International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5772
***Article Received**: 12 August 2022 **Revised**: 25 September 2022 **Accepted**: 08 October 2022*

AODV (ST_AODV) on MANETs with Path Security and Trust-based Routing

[1]Vijaya Bhaskar .Ch, [2]Dr. D.S.R.Murthy, [3]Dr. V. Kakulapati
[1]Sreenidhi Institute of Science and Technology
Hyderabad, Telangana-501301, India
e-mail: vijayabhaskar.ch@gmail.com
[2]Department of Computer Science, Anurag University,
Hyderabad, Telangana-501301, India
e-mail: dsrmurthy.1406@gmail.com
[3]Sreenidhi Institute of Science and Technology
Hyderabad, Telangana-501301, India
e-mail: vldms@yahoo.com

Abstract—The nodes of the MANET are connected by an autonomous that has no predetermined structure (Mobile ad hoc Network). When a node's proximity to other nodes is maintained dynamically via the use of relying nodes, the MANET network's node-to-node connection is un-trusted because of node mobility. If a node relies on self-resources at any point in time, it runs the risk of acting as a selfish or malicious node, the untrusted selfish or malicious node in the network. An end-to-end routing route that is secure has been presented to enhance the security of the path based on the AODV routing protocol using ST AODV (Secure and Trust ADV). To do this, we must first identify the selfish/malicious nodes in the network and analyse their past activity to determine their current trust levels. A node's stage of belief is indicated by the packet messages it sends. In order to resolve each route, trust must be identified and the path's metadata in RREP must be updated.

Keywords- MANET, AODV, MANET, End to End path Secure

I. INTRODUCTION

The Dynamic Mobility and Infrastructure Fee Network are Ad Hoc Networks. All of the network's nodes stay connected to each other through wireless networks. VANETS (Vehicular Ad Hoc Networks), SPAN (Smart Mobile Phone Ad Hoc Network), MA-NET (Mobile Ad Hoc Networks) and iMANET (Internet-based Ad Hoc Networks) are all types of Ad Hoc networks. [7] MA-NET is a major cause of network swells in Ad Hoc networks. P2P wireless network features and a shared wireless channel [8]. Ad-Hoc, like dispersed acts, has many of the features of ad-hoc. In the multi-Hop routing, the network topology is self-motivated, with independent access points and common medium [9, 10], self, infrastructure-less, dynamic system topology and self-action, and self-administration [11]. Every network has its own set of properties that make it unique.

Finding a middle ground is not the goal in MANET path security; the goal is to secure a route. End-to-end mobile node route message security in MANET must be resolved. Transporting RREP packets through Ad-Hoc networks, which are also within range, is how the communication nodes communicate with one other. RREP packets are sent out by the destination node to its neighbours, who then forward them to the source.

While travelling from its origin to its destination, a packet may encounter a node connection that views it as a harmless piece of data. We let the packet RREP to fall and not range the target in the typical Ad-Hoc manner.

Denial-of-service, wormhole, spying, and black hole attacks are all addressed by Protocol AODV [13] [12, 14]. Black-hole attacks in MANET use a single-hop node to display packets that have been completely transmitted. The broadcasts they own will also have an in-elevation target sequence[15]. Packets will be discarded at that point.

MANET has three different types of routing protocols [16]. AODV, DSR [17, 18] are examples of reactive routing, whereas OLSR, DSDV [19, 20] are examples of proactive routing, group the characteristics of routing is hybrid protocols they are ZRP [21].

We are using the reactive routing protocols AODV is used. For the ST AODV routing protocol, the proposed work is to design a safe and trust-based AODV rotting to minimise the security of the route from escaping malicious nodes in an Ad-Hoc network. All nodes in the RREP packet compute a safety position value for arriving sequins direction and disconnect malicious nodes from the network if the dangerous route node packet identifies the safety and trust level of the source node.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5772
***Article Received**: 12 August 2022 **Revised**: 25 September 2022 **Accepted**: 08 October 2022*

The paper's road map is discussed in section 2, the existing work. Section 3 proposed a method of detection and prevention of path. Section 4 the simulation results and analysis.

