JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

A REVIEW: SECURE ROUTING PROTOCOLS FOR MOBILE ADHOC NETWORKS (MANETs)

Srinivas Kalime[1], Dr.K.Sagar[2]

[1]Research Scholar, Osmania University, Hyderabad, Telangana (State)
[2]Professor, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana (State)

Emails: jits.cse2006@gmail.com[1] , kadapasagar@cbit.ac.in[2]

Received: 14 April 2020 Revised and Accepted: 8 August 2020

ABSTRACT: Mobile Ad-hoc Network is a multi-hop wireless networking of mobile nodes that have restricted resources by the conditions of battery life, memory, and processing power. The stream of traffic to the receiver nodes that are beyond the reach of sender devices will be routed by intermediate nodes. The routing in the MANETs is distinct from the traditional broadcasting network because the nodes not just serve as end machines although serve as routers. Because of the resource limitation of the nodes, the routing protocols for MANETs will need to be light-weight and presume a reliable environment. Protection in the Mobile Ad-hoc Network is a huge task since there is no centralized authority that can monitor the specific nodules that operate in the network. The attacks may also come from the outside and inside the network. This attack may result in either denial of services or misdirection of data traffic.This study organizes a safe and secure routing protocol in MANET and also examining the currently suggested method of alleviating such attacks. MANET routing protocols sent data packets to another node, certain intermediate nodule obtains valuable information about packets and sometimes cannot route the packet to the next node. Several nodes may change the contents of packets throughout the data transfer session. So that every single node can influence the initial data.

KEYWORDS: Ad-hoc Network, Routing Protocols, Security Attacks, SRP

I. INTRODUCTION

A MANET(mobile Ad-hoc Network) comprises a collection of mobile hosts that perform fundamental networking features such as routing, packet forwarding,without any assistance from a recognized organization. Nodes of an ad-hoc network depend on several intermediate nodes to send a data packet to the target location, because of the restricted scope of every mobile that is broadcast to the host. Security in MANET is an important element for fundamental network capabilities like packet routing and forwarding [1,2].

Figure1: Mobile ad-hoc network

Network functions may be conveniently endangered if the messages are not embedded within the underlying network capabilities during the early stages of their planning.Routing network utilizing dedicated nodes to provide support for essential functions like packet routing, forwarding, and networking management, in ad-hoc networks such tasks will be performed by all available nodes. This is extremely challenging for the central core of the security issues that are particular to ad-hoc networks. In contrast to the dedicated nodules of a traditional network, the nodules of an ad hoc network can no longer be trusted for the proper performance of key networking features.In wireless networks, there is a great requirement for security[3-5].The flexible performance of our wireless routing protocol network concentrated on the attack of the malignant agent. Table1[6] demonstrates the features and illustrations of passive and active attacks. Both passive and active attacks can be initiated on every layer of the network protocol stack. Table 2 [7] illustrates some instances of attacks on the various layers.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

Table 1. Active and Passive attacks

Type of Attack	Characteristics	Examples
Passive Attacks	✧ Obtains information without disturbing normal network operation ✧ Difficult to detect	Traffic Analysis, Traffic Monitoring, Eavesdropping
Active Attacks	✧ Can be internal(attacker within the network) or external(attacker outside the network) ✧ Can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node	Modification,Impersonation, Jamming and Message replay

Table 2 .Protocol Stack and Attacks

Layer	Work of Layer	Attacks
Application	Application Interface	viruses,worms,Trojan Attacks,Repudiation, DOS, Malicious Codes, and application abuses.
Transport	End to end Communication	Session Hijacking, SYN Flooding, DOS.
Network	Routing, Logical Addressing (IP Addressing)	Modification,Fabrication,Flooding,Sybil Impersonation,Black-hole,Wormhole,Grey-hole, Byzantine,,Sinkhole, Location disclosure,Routing table overflow, DOS,False route information etc.
Data link	Flow control, Error Control, Physical Addressing	Traffic monitoring and Analysis, DOS.
Physical	Raw bit Transmission	Signal Jamming, Interception,Eavesdropping,

II. VARIOUS ROUTING PROTOCOL FOR MANET

In MANET, there are various kinds of routing protocols for sending the packets. Every single forwarding has a particular rule to the packet transmission technique. In a various situations the mobile ad-hoc network utilizes various protocols , such as

