposed system are compared with similar previous approach for validating the effectiveness of this approach

P.Sathya et al [29] designed effective multicast routing algorithm for selecting the route with minimum energy in MANET which was compared with existing protocol. The performance of this system has been evaluated in terms of in terms of throughput, delay, PDR and network lifetime.

Dr.B.Rosiline Jeetha, K.Sivakamipriya [30] developed zone based routing protocol for secure routing in MANET. The proposed BAT algorithm solved the cluster issues.

The essence of the existing protocols and technique are shown in table 2.

Table 2: Existing Protocol and its Features

AUTHOR	PROTOCOL& TECHNIQUE USED	TYPES OF ATTACKS ADDRESSED	HIGHLIGHTS
Jie Liu, F. Richard Yu, Chung-Horng Lung, Helen Tang, 2009	Iris Markov Model	DoS Attacks	High Security
Rizwan R. Rangara et al, 2010	Intelligent Secure Routing Protocol ADS	Black hole Attack, Replay, DoS	Find optimum routing
Shengrong Buet al, 2011	Iris sensor, and fingerprint sensor Dempster–Shafer theory	Monitoring network behaviour	Improve network security
Hiteishi Diwanji and J.S. Shah, 2011	Fingerprint DES	Brute Force Attack	Generated 48 bit encryption key FAR is Zero
Deny.J, Sivasankari.N, 2012	Dempster–Shafer theory Voice biometric	Intrusion	Detecting security state
B.Thanikaivel, B. Pranisa, 2012	OLSR protocol Central agent and process algorithm	Malicious Node	Packet size reduced
Vijaya Bhaskar.Ch, Dr. D.S. R. Murthy, 2013	Genetic Algorithm	QoS	Improve the data delivery over the network
A. Menaka Pushpa, Dr. K. Kathiravan, 2013	Multicast Ad-hoc On-demand Distance Vector routing (MAODV) PUMA	Internal Attack	High Packet delivery ratio
Elakkiya.M, Dr.Edna Elizabeth.N, 2014	Opportunistic routing technique Trust Management System	Selfish Nodes; Malicious Node, flooding attack	Increase the overall network Performance.
D.Saravanan, T.Sangeetha, 2014	Face Routing Protocol Genetic Algorithm	Optimization problem, flooding	Reduces the routing overhead such as

			time delay, packet loss
Neha Agarwal, Neeraj Manglani, 2015	Energy efficient routing protocol Genetic algorithms	Path fails	Increases the overall lifetime of the network
SherinZafar, M.K.Soni, M.M.S Beg, 2015	Ad-hoc On-demand Distance Vector Routing (AODV) Genetic algorithms Iris	QoS based attacks	Accuracy=0.98889
Remya S, Lakshmi K S, 2015	Secured Hierarchical Anonymous Routing Protocol (SHARP) RSA	Anonymity	High Security
Ashish Sharma, Dinesh Bhuriya, Upendra Singh, 2015	Secure Ad Hoc On-Demand Vector Routing protocol (SAODV) DES, RSA	Active Attack	High Packet delivery ratio, Throughput
Raj Kamal Kapur, Sunil Kumar Khatri, 2015.	Ad-hoc On-demand Distance Vector Routing (AODV) Symmetric, asymmetric cryptographic technique	snooping, modification, replay and fabrication attack	confidentiality, integrity, authenticity
Deore Suvarna et al, 2015	Enhanced Adaptive Acknowledgement (EAACK) Digital signature and clustering algorithm	Misleading misbehaviour, finite transmission Range and receiver Collisions.	Found secure routing
AnjaliAnand, Himanshu Aggarwal, and Rinkle Rani, 2016	DSR Protocol DynamicChips Allotment (DCA) Mechanism	Misbehaving nodes	Secure Routing Improved network performance.
Archana P. Mandhare, Sujata V. Kadam, 2016	SRP (Secure and Reliable) routing protocol	Packet loss Break routes	Improve packet delivery ratio
Priyanka Patil, Nilesh Marathe, Vimla Jethani, 2016	ALERT protocol SHA-1 algorithm	DoS Attack	100% packet delivery
Nachammai. M, Dr. N. Radha, 2016	Cooperative bait detection scheme (CBDS) RC4 and MD5 algorithms	Gray hole black hole attack	routing path can be minimized

