A Proficient Attack Prediction using Hash Algorithm in Manet

Dr. Md Riyazuddin
Assistant Professor
Department of IT
Anurag University
Telangana, India.
riyaz.mdr1@gmail.com

Dr. Md Jaffar Sadiq
Associate Professor and Head
Department of CSE-Data Science
Sreenidhi Institute of Science and Technology
Telangana, India.
dr.jaffarsadiqmd@gmail.com

Dr. Rajeev Agrawal
Director
Lloyd Institute of Engineering and Technology
Greater Noida, Uttar Pradesh, India.
director.engineer@lloydcollege.com

Surendra Kumar Shukla
Department of CSE
Graphic Era Deemed to be University
And Graphic Era Hill University
Dehradun, Uttarakhand, India.
Telangana, India.
surendrakshukla21@gmail.com

Ajay Rana
Amity University
Greater Noida
Uttar Pradesh, India
Ajay_rana@gn.amity.edu

Rajesh Singh
Division of Research & Innovation
Uttaranchal University
Uttarakhand, India.
rajeshsingh@uttaranchaluniversity.ac.in

2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS) | 978-1-6654-7657-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICTACS56270.2022.9988726

***Abstract*—An instantly established network without any infrastructure is known as a mobile ad hoc network (MANET). The issue is that rogue nodes might or might not take part in the process of route discovery in an effort to lower the network's overall performance. Intrusions have a considerable negative influence on the percentage of packets that are delivered rather than routed. The Hash Algorithm paradigm provides a blend of detection and preventive strategies. An Adhoc Network ensures that attacks are recognized and stopped during data routing by doing this. The model that was provided demonstrates that the attacks were successfully repelled.**

Keywords—Attacks, Ad Hoc Network, Defense, and Data Routing

I. INTRODUCTION

1) Manet Challenges: Issues that must be resolved in the MANET environment are presented in the list of problems that follows. There is a serious threat to this occurrence. Networks can be set up carefully to guarantee security before, during, and after data transit. Figure 1 illustrates common issues in MANET.

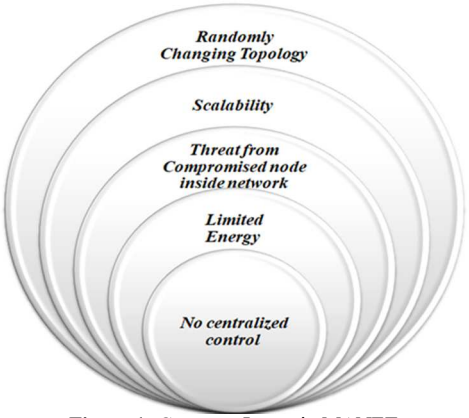

Figure 1: Common Issues in MANET

The amount of data that can be transmitted by wireless networks is substantially smaller than that of fixed networks since wireless networks have a constrained radio spectrum. For the best possible bandwidth use, this calls for a wireless network routing system. As little overhead as feasible can be used to accomplish this. The limited transmission range places restrictions on the routing strategies used to manage terrain data as well. Frequent topology changes in MANETs necessitate higher controller overhead, which further reduces bandwidth. the time-varying properties of wireless connections A wireless channel might experience route breakdowns, attenuation, interference, or jamming, among other transmission impairments.

The coherence, order, and data rate of these wireless broadcasts are incompatible with these characteristics. The flexibility of the receiver and transmitter as well as the atmosphere's conditions determine how much these qualities interfere with transmission. The Nyquist and Shannon theorems, two distinct key limitations that control the capacity to transmit information over various data plans, can also be quantified.

2) Broadcast properties of the wireless medium: The broadcast properties of a wireless channel are established by all devices within direct transmission range of the channel, including broadcasts produced by devices. When a device is receiving data, no other adjacent devices are required to be sending except the transmitter. If a device's communications do not disrupt ongoing sessions, it can access shared media. Despite the possibility of several devices using the wireless network at modest speeds, the likelihood of data packet failures is rather significant. Even networks are capable of creating havoc and hiding device issues.

3) Packet loss: Data packets that are damaged at the receiving device as a result of a fleeting transmission from a node inside the receiver's communication chain but outside the sender's direct communication chain are referred to as "end-device blockage problems." The presence of hidden terminals causes higher crashes, intrusions, location-

978-1-6654-7657-7/22/$31.00 ©2022 IEEE

dependent conflicts, one-way associations, and periodic device movement in ad-hoc wireless networks, which are denoted by this symbol. Route disruption and a general decrease in wireless pass through properties. Ad-hoc wireless networks face a relatively high level of packet damage due to transmission faults.