(1) Proactive Protocol
(2) Reactive protocol
(3) Hybrid protocol

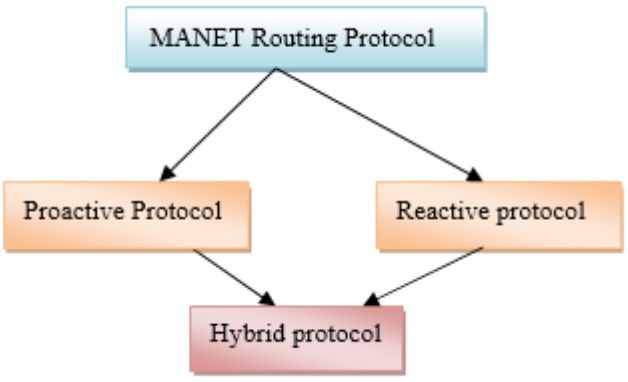

Figure2: MANET Routing Protocols

2.1 Proactive Protocol

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

In this routing protocol[8,9] network contains a distinctive routing table for establishing the connections and for sending the data packets to another node across the network. The routing information will be constructed in every single node throughout the exchange of Hello Messages that can connect the information to a nearby system. The TC (Topology Control) Message updates have been utilized to share the neighborhood connectivity information among all the nodules in the network. Each hub in the network provides a number of forwarding tables to hold the required updates that are event-driven and time-driven. The optimal routes to each other node are inferred from the following information. Multiple protocols under this category were planned. Such protocols have the benefit of minimal delay period in exploring the route but use plenty of resources in accordance with the conditions of power, memory, and bandwidth of the nodes.

The present protocol is one type of request-based function that will utilize network order to bandwidth and energy more effectively and efficiently. Model on a request basis instead of maintaining routing among all the nodes at all moments. In instances where the extra time delay in which request-based procedures might not be acceptable, if there are sufficient energy and bandwidth resources, proactive operations might be appropriate in those circumstances [10-13].

2.2 Reactive Protocol

This protocol looks for the route in an on-request approach and setting the connection to deliver and accept the packet from a sender device to the receiver device[14, 15] on request routing, the route discovery process is utilized to flood the RREQ (route request) packets across the entire network.

2.3 Hybrid Protocol

It is a special kind protocol that divides the network into multiple areas,which requires a hierarchical protocol such as the protocol ZHLS(zone-based hierarchical link state)[16-18].This protocol that successfully incorporates the optimal characteristics of the reactive and proactive routing protocol. In proactive protocols, hubs regularly switch information to sustain up-to-date routing information. Reactive protocols obtain the required route once it is necessary, by utilizing the process of route discovery. The Hybrid routing protocols are combining the fundamental characteristics of both methods. The Hybrid routing protocol will be based on the GPS (Global positioning system), that enables every node to recognize its physical location prior to planning a

particular area with a table to recognize it that it belongs to. There are various kinds of Hybrid protocols like Zone-based hierarchical link-state routing protocol, ZRP (Zone routing protocol) [19-21].

The routing protocols are susceptible due to the usage of collaborative routing algorithms that do not have security characteristics; resources are limited with the nodes, dynamic topology of the network and the lack of any security infrastructure within the network. The vulnerabilities of the routing protocols arise from the routing process. The control messages that are replaced for setting up the routes, maintenance of route, and upgrading of routing tables are susceptible to attack from the malicious devices which can function as an intermediate node or a source node. Once the mischievous hub is serving as the intermediate node it can either replay or change the accepted packets which can result in Denial of Service or disruption of the route. Once it is functioning as a source node it can either utilizes its individual address, the address of an arbitrary hub or an existing device to start an attack.The RERR, RREP and RREQ control messages were attacked by the malicious hub in a reactive routing protocol. In a proactive routing protocol, the TC and Hello messages were attacked by a malicious node to destroy the routing process[22-24]

III. VULNERABILITIES ON ROUTING PROTOCOLS

Currently, there is a wide range of routing protocols, but such protocols are not protected and are facing many attacks[25-27],which result in the vulnerability in the network and could extremely influence the effectiveness of the system.In mobile ad-hoc networks any node can influence by the various types of attacks. Mainly in MANET, there are two kinds of attack

1) Control traffic attack.
2) Data traffic attack.