Rasika R. Mali, Sudhir T. Bagade, 2016	Secure ACK Algorithm	Misbehaving nodes	Highly secured MANETs
Garima Jain, Dr.Gajendra singh Rajawat, 2016	HAODV protocol Homographic Encryption Scheme	Pollution Attack	40% greater than existing protocol in throughput
A.Maheswary, Dr.S.Baskar, 2016	Letter-Shape Encryption	Man in middle attacks	Less time for encryption and decryption than RSA
V.Sesha Bhargavi, S.Viswanadha Raju, 2016	Trust Aware Routing Protocol	worm hole and black hole	High Packet delivery ratio, Throughput
Banoth Rajkumar, Dr.G.Narsimha, 2016	Trust based threshold revocation method	Malicious nodes	Misbehaving nodes are eliminated
S. Harihara Gopalan, Dr. R. Radha Krishnan, ,2016	AODV Fuzzy Integrated Ant Colony Optimization	End-to-end delay, bandwidth, network lifetime and energy consumption	Packet delivery ratio.
Suveg Moudgil, Dr. Sanjeev Rana, 2016	OLSR routing protocol Trust value calculation	Flooding and spoofing attacks	Minimize end to end delays
Rohit Chourasia, Rajesh Kumar Boghey, 2017	Intrusion detection and prevention system	Misbehaviour of packet dropping	Improved data receiving Minimizes dropping data

Sherin Zafar, 2017	Iris
	Cryptographic technique
		DoS	FRR= 0%
			Accuracy=100%,

P.Sathya, N.R.Sathiskumar, Dr.K.Ramasamy, 2017	PUMA (Protocol for Unified Multicasting through Announcements)	Malicious nodes	Throughput is increased. Routing overhead is highly reduced. Achieves high network lifetime.
Dr.B.Rosiline Jeetha, K.Sivakamipriya, 2017	Ad hoc on-demand multipath distance vector (AOMDV) hybrid BAT algorithm	Hybrid Attacks	Reduces hot spot problem Routing overheads about 5-10%

V. CONCLUSION

This paper elaborates different MANET routing protocols mainly reactive, proactive, hybrid like DSDV, AODV, ZRP and their behaviour pattern. To enhance the security, selection of a routing protocol plays a significant role in mobile ad-hoc network. This paper also discussed on MANET issues and examines lot of security problems. This paper also summarizes the various security challenges, attacks, characteristics and application of MANET. As a result of literature survey it is found are that the dynamic structure of MANET is vulnerable to several attacks. There are several types of security algorithms that used to solve the security problem but still solving network layer attack is the most challenging task which will be address in future.

REFERENCES

[1] Jie Liu, F. Richard Yu, Chung-Horng Lung, Helen Tang,"Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks*", IEEE Transactions On Wireless Communications, Vol. 8, No. 2, February 2009.*

[2] Rizwan R. Rangara ,Rupika S. Jaipuria ,Gauri N.Yenugwar, "Intelligent Secure Routing Model For MANET", *IEEE, 2010.*

[3] Shengrong Buet, F. Richard Yu, "Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks", *IEEE Transactions On Vehicular Technology, Vol. 60, No. 3, March 2011.*

[4] Hiteishi Diwanji and J.S. Shah," Enhancing Security in MANET through Unimodal Biometric Encryption Key, *IEEE,2011.*

[5] B.Thanikaivel, B. Pranisa, "Fast and Secure Data Transmission in MANET" *International Conference on Computer Communication and Informatics (ICCCI -2012), Jan. 10 – 12, IEEE, 2012.*

[6**]** Vijaya Bhaskar.Ch, Dr. D.S. R. Murthy," A Reliable Routing Approach in Mobile Ad-Hoc Network based on Genetic Algorithms*", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, October- 2013.*

[7] A. Menaka Pushpa, Dr. K. Kathiravan, "Secure Multicast Routing Protocol against Internal Attacks in Mobile Ad Hoc Networks*", IEEE GCC Conference and exhibition, November 17-20,2013.*

[8]Elakkiya.M, Dr.Edna Elizabeth.N,"Opportunistic routing to forgo flooding attacks in MANET", *International Journal of Engineering Development and Research, 2014.*

[9] D.Saravanan, T.Sangeetha, "Enhancing Network Performance Using Genetic Algorithm in Face Routing Protocol", *International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 1, February 2014.*