4) Mobility related route changes: As nodes move about, the wireless ad-hoc network's system topology becomes very dynamic, leading to several path breakdowns in a single meeting. In such circumstances, course modifications are common. As a result, flexibility management is a crucial area of study for ad-hoc networks.

5) Mobility related packet losses: Ad-hoc network communication links are insecure, and regular usage of cautious techniques with serious damage frequency reduces MANET performance. Although if the frequency of errors is excessive, it is challenging to transport a packet of data to its destination.

6) Battery constraints: Lack of resources is the main obstacle for mobile devices over ad hoc networks. There are dominance-based constraints on the nodes embedded in such networks to preserve mobility, size, and capacity. Due to the processing power and energy they store, nodes are bulky and immobile. Therefore, this resource can only be used by MANET devices.

7) Network partitions: In ad-hoc networks, nodes are frequently accidentally shifted, which can lead to network splits. In rare circumstances, this gap might have a significant negative influence on intermediary nodes.

8) Ease access to wireless transmissions: Wireless transmission is easily accessible (security concern): Ad-hoc networks broadcast in outdoor settings. The network's devices all share it. The transmission of data by one device is acknowledged by all other devices on the direct line of communication. As a result, any data or information sent across the network will undoubtedly be taken by a hacker. A party may be in violation of confidentiality agreements if they may infer information obtained through snooping [6].

9) Routing: Since network node requirements for unicasting, multicasting, and geocaching are higher in MANETs than in single-hop wireless networks, routing is a crucial problem. The varied speeds of movement and the quick changes in network structure are the cause of this.

10) Quality of Service: Because of the various quality level expectations that network nodes have set, MANET quality of service is a significant concern. These networks need the strictest QoS restrictions, especially for multimedia, as it gets harder to satisfy various quality of service criteria in terms of tiers and priorities [7].

11) Security: Security is one of MANET's primary concerns due to the wireless environment. From one node to another, user data must be delivered properly and securely. The idea of least privilege can also be used to increase the security of MANET systems that are advised for use in businesses. There is also a hybrid model that combines the advantages of the two access control strategies [8,9].

II. Adaptive Routing Protocol For Data Communication In Manet

Every time a node communicates with a specific node, it broadcasts its current status to other nodes close by. Proactive, reactive, and mixed routing protocols are the three different subtypes.

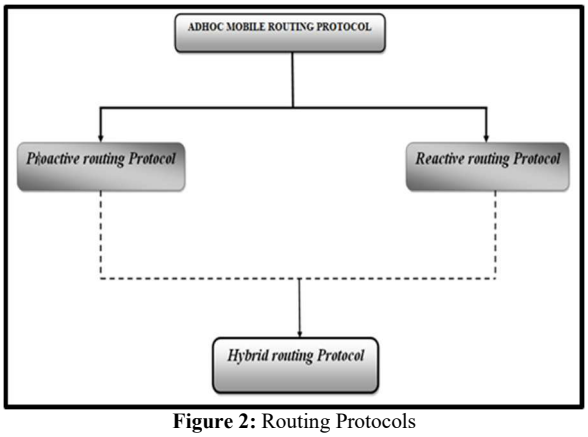

Figure 2: Routing Protocols

1) Proactive Routing Protocol: The proactive routing protocol is a variant of the table-driven routing protocol that was released in version 2.1. Each node maintains a routing table that contains information about its neighbors, reachable nodes, and hop count. As the network expands, costs rise and performance suffers. OLSR and DSDV (Destination Sequenced Distance Vector) are examples of proactive protocols (Optimized Link State Routing).

2) Reactive Routing Protocol: Reactive routing protocols are also referred to as on-demand routing protocols. As soon as a node attempted to send a data packet, a reactive protocol began. The benefit of this method is that it lessens bandwidth waste from round-robin transmission. This protocol's fundamental flaw is that it causes packet loss. Ad Hoc On Demand Distance Vector (AODV) and Dynamic Source Routing are examples of reactive routing protocols (DSR). Each AODV node maintains a routing table that contains the next hop information. A route discovery method is started if the destination node cannot be reached from the source node. A source node broadcasts an RREQ packet in order to start the route discovery procedure. If the routing table of a receiving node contains information about the destination node, that node sends a Route Reply Packet (RREP) to the source node. When the network topology changes or a link fails, a route maintenance procedure is

started. A route error packet (RRER) alerts the originating node of the problem. From source nodes to destination nodes, DSR nodes track route caches. The packet delivery rate within the upstream network declines and DSR performance deteriorates as network mobility rises.