Control packets are affected in control traffic attacks such as Blackmail attack, Sybil attack, Rushing attack, bogus registration attack, Hello flood attack, and Worm-hole attack. Data packets are affected in data traffic attacks such as Jellyfish attack, Grey- hole attack, Cooperative Blackhole attack, Blackhole attack, and so on.

3.1 Control Traffic Attack

3.1.1 Wormhole Attack

In the event that connection becomes the most minimal way to the receiver, at that point, these malignant hubs consistently selected, although routing way to the path.The wormhole attack is conceivable regardless of whether the hacker has not cooperated with any hosts, and regardless of whether all correspondence gives confidentiality and authenticity[28].In the wormhole attack, a hacker records data packet at one area in the system tunnels them to another area and re transmits them there into the system. The wormhole attack can perform by a solitary hub and it interfaces more than one hub as a wormhole connection.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

The wormhole attack is a genuine danger in numerous ad hoc network routing protocols.

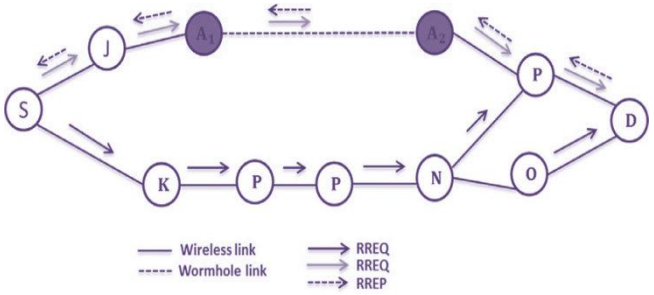

Figure3: Wormhole Attack

3.1.2 Hello Flood Attack

In this attack, each device forwards their packets in the direction of this node hopping to the improved target route. Hub communicates a solitary high-power transmitter to all its nearby devices[29]. At that point, hacker hub doesn't produce any traffic,so the premise of the execution hub takes the data packet and proceeds as a specific replay attack.

3.1.3 Bogus Registration

In this attack, hacker differentiates itself as a hub and create incorrect information to the nearby devices [30,31]. Once the packet is forwarded then interrupt the nearby devices.

3.1.4 Rushing Attack

In this attack, every hub prior to sending the data initially set the route from the sender to receiver. The client route the forward request and the nearby device route reply with the correct information about routing, and this process is repeated [32]. This attack rapidly sent with a transmitted message to the nearby devices; once a real request is received from nearby hub just reject the request, because of acceptance of the earlier requests.

3.1.5 Sybil Attack

Sybil attack demonstrates the various false characteristics, display multiple hubs in the networking [33]. So single device assume the various nodes and can interfere with several nodes at a moment.

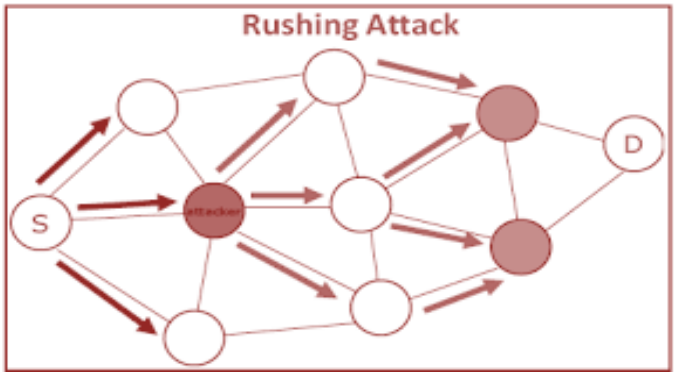

Figure4: Rushing attack

3.1.6 Blackmail Attack

In this attack, the hacker nodes being charged with a harmless connection [34]. Once the routing table will attempt to recognize the ideal node as per the vote and then if the hacker device contains an inadequate number of such MANET it can provide incorrect information in accordance with the route.

