Deepak Badgujar ,2022, 10:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Wormhole Attack Detection in MANET Using a Trusted Method

M.Tech. Scholar Deepak Badgujar, Assistant Professor Lokendra Jat
Department of Computer Science
Patel College of Science & Technology , Indore , India
deepakbadgujar1995@gmail.com,lokendra.jat@patelcollege.com

Abstract: The Wireless Network is what's known as a mobile ad-hoc network, or MANET for short. This implies that nodes may move about freely inside the network. There will be several attacks on the network layer, but you will only be introducing the worm hole assault. Wormhole attacks are so-called because they involve more than one rogue node creating a tunnel. In this research, we present the trusted AODV routing protocol, which calculates the trust value by using the tangent hyperbolic function. When compared to the standard AODV protocol, the result demonstrates an improvement in performance.

Keywords- MANET, AODV, worm hole attack, trusted AODV,NS2.

I. INTRODUCTION

Network that means it's not recurred infrastructure. In MANET nodes are move energetically nature. The dynamic natures of MANET make it more vulnerable. In network layer many attacks possible but we focus only worm hole attack. When more than one malicious node are create tunnel is called wormhole attack [2]. Due to high mobility of mode routing is big challenge in ad-hoc network. In the proposed work, trust based routing protocol is defined in which trust computation is done using tangent hyperbolic function which calculate the trust value of their neighboring nodes promiscuously. They have a rest of the paper is organized as follows Section II runs some background of related work. Section III for working of AODV routing algorithm Section IV working of worm hole attack Section V introducing worm hole attacks as our proposed work. Section VI suggests simulation work and result. Finally, we conclude in section VII.

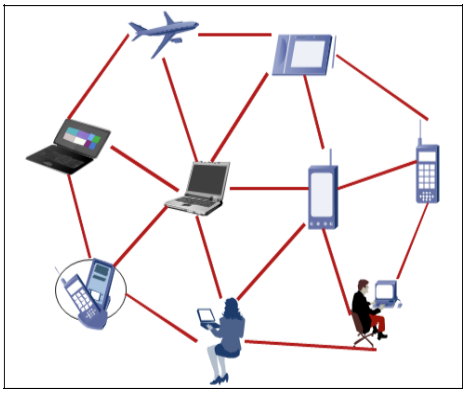

Fig.1. mobile ad-hoc network architecture

II. RELATED WORK

Varshaet.al., AODV protocol changed to detect wormhole attacks (MAODV). Wormhole attacks are identified by counting hops and delays on various pathways from source to destination. It analyses the latency per hop of every node in the usual network with a path under wormhole attack and finds that the wormhole attack path is slower. This approach needs no extra hardware or clock synchronisation. This approach fails when all routes are wormhole-affected [1].

Neetu Gupta/Harleenkaur WSN AODV wormhole protection technology. This work suggested wormhole detection and isolation. [19] The strategy aims to identify wormholes along the path suggested by AODV by employing data trackers to detect wormholes between all conceivable combinations of nodes and make decisions based on each combination. If a wormhole is found in any conceivable combination, the whole recommended route is considered wormhole-affected [2].
SharmaNishant Location-based attack prevention in wireless sensor networks. The suggested approach identifies and inhibits wireless wormhole attacks. The suggested approach leverages node location information and Euclidean Distance Formula to identify and prevent wormhole attacks [3]. Subhaet. Wireless Sensor Network Message Authentication and Wormhole Detection. Proposed system to discover wormhole attacks using RTT [20] between nodes. A malicious node tunnels network messages through a low-latency connection and replays them in another area of the network. Due to wireless transmission, an attacker may establish a wormhole even for packets not intended to him, as he can overhear them and tunnel them to a cooperating attacker [4].

Rakhil R. proposed pre-handshake neighbour finding. A pre handshaking technique analyses neighbouring node actions to prevent collision during data transmission and deliver each packet to the proper recipient without losing. Wormhole attacks are one of WANET's most serious, disrupting network connections. One or more hostile nodes initiate this replay assault. This assault is difficult to defend and simple to execute. This study proposes a new method for neighbour finding and wormhole defence. The suggested method requires no costly hardware or mechanisms on wireless nodes [5].