II. Literature Survey

Path failure detection and prevention, but safe and trust-based association for all nodes is recommended. The innovative routing is unaffected by any of the offered methods. To catch rogue nodes, Marti [22] suggests using a watchdog or path score. Certificate-based node snooping is used in this source to verify that the next hop node has been des patched. Nodes are harmful if they have not been sent at a predetermined interval.

A lot more effort is required for this strategy. An approach is defined by Tan and Kim [15] as the identification of a safe path to the AODV protocol. For small, moderate, and exceptional surrounds they mention six percent, four percent and two percent of the sequence no. in a single sentence. This strategy, which used a longer sequence to look for the node, succeeded in isolating it.

The speed of the routing protocol was further impacted by the addition of more fields and tables to attempt. Also, it needs extra bandwidth and buffers for performance, leading to overhead problems. Banerjee's [23] method uses two messages called intro, and the epilogue is sent to inform to receiver node transmission information from the start, at the end node informs to postlude message. The author Tamilselvan, Sankaranarayanan ensures the projected set of rules contains a table for gathering RREP table, the arrival time, and sequence number of any inwards packet [24]. Depending on the transition, the path is chosen dynamically among the paths in the path table.

Hybrid technology modifies routing protocol and trust relationships to form the path in secure end-to-end communication. Routing overhead and maintaining routing tables are the key drawbacks of these systems. Reliable AODV was suggested by the [25] writers Jhaveri, Patel, and Jinwala. They added several tables to the RREQ and RREP packet files and then modified them. As soon as a malicious node was discovered, a malicious node-list table informed RREQ and RREP, and the RREP packet replay node was used as an infiltrator for the harmful node list. Our network can be protected against rogue nodes thanks to this. The updated version was submitted by the author Jhaveri [26], who eliminated the Do-not-consider option, which causes node misbehaviors' to stop forwarding RREP to other nodes, hence reducing routing.

III. Proposed Methodology

A. ST AODV Route-Reply-Mechanism

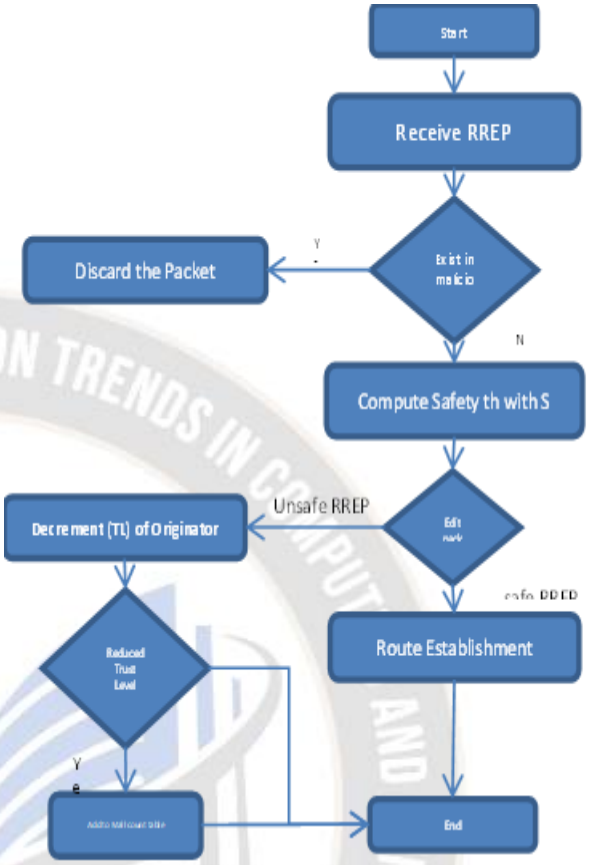

Fig. 1 depicts the ST AODV Route-Reply-Mechanism.