3.2 Data Traffic Attack:

3.2.1 Black Hole Attack:

In this attack, a malicious device performs as a Blackhole[35]declining all data packets that pass through it as like issue and energy fade from the route in a Blackhole. If the attacking hub is an associated hub of two systems, at that point, it completely isolated as the two systems.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

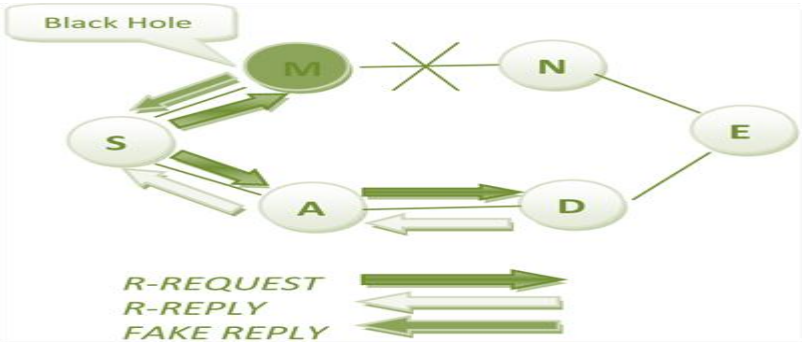

Figure 5. Blackhole attack

In MANET, the Blackhole issue is a serious security issue that is to be resolved.In this challenge, malignant devices utilize the routing protocol to promote itself as allowing the shortest route to a node for which the packets it needs to intercept. A malicious node corresponds to the paths of the sender and receiver in an internal Blackhole attack. As it appear inside so this hub makes itself active data route component. Now that node can conduct attack within the network. The Internal attack is an even greater split then an external attack. An External attack can turn into a type of internal attack once it holds the management of the inner malicious hub and manipulates it to attack another node in the MANET. External Blackhole Attacks remain exterior to the system and prevent access to network traffic or establishing a traffic jam in-network or by interrupting the whole network [36].

3.2.2 Cooperative Black Hole Attack

It is one of the highly significant attacks and can entirely interrupt the function of an Ad hoc network. This attack is comparable to the Blackhole attack, but higher than one malignant hub attempts to interrupt the network at the same moment[37].Mainly the only possible solution turns into a locating alternate path to the receiver, if at all occurs.

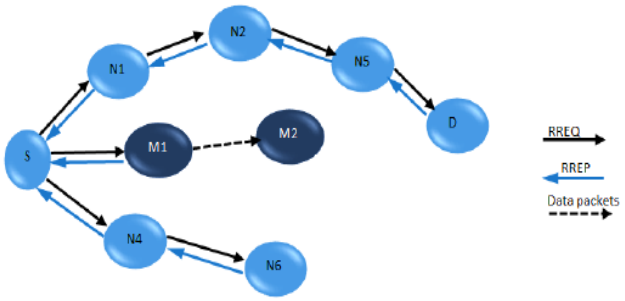

Figure 6. Cooperative black hole attack

3.2.3 Grey-Hole Attack

It too falls data packets, although malicious action of a node is restricted to particular conditions or activate. In this attack, the two most common kinds of performance took place[38].

- **Node dependent attack** drops data packets originating from a particular device or designed towards a particular victim device, [39] whereas for other hubs it is functioning normally by transmitting data packets to the receiver hubs accurately.
- **Time-dependent attack** [40] drops data packets that are based upon several preset/trigger time but is functioning properly throughout the other cases.

3.2.4 Jellyfish Attack

In this attack rather than instinctively dropping the data packets, it delays them prior to finally providing them. It handles the order of packets in accordance with the requirements they are being received and transmits randomly [41]. This interrupts the regular flow control mechanism utilized by the modules for dependable broadcasting. This attack can lead to a substantial end to end delay so there corrupting QoS.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

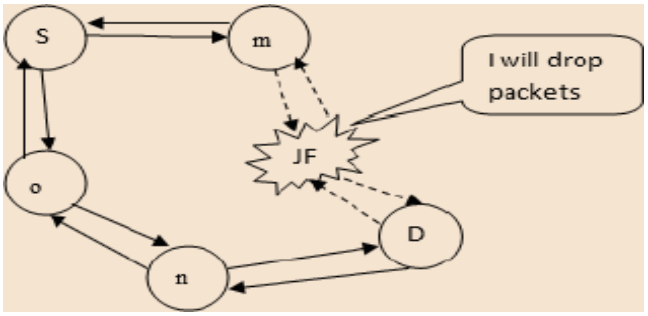

Figure7: Jellyfish attack

IV. VARIOUS SECURE ROUTING PROTOCOLS

Initially, an appropriate authentication is required for the secure routing protocol to require the digital signature of any authenticated hubs[42,43].It also requires changing the data of the control packets. It also frequently accompanied by the usage of single-way hash functions[44].Such routing method offer authentication facilities and services which protect against the change and repeating of routing control messages and utilizes various cryptographic fundamental elements to provide secure routing.