3) Hybrid Routing Protocol: The hybrid routing technology combines proactive and reactive routing's benefits. Proactive protocols are used to gather unknown routing information when the topology changes, and reactive protocols are subsequently used to store the routing information. Temporarily Ordered Routing Algorithm (TORA) and Zone Routing Protocol are two examples of hybrid protocols (ZRP).

III. Overview Of Possible Attacks In Manet

As a result, the decentralized character of the network is advantageous. Decentralization increases the network's dependability and flexibility. Mobile ad-hoc networks can be subjected to a range of passive and active attacks.

1) Passive Attack: This kind of assault does not involve the use of fake information. To find out more about the flow, click on the links below. This attack technique is used by attackers to gather data, leave traces on affected networks, and launch effective attacks. Eavesdropping, traffic analysis, and surveillance are examples of passive attacks.

a. ***Eavesdropping:*** Eavesdropping is a strategy of passive attack. Nodes only record personal information. This data is accessible to rogue nodes in the future. The location, public key, private key, password, and other sensitive information can all be obtained by an eavesdropper.

b. ***Traffic Analysis:*** For MANET attackers, both data packets and traffic patterns are crucial. For instance, you may learn a lot about network structure by looking at traffic patterns. Node destruction enables the collection of useful topology-related data, network self-organization, and traffic analysis as an active attack.

c. ***Snooping:*** Snooping is the act of gaining unauthorized access to someone else's data. While not usually confined to intercepting data in transit, this is comparable to eavesdropping. Snooping is the act of casually scanning a computer screen showing another person's inbox or keeping track of email entries. In advanced espionage, software tools are used to remotely monitor computer or network device behavior. Hackers that wish to do harm (crackers) frequently employ spying methods to monitor keystrokes, collect login and password data, and intercept emails and other private interactions and data transfers. To monitor employees' internet behavior and use of company computers, businesses occasionally have justifiable reasons to spy on their workers. Governments are permitted to spy on citizens in order to gather information and combat crime and terrorism. Any application or service that employs computer technology for spying is referred to as snooping, which typically carries a negative connotation.

2) Active Attack: The attacker successfully violates either network resources or sends data in this form of intrusion by interfering with routing, depleting network resources, and disturbing nodes. The following illustrates the nature of the attacker's current MANET attacks and how they carry out their threats.

a. ***Black hole Attack:*** In flooding attacks, attackers use up all available network bandwidth, drain the processing and battery capacity of nodes, interfere with routing, and significantly reduce network performance. The AODV protocol, for instance, enables a malicious node to swiftly transmit a large number of RREQs to target nodes that are not connected to the network. No one reacts, and the RREQ overwhelms the entire network. This uses up network bandwidth and depletes the node's total battery, which may result in a denial of service.

b. ***Gray-hole attack:*** AODV routing techniques are subject to such assaults. Any intermediate node can react to an RREQ message if it has a suitably up-to-date route, thanks to a mechanism used by a malicious node to reduce routing delays. In this attack, a malicious node responds to route request packets on the network by claiming to have the most direct and latest route to the target node. Thus, it would be simple for a rogue node to divert network traffic and then discard transient packets that were targeted to it. Routing malfunction attacks are another name for assaults known as "gray holes" that result in dropped messages. Greyhole attacks take place in two stages. In the first phase, a node advertises its suitability as a path to a destination, and in the second phase, the node discards intercepted packets with a specific probability.

c. ***Wormhole Attack:*** A wormhole attack involves an attacker "tunneling" packets to a different location on the network and injecting them into the network from there. Unreliable routing may result from tunneling routing control messages. The phrase "wormhole" describes a route between two planned strikes. This DSR attack can halt route discovery due to the broadcast and potentially force unaddressed packets into a wormhole. Because information is frequently transmitted over paths that are not actually part of the network, wormholes can

be hard to spot. Wormholes can unintentionally harm your network, making them risky.