Let's put a Pi node in place (in this manner): pa I Pa in any location This is the set of Take part nodes in the network, with Pa= p1, p2, p3, pN" and N being the number of a take part node that is i= p1, 2, 3... N. Tables for each node's Trust Level (TL) and Mischievous Nodes (MN) are available. The trust level of the TL network is maintained by each node.

The value will be changed to reflect the arrival of new route responses after all nodes have been trusted. The safety S of each received response was then computed, and the threshold had to be established. The T value is calculated using (1).

$$T = \frac{1}{N}\sum_{i=1}^{N}\left(RpSNo_{pi} - CtSNo_{pi}\right) \qquad (1)$$

Nodes in the N(p) routing table have a total count of N. RpSNo and CtSNo are found in the destination node(s). Node-i, node-p routing table is the current Seq-number for an endpoint. An additional consideration in the choice of a route is a node's hop count and Seq number to the destination. the number of sequences and hops is derived from where the primary path will take. In the MN table, every route response will be reviewed. The route is deleted since the reply route node is in the MN table. S value will be computed if it is not inspected in each RREP otherwise (3).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5772
***Article Received**: 12 August 2022 **Revised**: 25 September 2022 **Accepted**: 08 October 2022*

$$\Delta Seq = RpSNo_{pi} - CtSNo_{pi} \quad (2)$$

$$S = \Delta Seq - \alpha T \quad (3)$$

The safety of the next node will be calculated (4) using the S value (3). The barrier that protects the passage is in place.

If S >0 unsafe RREP
If S <=0, Safe RREP (4)

The TL cost of a node will be reduced by one if RREP has security problems. – The impact of the node in the MT routing table is driven by the TL assessment node.

If the Route Reply-RREP value is safe, the threshold cost must be raised by averaging the biased changes to the CtSNo and Seq-no values in the routing table (5).

$$T = (T_{old} \ X \ N_{seq}) + \Delta_{Seq} \ / \ N_{seq} + 1 \quad (5)$$

The CtSNo routing table is a feature of RREP packets that have been bluffed; the Nseq is unchanged. The routing database maintains a match for each incoming RREP with the one that was deposited. In order to identify conventional safety information, CtSNo of the incoming value difference and routing value difference between info is used. CtSNo is added to the routing table as a new field if there is no information about the endpoint. Without the malicious DST-seq-no being added to the routing table, any RREP may be checked for valuable information using (6) instead of (3).

$$S = RpSNo_{pi} - \alpha T \quad (6)$$

IV. Results and Discussion

A. *Simulation Parameters*

NS2.35 is used in the simulation, which has an area of 800 × 800 metres and 25 nodes. A random waypoint model is also utilized in the simulation. Simulator environment settings are shown in the Table:

TABLE: Network SIMULATIONPARAMETERS

A malicious node uses a fraudulent RREP packet to keep track of the number of hops, while the fictitious destination sequence number is chosen at random from 30 to 90.

Parameters	Value
Simulator	NS2 (ver2.35)
Simulation Time	100s
Simulation Area	800m x 800m
Number of Nodes	25
Transmission Range	250m
MAC Protocol	IEEE 802.11
Routing Protocol	AODV
Traffic Type	CBR
Number of Sources	12
Number of Destinations	12
Number of Malicious Nodes	1 to 4
Data Payload	512 bytes

B. *Simulation Results with Analysis*

Packet delivery ratios (PDR), latency from the end to the beginning, and throughput have all been suggested as measures of network performance [28]. Packets received by the end node are counted as part of the PDR success full packet delivery ratio between sources and destinations.

No selfish/malicious network node means that PDR is at its highest compared to an existing network with such nodes. PDR, AODV and ST AODV are equal if malicious nodes in the network drop packets in the ratio of 25 percent and 0 percent, respectively, when there are one and three selfish/malicious nodes in the network. ST AODV's PR ranged from 98 percent to 97 percent for this time period.