4.1 Fundamental Routing Protocols

This protocol kept by creating hub hashing the messages and initialing the resulted message digest, and that is authenticated by the receivers of a route request, by calculating the hash of a message utilizing the decided upon hash function[45,46].The benefit is that the protocol can fight against external attacks by monitoring for validity. The benefit of this protocol is that it expands the ICMP router discovery packet format to incorporate the IP and MAC address of the source and information about authentication that could be utilized to confirm the beacon transmission[47,48].But the difficulty of it is that it needs hubs to have shared secret keys to generate message authentication codes which are utilized to validate the control messages of routing and the program is based on the premise that the hubs in the network equally have confidence in each other and it utilizes public key cryptography to offer the security facilities.

4.2 Trust Based Routing Protocols

Trust is a worth that can be determined based on hubs activity once it required. Trust utilized to keep from different attacks such as a Selfish attack, DoS, Blackhole, Wormhole and so on. Trust can be executed in different manners, for example, by reputation, from the assessment of hubs and so on. These routing security plans which fall in this class allocate quantitative qualities to the hubs in the system, because of the noticed performance of the hubs being referred to. Then the trust esteems are utilized as extra measurements for the routing protocols [49,50]. The favorable position is that it is strong against hackers and equipped for altering its degree among neighborhood and system wide topology discovery. It can likewise work well in systems in which the membership and topology are altering regularly.

4.3 Incentive-Based Routing Protocols

Machines have to work together in ad hoc networks. Independent machines tend to refrain from collaboration. Incentive plans were planned as a way of promoting cooperation in such a situation. To operate effectively, incentive schemes have to be carefully customized to the features of the cooperation protocol they are supposed to provide support[51].Such routing programs were executed by utilizing credits that are provided to nodules that are working together and route packets. In turn network services like routing is offered only to such hubs that have excellent credit. If a hub at an adverse location might not get sufficient packets to route and therefore may not ever be able to obtain credits to route its packets.

4.4 Detection And Isolation Based Secure Routing Scheme

The attacks like Blackmail,Wormhole,Grayhole,Blackhole,Flooding were detected by this protocol. On exposure, the protocol requires direct actions to exclude such devices from the network, thus reducing the number of malignant hubs in a network, therefore increasing the additional QoS factors [52,53]. This protocol isolates a detects mischievous hubs in MANET. It is an improvement of DSR routing and is based on the choice of unselfish and selfish nodules. The benefit is that the confidence and routing computation procedure has been assessed through experience, examination and performance of the additional nodes, appear in the network [54-57]. This protocol can successfully identify selfish hubs and extract the wormhole hubs that decline packets.

4.5 Energy-Efficient Based Routing Algorithm

The trust is constantly present by implication in the protocols based upon the cooperation, particularly, among the entities implicated in routing functions in WSN Networks. WSN Networks remain to develop; they come to be vulnerable to attacks and therefore the requirement for an efficient security mechanism. Recognition of the appropriate encryption technologies for WSN is an essential task because of storage resource, computation capability and restriction of energy of the sensor nodes.For Adhoc networks, an innovative energy-aware routing algorithm to be recommended was known as a reliable minimum TSEOAP. Trust Secure Energy

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

Optimized Aggregation Protocol directs essential needs of WSN: attacker's detection, Data Aggregation, reliability, and energy-efficiency. It is an energy-effective routing algorithm that finds routes that minimize the overall energy necessary for packet traversal of end-to-end and improved detection of malicious nodes. A cryptography-based security mechanism was proposed, and the Elliptic Curve Cryptography technique was applied in WSN. This can improve the cryptography of technology through the characteristics of the algorithm, and produces the method for outstanding security [58,59].