Parmar Amisha, A method for detecting and preventing wormhole attacks is suggested. AOMDV (Ad hoc On demand Multi path Distance Vector) [21] is a routing system based on RTT (Round Trip Time) and wormhole attack characteristics. The suggested technique appears promising compared to alternative solutions. All simulations utilise NS2 [22] [6].

Patel Manish Dynamic Wireless Sensor Network Wormhole Detection Proposal. They think a malevolent entity can launch wormhole assaults. It launches high-speed, low-latency tunnels. One malicious node captures packets at one point and repeats them to another using an out-of-band tunnel. Malicious nodes don't forward packets. The base station cannot receive any data from the target region. Malicious entity may alter data packets [7].
Patel, Aggarwal Proposed a wormhole detection methodology based on neighbourhood and connectedness. The suggested method can identify wormhole attacks with minimal storage. Proposed approach detects wireless sensor network wormhole attacks. It has excellent storage costs and is relevant to resource-constrained wireless sensor networks [8].

Proposed Modified Hop Count Analysis Algorithm (MHCAA) for Wormhole Attack [24] in WSN. This research tries to identify and prevent wormhole nodes in mobile ad-hoc networks. This work studies wormhole attacks and develops approaches to identify and avoid them using AODV [9].

et al. The whole analysis shows that packages pose security risks and corrupt system execution. To combat weakness, researchers will examine wormhole [24] attacks and infer a component to safeguard flexible systems. Wormhole attacks target system layer guiding conventions. The whole paper considers Ad-hoc On-Demand Routing and its vulnerabilities [10].

Amish, Parmar This study studies tactics for handling wormhole attacks in WSN and proposes a mechanism for detection and countermeasures. This strategy relies on AOMDV (Ad hoc on Interest Multipath Distance Vector) steering convention and wormhole attack features. Compared to previous written arrangements, the suggested technique appears promising. All games use NS2[11].

Supriya Khobragade, etc. In wormhole assault, an aggressor hub stores information packets in one location of the Network and sends them to another far away through tunnelling. Wormhole Attack Prevention and Detection Using Authentication Based Delay per Hop Technique for Wireless Network is the suggested solution. Various system hops and deferrals are used to recognise wormhole attacks. The sender hub recognises both wormhole assaults. Quantitatively, the suggested strategy was approved using an NS2 arrange test system [12].

et al. In this study, we measure the execution of AODV [26] convention. With a changing number of harmful nodes, wormhole attacks are occurring often. A reproduction-based test was done using NS2 [27] to break down system execution based on Throughput, typical End-to-end Delay, and Packet Delivery Function [13].

M. B. M. Kamel et al. suggested STAODV to prevent MANET dark opening attacks. STAODV hubs have trust esteem and vengeful hub tables. Each incoming package has a security value that indicates its health. Predefined limit esteem determines shielded response. The STAODV inspects each RREP[28] parcel with the arrangement number, hub-to-goal leap check, and course response health status. Numerous studies suggest a recognition method using arrangement number. Assailants will foil STAODV by forging course response message [14] grouping numbers.

B.Cerda, The PPP was created to identify dark gap assaults from malicious switches. In PPP, a trusted source hub distributes a phoney information and treatment package. The fake treatment bundle follows a Hamiltonian path and switches. A nasty hub drops a bogus treatment package because it thinks it's a normal data packet. Re-enactment findings showed the PPP can detect harmful nodes. Larger system scales require more fake treatment parcels to find harmful nodes. Last, the scientists didn't compare the PPP setup to current plans [15].