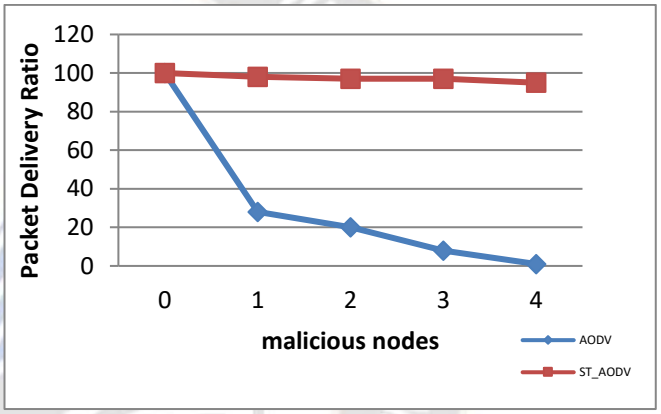

Fig. 2. PDR of AODV and STAODV

The rate at which successful bits are sent each second is known as throughput. As can be seen in Figure 3, the throughput of AODV and ST AODV in different circumstances is shown. There were no self-centered or malicious nodes in the AODV or ST AODV in the typical situation.

The malicious nodes discard the packets and forward them. The throughput was dropped to 180bps and 80bps with 3 and 4 selfish/malicious nodes, while the ST AODV is between 99.5 and 98 kbps.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5772
***Article Received**: 12 August 2022 **Revised**: 25 September 2022 **Accepted**: 08 October 2022*

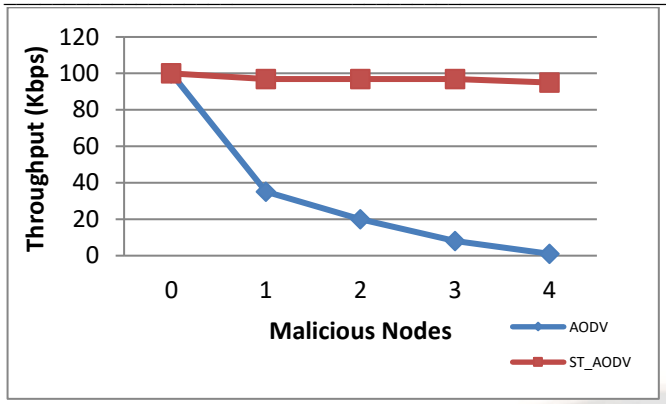

Fig. 3. Throughput of AODV and STAODV

Routing, protocol, and number of nodes may all affect the delay of packets from point A to point B. AODV with ST AODV is shown in Figure 4 as an End-2-End Delay.

Our goal is to find route-replay RREPs sent by nodes that take a different route to their destination in ST AODV and separate selfish or malicious node RREPs. Delays of up to 140 ms are possible depending on the RREP and sequence number of selfish or malicious nodes. RREP packet transmissions are seeing an increase in end-to-end latency as a result.

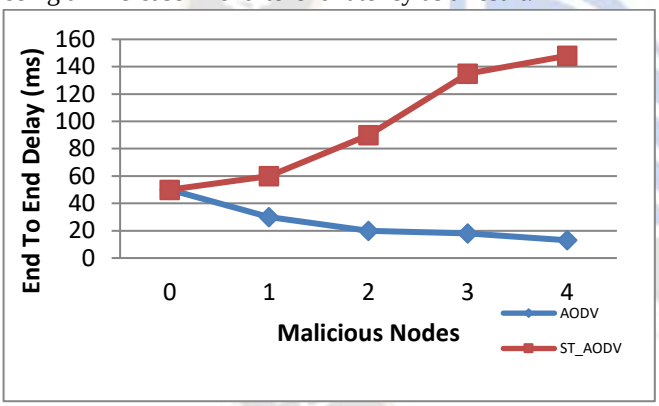

Fig. 4. End to End Delay of AODV and STAODV

In order to maintain contemporary routing between nodes, the protocol may use the steering network overhead, unicasted packets, and extra broadcasted packets. The total number of extra packets sent over a network is what's known as the "normalised routing overhead." Selfish or malicious nodes may have an impact on AODV, as seen in figure 5. The ST AODV is stable in the presence of malevolent or selfish nodes if the routing overhead is normalised.