V. CONCLUSION

A number of challenges persist in the area of securing wireless adhoc networks.The problem is designing efficient routing protocols that have both strong security and high network performance.From the broad examinations on the current routing protocols to secure MANET, it was seen that these protocols don't sufficiently moderate attacks by mischievous hubs which change packets as well as specifically drop a few or all the packets.Such mischievous hubs cause different network communication issues.These investigations have at last inspired us to desire an elective structure towards progressively productive,secure routing protocols for MANET to be utilized in a confrontational environment. Although researchers have studied security extensions for several existing protocols, many of these extensions remove important performance optimization's.Optimistic approaches can provide a better trade-off between security and performance.

VI. REFERENCES

[1]. Babu, A. V., P. Meenakshi Devi, and B. Sharmila. "Comparative Study of Manet Routing Protocols." Asian Journal of Research in Social Sciences and Humanities 6.6 (2016): 1924-1934.

[2]. Yassein, Muneer Bani, and Nour Alhuda. "Flying ad-hoc networks: Routing protocols, mobility models, issues." International Journal of Advanced Computer Science and Applications (IJACSA) 7.6 (2016).

[3]. Dearlove, C. Identity-based signatures for mobile ad hoc network (MANET) routing protocols. RFC 7859, DOI 10.17487/RFC7859, May 2016,< http://www. rfc-editor. org/info/rfc7859, 2020.

[4]. Zuo, Zhibin, et al. "P4Label: packet forwarding control mechanism based on P4 for software-defined networking." Journal of Ambient Intelligence and Humanized Computing (2020): 1-14.

[5]. Raj, Nawneet, Priyanka Bharti, and Sanjeev Thakur. "Vulnerabilities, challenges and threats in securing mobile ad-hoc network." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015.

[6]. Ning, Jianting, et al. "Passive attacks against searchable encryption." IEEE Transactions on Information Forensics and Security 14.3 (2018): 789-802.

[7]. Nazir, Muhammad Kashif, Rameez U. Rehman, and Atif Nazir. "A novel review on security and routing protocols in MANET." Communications and Network 8.4 (2016): 205-218.

[8]. Babu, M. Rajesh, et al. "Proactive alleviation procedure to handle black hole attack and its version." The Scientific World Journal 2015 (2015).

[9]. Raj, Nawneet, Priyanka Bharti, and Sanjeev Thakur. "Vulnerabilities, challenges and threats in securing mobile ad-hoc network." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015.

[10]. Nazhad, Seyed Hossein Hosseini, et al. "An efficient routing protocol for the QoS support of large-scale MANETs." International Journal of Communication Systems 31.1 (2018): e3384.

[11]. Alkhamisi, Abrar Omar, and Seyed M. Buhari. "Trusted secure adhoc on-demand multipath distance vector routing in MANET." 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2016.

[12]. Kumar, V. Vinoth, and S. Ramamoorthy. "Secure adhoc on-demand multipath distance vector routing in MANET." Proceedings of the International Conference on Computing and Communication Systems. Springer, Singapore, 2018.

[13]. Ubarhande, Sachin D., Dharmpal D. Doye, and Prakash S. Nalwade. "A secure path selection scheme for mobile ad hoc network." Wireless Personal Communications 97.2 (2017): 2087-2096.

[14]. Moon, Ayaz Hassan, et al. "Simulating and analyzing RREQ flooding attack in wireless sensor networks." 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). IEEE, 2016.

[15]. Faghihniya, Mohammad Javad, Seyed Mojtaba Hosseini, and Maryam Tahmasebi. "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network." Wireless Networks 23.6 (2017): 1863-1874.

[16]. Nair, Ranjana R., and S. Indira Gandhi. "Performance analysis of threshold based hybrid routing protocol for MANET." 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, 2015.