Sharma, The designers suggested the group and notoriety-based CRCMD&R conspiracy. CRCMD&R conspire records the group head's ID after it leaves the originator. In RREP bundle, it stores the hub ID, the hub that transmitted RREP, prime item number, and bunch head ID. Neighbor, authenticity esteem, and notoriety tables are needed in CRCMD&R scheme. Each bunch head in neighbour table has a hub ID and group head ID. In the authenticity esteem table, hub ID, accomplishment tally, and sum are recorded. The credibility gained by a cumulative accomplishment check. The notoriety level table connects indiscriminate mode to bunch heads. The hub's renown is defined by the hub it RREPs. Pernicious, doubtful, less reliable, and dependable are renown levels. Re-enactment findings show CRCMD&R conspire has greater aggregate throughput than AODV. The used techniques are out-of-date compared to the new bunch system [16].

et al. MANET [29][30] [31] is a network of nodes that communicate via the Internet without a central organisation. Due to its open nature and lack of foundation, security is confusing compared to other systems. These systems are vulnerable to many levels of assault. Malevolent nodes might assault the system by listening covertly or interfering dynamically. Wormhole is a high-profile severe assault. It redirects traffic between two end-nodes via a Wormhole burrow and regulates the directing calculation to make distant nodes seem as neighbours. We offer a unique location model that allow a hub to evaluate whether an assumed most constrained path includes a Wormhole burrow. Our strategy hinges on how the Wormhole burrow shortens paths [17].

et al. The remote sensor network gathers sensors that provide data to the base station. As there is no physical connection between sensor and base station, vital data may be sent without wires. The remote sensor arrangement's communication concept poses a security risk to sensitive data. The assailant hub may gather and direct information. Possible system layer assaults. Wormhole is one of these assaults that may affect remote sensor steering technique. In this assault, the attacker hub controls the system's bundle transmission and routes it to nodes. This assault expands package drop and complicates directing. The analyst creates several security approaches to reduce parcel drops and safeguard the system's directing component. Few bundle drop techniques are discussed in this study. Light weight countermeasure for wormhole attack (LITEWORP) based on Dynamic Source routing (DSR) convention security method, Delay per Hop Indication (Delphi) in view of AODV (Avoidance Routing Protocol) [32] Protocol security system and MOBIWORP based on DSR convention security procedure reduce bundle loss rate by 40%, 43%, and 35%, respectively [18].

III. AODV ROUTING PROTOCOL

AODV routing protocol is work on ad hoc network. Its use three parameter first RREQ message which request wide-ranging transmit to every neighbour nodes, second RREQ message which use unicast technique during communication and RERR Route error. Mostly AODV routing protocol routing progression necessity is base on sequence number. This is removing the difficulty of calculation in the

direction of infinity. In fig.2 display the REEQ and RREP message exchange between S & D [4][5].

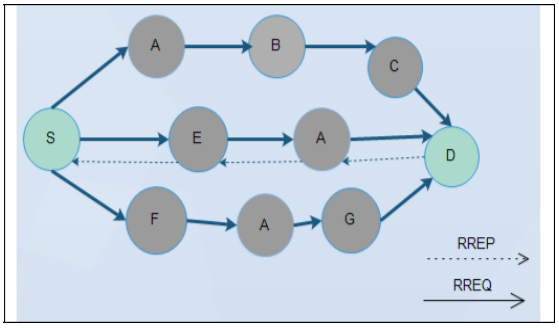

Fig.2 RREQ and RREP message exchange between S & D

IV. WORM HOLE ATTACK

4.1 WORM HOLE ATTACK: - Two malicious node is create a tunnel is called worm hole attack. Means two join together nodes that are far apart are linked by a tunnel giving am is apprehension that they are neighbors. each one of these nodes allow route request and topology manage communication from the network and send it to the other collude node via tunnel which determination then replay it interested in the network starting there. Through by this extra tunnel, these nodes are able to advertise that they have the direct path through them. just the once this link is establish, the attackers may choose each other as multipoint relays, which then lead to an replace of various topology manage messages and data packets through the wormhole tunnel and Worm hole node drop all the packets [4, 5]. Show on fig 3.

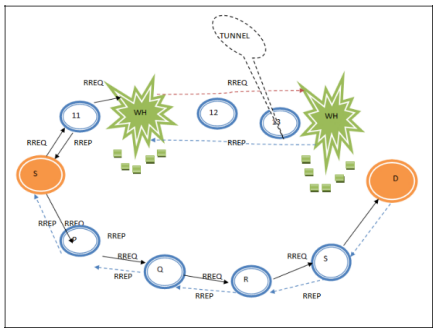

Fig 3 Worm Hole Attack.