d. ***Link spoofing attack:*** To obstruct routing, a rogue node advertises phony links with no neighbors. An attacker could, for instance, share a fake connection with the target's two hop neighbors using the OLSR protocol. The malicious node is consequently chosen as her MPR for the target node. A malicious node that poses as an MPR node has the ability to alter data or change traffic. Altering or stopping traffic or initiating different kinds of DoS attacks.

e. ***Malicious code attacks:*** Viruses, worms, spyware, and Trojan horses are examples of malicious code attacks that target both operating systems and user applications. Denial Attack: Refusing to take part in all or a portion of a communication is known as denial.

f. ***Session Hijacking:*** Session hijackers use the chance to take advantage of the unsecure session after it has been established. A series of denial-of-service attacks are then launched after the attacker in this attack spoofs her IP address on the victim node and acquires the proper sequence number (or the target's expected number). A hostile node tries to take secure data (passwords, private keys, login names, etc.) and other information from a node through session hijacking. Address attacks on the OLSR protocol are sometimes known as session hijacking attacks. When a hostile node initiates a TCP session hijacking attack, it may result in a TCP ACK storm issue.

g. ***SYN Flooding Attack:*** Multiple TCP connections are made with the target node during a SYN-flooding attack, many of which are only partially open. These half-opened connections don't provide a full handshake and connection.

h. ***Denial of service attack:*** Denial-of-service attacks that utterly obliterate routing information target the full functionality of ad-hoc networks. When a rogue node discovers a transmission frequency, it launches an unique kind of DoS attack known as jamming. In this kind of attack, the jammer poses a security risk. Attacks that employ jamming also prevent the reception of valid packets.

i. ***Selfish Misbehavior of Nodes:*** These assaults directly affect node performance without affecting network activities. There could be two significant parts to it. Due to the uneven bandwidth distribution between batteries, energy is saved.

j. ***Traffic monitoring and analysis:*** It is possible to discover new attack launchers and communication channels by using traffic analysis and monitoring tools. Not only is MANET susceptible to these assaults, but other wireless networks are as well. Networks like Wi-Fi, cellular, and satellite are also prone to attack. We pay less attention to this level of attack in order to protect MANET.

3) Routing Attack: The network's routing protocols break as a result of these attacks. Router assaults can take a variety of shapes, including:

a. ***Rush Attack*:** The attacking node transmits packets containing route discovery requests throughout the network without waiting for other nodes to follow suit. As a result, if a node has already received a request packet delivered by an authorized node, it views it as a duplicate and discards it. As a result, attackers are always moving, making it incredibly challenging to locate such hostile nodes.

b. ***Selfish Behavior:*** Attacking nodes take part in route discovery and join active routes voluntarily in this attack. The attacking node will begin deleting pointless data packets after entering an active route, conserving the energy required to convey data packets from other nodes.

c. ***Jellyfish Attack:*** Attacks by jellyfish are slightly distinct from those by black holes and grey holes. Instead of being simply discarded, data packets are blocked before being transferred. Even worse, you run the risk of messing up the order in which the packets were actually received by delivering them in random order. This interferes with the typical flow control technique that nodes depend on for trustworthy transmission. An attack by jellyfish may cause considerable end-to-end delays and subpar service.

IV. PROPOSED METHOD

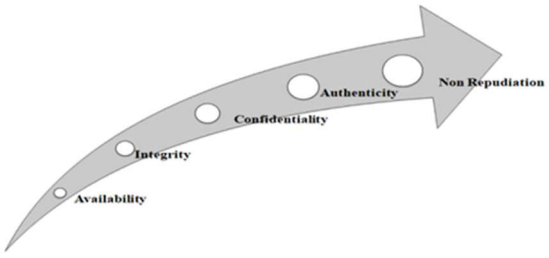

Figure 3: Wireless network's security restrictions

Using a network simulator and the fundamental wireless network security restrictions depicted in Figure 3, the suggested model is constructed and tested.