[17]. Pandey, Kavita, and Abhishek Swaroop. "A comprehensive performance analysis of proactive, reactive and hybrid MANETs routing protocols." arXiv preprint arXiv:1112.5703 (2011).
[18]. Er, Jatinder Kaur, and Gurpreet Singh Er. "Review study on MANET routing protocols: challenges and applications." International Journal of Advanced Research in Computer Science 8.4 (2017).
[19]. Ghode, Sushma D., and Dr KK Bhoyar. "A Comparative Study of ZRP and Energy Efficient ZRP (E-ZRP)." Available at SSRN 3426257 (2019).
[20]. Malwe, Shweta R., Soniya Rohilla, and G. P. Biswas. "Location and selective-bordercast based enhancement of zone routing protocol." 2016 3rd International Conference on Recent Advances in Information Technology (RAIT). IEEE, 2016.
[21]. Selvi, P. Tamil, and C. Suresh GhanaDhas. "A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET." Mobile Networks and Applications 24.2 (2019): 307-317.
[22]. Bhargavi, V. Sesha, M. Seetha, and S. Viswanadharaju. "A trust based secure routing scheme for MANETS." 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence). IEEE, 2016.
[23]. Karthikeyan, B., S. Hari Ganesh, and N. Kanimozhi. "Security Improved Ad-Hoc on Demand Distance Vector Routing Protocol (SIm AODV)." International Journal on Information Sciences & Computing 10.2 (2016).
[24]. Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating route request flooding attack in MANET." Wireless Networks 24.8 (2018): 2899-2914.
[25]. Anjum, Shaik Shabana, Rafidah Md Noor, and Mohammad Hossein Anisi. "Review on MANET based communication for search and rescue operations." Wireless personal communications 94.1 (2017): 31-52.
[26]. Potukuchi, Raghu Vamsi, and Krishna Kant. "Trust aware cooperative optimised link state routing protocol." International Journal of Systems, Control and Communications 8.1 (2017): 1-21.
[27]. Saddiki, Kamel, et al. "Black hole attack detection and ignoring in OLSR protocol." International Journal of Trust Management in Computing and Communications 4.1 (2017): 75-93.
[28]. Sankara Narayanan, S., and G. Murugaboopathi. "Modified secure AODV protocol to prevent wormhole attack in MANET." Concurrency and Computation: Practice and Experience 32.4 (2020): e5017.
[29]. Gill, Reenkamal Kaur, and Monika Sachdeva. "Detection of hello flood attack on LEACH in wireless sensor networks." Next-Generation Networks. Springer, Singapore, 2018. 377-387.
[30]. Quyoom, Abdul, Aftab Ahmad Mir, and Abid Sarwar. "Security Attacks and Challenges of VANETs: A Literature Survey." Journal of Multimedia Information System 7.1 (2020): 45-54.
[31]. Usman, Muhammad, et al. "Mitigating distributed denial of service attacks in satellite networks." Transactions on Emerging Telecommunications Technologies 31.6 (2020): e3936.
[32]. Reddy, K. Ganesh, and P. Santhi Thilagam. "5 TRUST-BASED HYBRID IDS FOR RUSHING ATTACKS IN WIRELESS MESH NETWORKS." Recent Advances in Computer Based Systems, Processes and Applications: Proceedings of Recent Advances in Computer based Systems, Processes and Applications (NCRACSPA-2019), October21-22, 2019 (2020): 49.
[33]. Dong, Shi, Xin-gang Zhang, and Wen-gang Zhou. "A Security Localization Algorithm Based on DV-Hop Against Sybil Attack in Wireless Sensor Networks." Journal of Electrical Engineering & Technology 15.2 (2020): 919-926.
[34]. Kaushik, Ila, and Nikhil Sharma. "Black Hole Attack and Its Security Measure in Wireless Sensors Networks." Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's. Springer, Cham, 2020. 401-416.
[35]. Gurung, Shashi, and Siddhartha Chauhan. "A dynamic threshold based approach for mitigating black-hole attack in MANET." Wireless Networks 24.8 (2018): 2957-2971.
[36]. Gurung, Shashi, and Siddhartha Chauhan. "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET." Wireless Networks 25.3 (2019): 975-988.
[37]. Gurung, Shashi, and Siddhartha Chauhan. "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability." Wireless Networks 26.3 (2020): 1981-2011.
[38]. Schweitzer, Nadav, et al. "Contradiction based gray-hole attack minimization for ad-hoc networks." IEEE Transactions on Mobile Computing 16.8 (2016): 2174-2183.
[39]. Baig, Zubair A., et al. "Averaged dependence estimators for DoS attack detection in IoT networks." Future Generation Computer Systems 102 (2020): 198-209.
[40]. Althunibat, Saud, et al. "Countering intelligent-dependent malicious nodes in target detection wireless sensor networks." IEEE Sensors Journal 16.23 (2016): 8627-8639.
[41]. Thapar, Shruti, and Sudhir Kumar Sharma. "Detection and Prevention Policies of Jellyfish Attack in MANET." Available at SSRN 3548382 (2020).
[42]. Keys, Andrew T., et al. "Service channel authentication processing hub." U.S. Patent No. 9,306,930. 5 Apr. 2016.