4.2 Trusted Aodv Routing Protocol

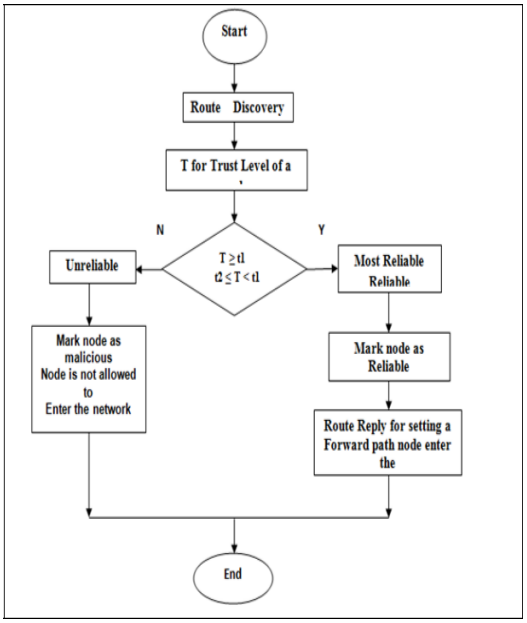

Figure 4. Flow chart for proposed model

Trusted AODV is a trusted routing protocol based on trust model for mobile Ad-hoc network. Trusted AODV has many relevant features like Nodes perform trusted routing behaviors mainly according to the trust relations between them .A node that performs malicious behaviors will finally be detected and denied to the entire network. System routine is improved at every routing hop[5].

1.Trust category of a node

In this work the AODV routing protocol is embedded along with the ***trust function***. The communication between the nodes in the mobile Ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the trust on neighbor and appropriate threshold values the nodes be capable of be categorize in to the subsequent.

I. **Unreliable-** it's having trust value between 0 to 0.5.

II. **Reliable-** it's having trust value between 0.4 to 0.7.

III. Most Reliable- it's having trust value between 0.7 to 1.During the route discovery phase of the AODV Routing protocol, the trust value is also computed for every one the neighbors of some node. The result of trust estimation function is the Trust-status of each and every one of neighbors as Most Reliable, Reliable or Unreliable.

2. Threshold Value of a node

Different threshold values are defined for different type of neighbors to develop into Most Reliable, Reliable and Unreliable. **T***ur*, **T***r* and **T***mr* are the

threshold values for the Unreliable, Reliable and the Most Reliable respectively [5]. We evaluate a Trust estimation function for the calculation of trust value.

$$T = \tanh(R1+R2)$$

Where

Tan h is tangent hyperbolic function, which has value

$$\tanh x = (e^{x} - e^{-x})/(e^{x} + e^{-x})$$

T = Trust value

R1= percentage between the number of packets really forward and number of packets to be forward.

R2 = percentage of number of packets received from a node but originate as of others to total number of packets acknowledged from it. After evaluation Trust value is -1 to +1, but use our propose solution value between 0 to +1.

V. SIMULATION AND RESULT

We perform a simulations base on *NS-2*with extensions for mobile wireless networks. To evaluate the performance of Trusted AODV we have taken following simulation parameters in our simulation.

Simulation Parameters

Simulation Parameters	Value
Number of nodes	34
Network size	1200*1000
Simulation duration	100(Sec)
Initial Energy	100
txpower	0.9
repowers	0.8
Idle power	0.0
Sense power	0.0175
Source node	15
Destination node	13
Collaborative Malaysia's	6
Packet size	1024

CBR source and the total packets received by the CBR sink at the final destination

5.1 End to end Delay:

End to end Delay is the time taken for the packet to travel from source to the destination node. With raise in quantity of malicious nodes, End to end delay of AODV increase. End to end delay of TAODV also increases but is stable with respect to AODV.