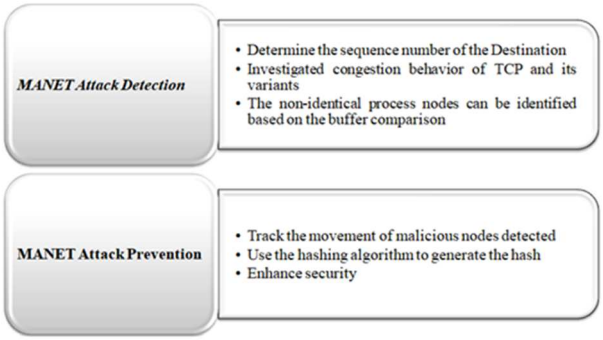

Figure 4: MANET Attack detection and Prevention

1) ***MANET attack detection and prevention approach*****:** Figure 4 depicts the detection and prevention of MANET attacks. A forwarding node needs to do more than just send a packet to the next hop node in order to forward a message correctly and unmodified. Sending a data packet after the recipient's neighbor on the other end has updated the data is an example of a failed transmission. If the sender learns that its neighbors are being illegally throttled, it reduces their transfer rates. The trust value of the path is calculated using the trust values of intermediate nodes along the route when a source uses adjacent nodes to find a path to a destination.

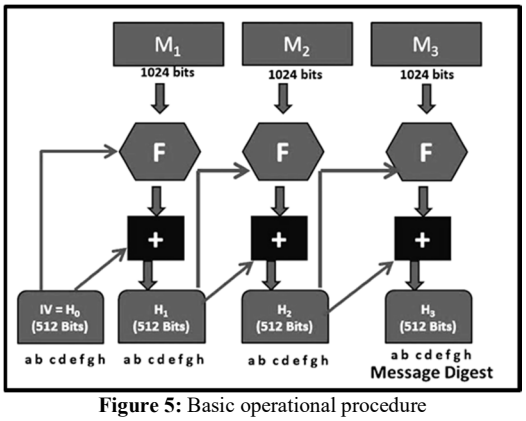

Figure 5: Basic operational procedure

The suggested trust model increases its capacity to further defend data from known attacks by utilizing the SHA algorithm. Because it is computationally challenging to locate a message that fits a specific message digest or to locate two different messages that yield the same message digest, hashing techniques are secure. A different message digest will almost likely occur from changing the message. The algorithm then begins the verification process. The hash code's size affects how resilient a hash function is to attacks. The SHA algorithm with 1024 bits per round is depicted in Figure 5. This method produces an extremely secure digest message by adding more rounds.

V. Results And Discussions

Table 1 displays the facility restrictions for the planned task. The performance of hash algorithm models is assessed using network indicators. Throughput, detection rate, packet overhead, are a few of these.

TABLE I. Setup Simulation

Setup Constraints	Actuality
Simulator	NS2
Mobility model	Random Waypoint model
Transmission Protocol	UDP
Number of Malicious nodes	0-25
Packet size	512 bytes
Types of Attack	Proactive Routing attacks

The quantity of packets received by the destination node and the quantity of (PDR) packets supplied by the source node are used to calculate the packet delivery rate. His PDR simulation results by number of attackers are displayed in Figure 6. When there are no attacker nodes present on the network, PDR can rise to 98.48%. As the number of assaulting nodes rises, PDR falls. When compared to other network attacks, this is high. Attacks that are frequent and large in volume thus add to packet overhead. Seen in Figure 7. The effectiveness of the hashing technique in limiting access to the data is seen in Figure 8 of the suggested model.