[43]. Duraipandian, M., and H. Packiaraj. "Review on Message Authentication and Source Privacy in Wireless Sensor Networks." sensors 1.4 (2016).

[44]. Chevalier, Céline. "UC-Secure Protocols using Smooth Projective Hash Functions." Soutenance le 11 (2017): 12.

[45]. Das, Supriya, and Parma Nand. "Survey of hash security on DSR routing protocol." 2016 International Conference on Computing, Communication and Automation (ICCCA). IEEE, 2016.

[46]. Nithya, S., and C. Gomathy. "Detection and Prevention of Collaborative Attack and Energy Efficient Routing in Wireless and Ad hoc Network." Indian Journal of Science and Technology 9 (2016): S1.

[47]. Mohammadi, Payam, and Ali Ghaffari. "Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis." Wireless Personal Communications 106.2 (2019): 365-376.

[48]. Varadarajan, Vijayakumar, Madhavi Sinha, and Rahul Kushwaha. "Detection and Removal of Black Hole Attack in Vehicular Ad-Hoc Network Using secure AODV Routing Algorithm." (2020).

[49]. Marchang, Ningrinla, Raja Datta, and Sajal K. Das. "A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks." IEEE Transactions on Vehicular Technology 66.2 (2016): 1684-1695.

[50]. Ahmed, Adnan, et al. "A trust aware routing protocol for energy constrained wireless sensor network." Telecommunication Systems 61.1 (2016): 123-140.

[51]. Singh, Amit Kumar, and Rajendra Pamula. "IRS: Incentive based routing strategy for socially aware delay tolerant networks." 2018 5th international conference on signal processing and integrated networks (SPIN). IEEE, 2018.

[52]. Gandhi, Jenish R., and Rutvij H. Jhaveri. "Packet forwarding misbehaviour isolation using fuzzy trust-based secure routing in MANET." International Journal of Computer Applications 122.3 (2015).

[53]. Shah, Sachi N., and Rutvij H. Jhaveri. "A survey of various energy efficient secure routing approaches for wireless ad-hoc networks." 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015.

[54]. Govindasamy, Jegan, and Samundiswary Punniakody. "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack." Journal of Electrical Systems and Information Technology 5.3 (2018): 735-744.

[55]. Majumder, Sayan, and Debika Bhattacharyya. "Relation estimation of packets dropped by wormhole attack to packets sent using regression analysis." Emerging Technology in Modelling and Graphics. Springer, Singapore, 2020. 557-566.

[56]. Tiruvakadu, Divya Sai Keerthi, and Venkataram Pallapa. "Confirmation of wormhole attack in MANETs using honeypot." Computers & Security 76 (2018): 32-49.

[57]. Kumar, Gulshan, Mritunjay Kumar Rai, and Rahul Saha. "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in wireless sensor networks." Journal of Network and Computer Applications 99 (2017): 10-16.

[58]. VEENA, S., and P. JANSHI. "A Trust with an Energy Optimized Model in WSN." (2018).

[59]. Singh, Opinder, Jatinder Singh, and Ravinder Singh. "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET." Cluster Computing 21.1 (2018): 51-63.

[60]. International Journal of Computer Sciences and Engineering Survey Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693 "Different Attacks and their Defense Line in Mobile Ad hoc Networks: A Survey".

[61]. Srinivas Kalime,Dr.K.Sagar,"Recent Trends and Security Challenges in Mobile Adhoc Networks" © 2019 IJRAR March 2019, Volume 6, Issue 1 www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138)

[61]. Srinivas Kalime,© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X " A Novel review on Secure Routing Protocols in MANETs" .

[62]. A Survey of Secure Wireless Ad Hoc Routing, IEEE COMPUTER SOCIETY 1540-7993/04/$20.00 © 2004 IEEE IEEE SECURITY & PRIVACY.