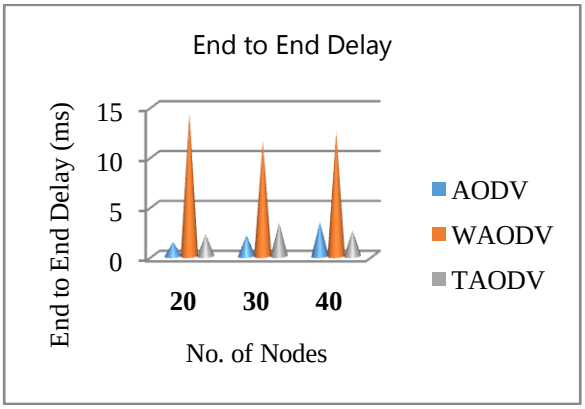

Fig.5 End to End Delay for scenario of wormhole attacks

5.2 Throughputs Throughput is the average rate of winning message delivery over a communication channel.

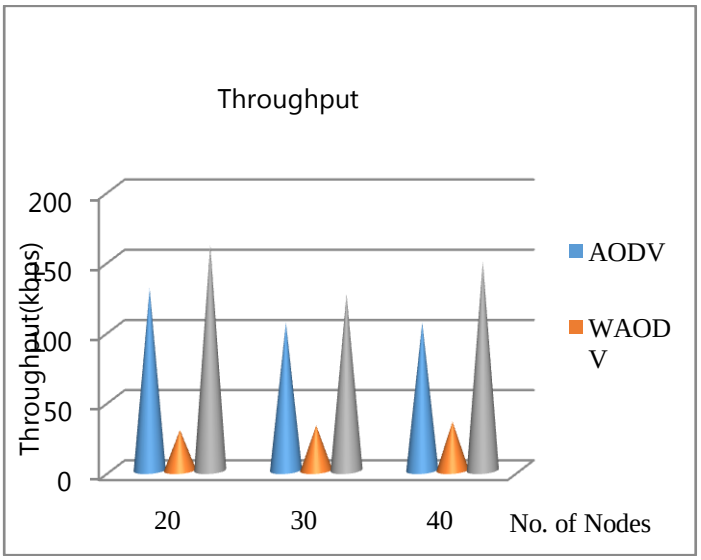

Fig .6 Throughputs for scenario of wormhole attacks

5.3 Packet Delivery Ratio: The ratio between the total packets originated by the "application layer"

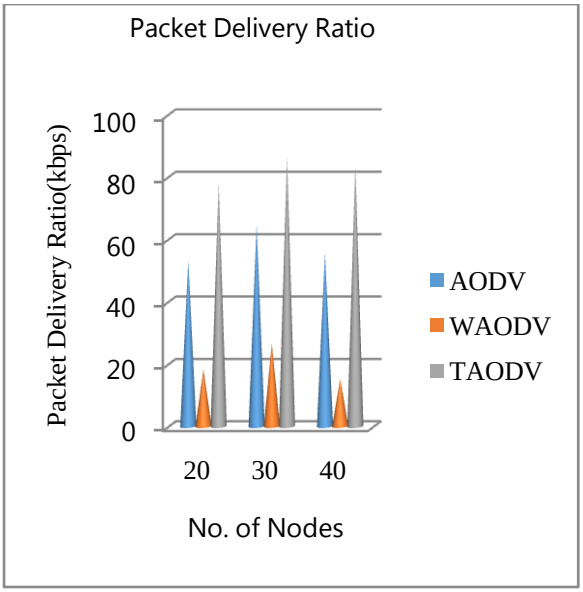

Fig .7 Packet Delivery Ratios for scenario of wormhole attacks

VI. CONCLUSION

In this paper we are discovery following conclusion on NS-2simulation. Like End to end delay of TAODV is better compare to wormhole AODV, Throughput of TAODV is better compare to wormhole attack AODV, by increasing the time an effect in throughput in both the case. Packet delivery ration is better compare to wormhole AODV, when we raise the time packet deliver ratio of together is raise. As shown in fig.5, 6, 7when we want more throughputs, more packet delivery ratio and more end to end delay we use TAODV.

VII. FUTURE WORK

In this paper we have calculate trust value of wormhole by using different parameter and simulate by NS-2 tool. In future we will calculate trust value of other attacks on MANET.

REFERENCES

[1] Umesh kumar chaurasia and Mrs.Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol", IEEE 2013.

[2] Harleen Kaur and Neetu Gupta, "Protecting AODV from Wormhole Attack in WSN" in International Journal of Engineering and Computer Science (IJECS),vol. 3, Page No. 8668-8672, October 2014.