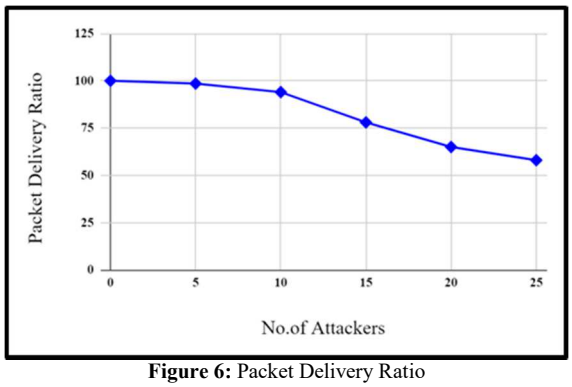

Figure 6: Packet Delivery Ratio

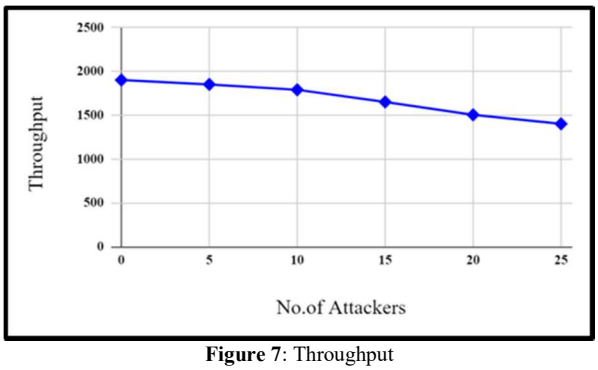

Figure 7: Throughput

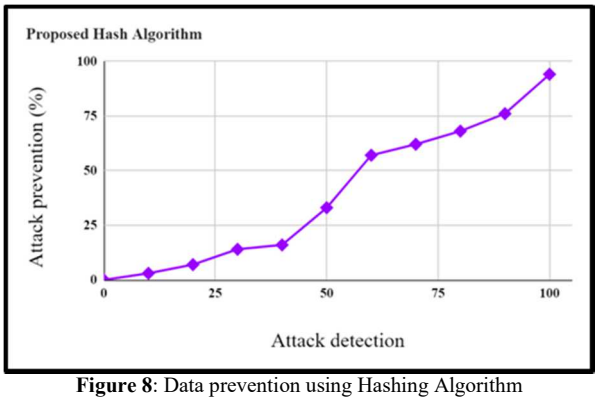

Figure 8: Data prevention using Hashing Algorithm

VI. CONCLUSION

The simulation results show that the algorithm-based routing protocol is built to achieve high packet delivery rate, detects malicious nodes at high rate, decreases the amount of time it takes for packets to reach their destination, and increases packet efficiency. It demonstrates the growth. Additionally, it produces fantastic throughput outcomes. A second stage of attack prevention that concentrates on hashing techniques is combined with the suggested trust-based paradigm for maintaining confidentiality.

REFERENCES

[1] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, ICNP '02, pp 78–89, Washington, DC, USA, 2019. IEEE Computer Society.

[2] Hu Y-C, Perrig A, Johnson DB (2013) Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security,WiSe '03, pp 30–40, New York, NY, USA. ACM

[3] Zapata MG, Asokan N (2012) Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security, WiSE '02, pp 1–10, New York, NY, USA. ACM

[4] Al-Shurman M, Yoo S-M, Park S (2014) Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference, ACM-SE 42, pp 96–97, New York, NY, USA. ACM

[5] Hu Y-C, Perrig A, Johnson DB (2017) Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3, pp 1976–1986, march-3 April 2003

[6] Johnson DB, Maltz DA (2016) Dynamic Source Routing in Ad HocWireless Networks. Kluwer Academic Publishers

[7] Perkins CE, Bhagwat P (2014) Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers. In Proceedings of the conference on Communications architectures, protocols and applications, SIGCOMM '94, pp 234–244, New York, NY, USA. ACM

[8] Perkins CE, Royer EM (2014) Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, pp 90–100, Feb 1999

[9] Zhou L, Haas ZJ (2020) Securing ad hoc networks. Network, IEEE 13(6):24–30

[10] Buttýan L, Hubaux J-P (2013) Stimulating cooperation in selforganizing mobile ad hoc networks. Mob Netw Appl 8:579–592

[11] Kong J, Luo H, Xu K, Gu DL, Gerla M, Lu S (2002) Adaptive security for multilevel ad hoc networks

[12] Hu Y-C, Perrig A, Johnson DB (2015) Ariadne: a secure ondemand routing protocol for ad hoc networks. Wirel Netw 11:21– 38

[13] Yang H, Meng X, Lu S (2012) Scane: Selforganized network-layer security in mobile ad hoc networks. In Proceedings of the 1st ACM workshop on Wireless security, WiSE '02, pp 11–20, New York, NY, USA.

[14] Anurag Shrivastava; Rajneesh Sharma; Mohit Kumar Saxena; V. Shanmugasundaram; Moti Lal Rinawa; Ankit, Solar energy capacity assessment and performance evaluation of a standalone PV system using PVSYST,Materials Today: Proceedings,2021-07, DOI: 10.1016/j.matpr.2021.07.258

[15] Srivastava, A., Singh, A., Joseph, S.G.Borole, Y.D., Singh, H.K.,WSN-IoT Clustering for Secure Data Transmission in E-Health Sector using Green Computing Strategy,2021 9th International Conference on Cyber and IT Service Management, CITSM 2021, 2021

[16] Shrivastava, A.; Ranga, J.; Narayana, V.N.S.L.; Chiranjivi; Borole, Y.D., Green Energy Powered Charging Infrastructure for Hybrid EVs, 2021 9th International Conference on Cyber and IT Service Management, CITSM 2021,DOI: 10.1109/CITSM52892.2021.9589027.