[10] Neha Agarwal, Neeraj Manglani," A New Approach for Energy Efficient Routing in MANETs Using Multi Objective Genetic Algorithm*", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015.*

[11] SherinZafar, M.K.Soni, M.M.S Beg, "An Optimized Genetic Stowed Biometric Approach to Potent QOS in MANET", *International Conference on Soft Computing and Software Engineering, Elsevier, 2015.*

[12] Remya S, Lakshmi K S, "SHARP: Secured Hierarchical Anonymous Routing Protocol for MANETs", International *Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, IEEE, 2015.*

[13] Ashish Sharma, Dinesh Bhuriya, Upendra Singh, "Secure Data Transmission on MANET by Hybrid Cryptography Technique", *IEEE International Conference on Computer, Communication and Control (IC4-2015).*

[14] Raj Kamal Kapur, Sunil Kumar Khatri, "Secure Data Transfer in MANET Using Symmetric and Asymmetric Cryptography", *IEEE, 2015.*

[15] Deore Suvarna et al "Acknowledgement security for MANET using EAACK*", IEEE, 2015.*

[16] Anjali Anand, Himanshu Aggarwal, and Rinkle Rani," Partially Distributed Dynamic Model for Secure and Reliable Routing in Mobile Ad hoc Networks", *IEEE Explore Journal Of Communications And Networks, Vol. 18, No. 6, December 2016.*

[17] Archana P. Mandhare, Sujata V. Kadam," E-TWRP: Establishing Trust Worthy Reliable Path in Mobile Adhoc Network", *IEEE, 2016.*

[18] Priyanka Patil, Nilesh Marathe, Vimla Jethani," Improved ALERT Protocol in MANET with Strategies to Prevent DOS & MITM Attacks", *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology , Pune IEEE, 2016.*

[19] Nachammai. M, Dr. N. Radha," Securing Data Transmission in MANET using An improved Cooperative Bait Detection approach", *2016 IEEE International Conference on Advances in Computer Applications (ICACA).*

[20] Rasika R. Mali, Sudhir T. Bagade," Detection of Misbehaving Node using Secure Acknowledgement in MANET", IEEE Explore, *International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016.*

[21**]** Garima Jain, Dr.Gajendra singh Rajawat, "Secure AODV Routing protocol based on Homographic Digital signature, *IEEE , 2016.*

[22] A.Mahe swary, Dr.S.Baskar," Letter To Shape Encryption For Securing MANET Routing Protocols", *IEEE International Conference on Computational Intelligence and Computing Research, 2016.*

[23] V.Sesha Bhargavi, S.Viswanadha Raju, "Enhancing Security in MANETS through Trust-Aware Routing", *IEEE WiSPNET 2016 conference*.

[24] Banoth Rajkumar, Dr.G.Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET", 2nd International Conference on Intelligent Computing, Communication & Convergence, Elsevier, *2016.

[25] S. Harihara Gopalan, Dr. R. Radha Krishnan," Trust Based Fuzzy Aided ACO for Optimal Routing with Security in MANET", *Asian Journal of Research in Social Sciences and Humanities Vol. 6, Special Issue Sept 2016, pp. 529-544.*

[26] Suveg Moudgil, Dr. Sanjeev Rana, "A Secure & Robust Scheme to Isolate DDoS Attacks Over MANET", *IJCSI International Journal of Computer Science Issues, Volume 13, Issue 3, May 2016.*

[27] Rohit Chourasi, Rajesh Kumar Boghe, "Novel IDS Security against Attacker Routing Misbehaviour of Packet Dropping in MANET", IEEE *, 2017.*

[28] Sherin Zafar, "Biometric Signature Based ApproachEnhancing Security of Networks Through a Novel", International Journal of Wireless Communications and Mobile Computing 2017; 5(1): 1-5 ISSN: 2330-1007 (Print); ISSN: 2330-1015 (Online).

[29] Sathya,N.R.Sathiskumar, .K.Ramasamy, “Effective Multicast Routing Algorithm for MANET”, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering ,Vol. 6, Special Issue 1, March 2017.*

[30] Dr.B.Rosiline Jeetha, K.Sivakamipriya, “Secure Routing and Detection of Hybrid Attacks in MANET”, *International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.*