[3] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun 121, 503–526 (2021). https://doi.org/10.1007/s11277-021-08647-1

[4] S Subha and UGowriSankar, "Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network" in IEEE Sponsored 9thInternational Conference on Intelligent Systems and Control (ISCO) 2015.

[5] Rakhil R and Rani Koshy, " An Efficient Algorithm for Neighbour Discovery and Wormhole Attack Detection in WANET" in International Conference on Control, Communication & Computing India(ICCC),November 2015.

[6] ParmarAmisha, V.B.Vaghelab, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol" in 7th International Conference on Communication, Computing and Virtualization(ICCCV) 2016.

[7] ManishM Patel and AkshaiAggarwal, "Two Phase Wormhole Detection Approach for Dynamic Wireless Sensor Networks" in IEEE 2016.

[8] Manish Patel and Dr. AkshaiAggarwal, " Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information" in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 6, No. 1, January 2016.

[9 Mosmi Tiwari, Deepak Sukheja, Amrita, " Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN" in Communications on Applied Electronics(CAE),vol.3,No.3 ,October 2016.

[10] Madhu Sharma , Ashish Jain , "Wormhole Attack in Mobile Ad-hoc Networks" , IEEE , Symposium on Colossal Data Analysis and Networking (CDAN) , 2016 , pp. 1-4.

[11] Parmar Amish,V.B.Vaghela , "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol" , Science Direct , 7th International Conference on Communication, Computing and Virtualization 2016 , pp. 700-701.

[12] Miss. Supriya Khobragade , Prof. Puja Padiya , "Detection and Prevention of Wormhole Attack Based on Delay Per Hop Technique for Wireless Mobile Ad-hoc Network" , International

conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016 , pp. 133-1339.

[13] Pratima Sarkar, Chinmoy Kar, Biswaraj Sen,Kalpana Sharma , "Sensitivity Analysis on AODV with Wormhole Attack" , IEEE , 2nd International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016 , pp. 803-807.

[14] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET," in Proceedings of IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017, pp. 1278-1282.

[15] B. Cerda, E. Martinez-Belmares, and S. Yuan, "Protection from black hole attacks in communication networks," in Proceedings of the International Conference on Security and Management, Las Vegas, NV,2017, pp. 7-11.

[16] S. Sharma and S. Gambhir, "CRCMD&R: cluster and reputation based cooperative malicious node detection & removal scheme in MANETs," in Proceedings of 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 336-340.

[17] M. Rmayti ; Y. Begriche ; R. Khatoun ; L. Khoukhi ; A. Mammeri University of Ottawa, Canada, "Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks" , IEEE, Fourth International Conference on Mobile and Secure Services (MobiSecServ) , March 2018 , pp. 1-6

[18] Surinder Singh and Hardeep Singh Sain , "Security Techniques for Wormhole Attack in Wireless Sensor Networks" , International Journal of Engineering & Technology, Issues 7 , 2018 , pp. 59-62

[19] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[20] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[21] U. Singh, M. Shukla, A. K. Jain, M. Patsariya, R. Itare, and S. Yadav, Trust Based Model for Mobile Ad-Hoc Network in Internet of Things, vol. 98. 2020.

[22] M. Muwel, P. Mishra, M. Samvatsar, U. Singh, and R. Sharma, "Efficient ECGDH algorithm through protected multicast routing protocol in MANETs," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212743.

[23] U. Singh, V. Vankhede, S. Maheshwari, D. Kumar, and N. Solanki, Review of Software Defined Networking: Applications, Challenges and Advantages, vol. 98. 2020.

[24] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[25] A. S. Chouhan, V. Sharma, U. Singh, and R. Sharma, "A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212740.

[26] L. Baghel, P. Mishra, M. Samvatsar, and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212741.

[27] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[28] A. Sharma, D. Bhuriya, and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375688.

[29] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in 2016 Symposium on Colossal

Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570906.

[30] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212719.

[31] D. Wagh, N. Pareek, and U. Singh, "Elimination of internal attacksfor PUMA in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212710.

[32] R. Parihar, A. Jain, and U. Singh, "Support vector machine through detecting packet dropping misbehaving nodes in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212711.