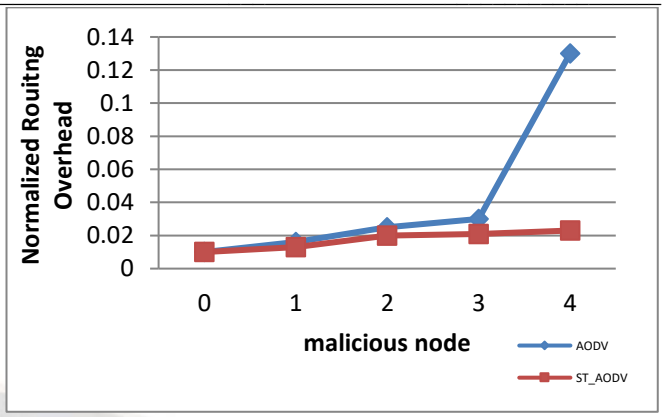

Fig.5. Normalized Routing Overhead of AODV and STAODV

V. Conclusion

Assuming that every node in the network of the RREP packet is trustworthy, a safe and trust-based technique is too local from end to end to end to secure the route. End-to-end latency and throughput rise as time lapse reduces in ST AODV.

References

[1] Vijaya Bhaskar Ch, Dr. D S R Murthy, "A path Recovery AODV optimistic Secure Route Reply Protocol in Ad Hoc Mobile Networks," International Journal of Emerging Technologies and Innovative Research www.jetir.org (ISSN-2349-5162), © 2020 JETIR October 2020, Volume 7, Issue 10, DOI: http://doi.one/10.1729/Journal.24671, Impact Factor: 5.87, ISSN: 2349-5162. http://www.jetir.org/view?paper=JETIR2010063.

[2] K. Cheng, "Smart Phone for Mobile Communication Community," International Journal of e-Education, e-Business, e-Management and e-Learning, vol. 3, no. 5, 2013.

[3] Y. Mao, J. Wang, B. Sheng, F. Wu, "Building smartphone Ad-Hoc networks with long-range radios" In 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), pp. 1-8, 2015.

[4] M. Corson, J. Macker, G. Cirincione, "Internet-based mobile ad hoc networking", IEEE internet computing, vol. 3, no. 4, pp. 63-70., 1999.

[5] X. Fan, J. Cao, Y. Liu, Y. He, "Gossip-based Cooperative Caching for Mobile Phone Games in IMANETs," In Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th International Conference, pp. 465-472, 2011.

[6] S. Lim, W. Lee, G. Cao, C. Das, "Cache invalidation strategies for internet-based mobile ad hoc networks," Computer Communications, vol. 30, no. 8, pp. 1854-1869, 2007.

[7] Vijaya Bhaskar Ch, D.S.R. Murthy," Qos Metrics for an end to end Stable Routing in MANET," International Journal of Computer Sciences and Engineering, Vol.6, Issue.12, pp.57-61,Dec-2018,CrossRef-DOI: https://doi.org/10.26438/ijcse/v6i12.5761, E-ISSN: 2347-

2693.https://www.ijcseonline.org/full_paper_view.php?paper_id=3293.

[8] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE wireless communications, vol. 11, no. 1, pp. 38-47, 2004.

[9] M. Alani, "MANET security: A survey. In Control System", Computing and Engineering (ICCSCE), 2014 IEEE International Conference on, pp. 559-564, 2014.

[10] D. Aarti, "Study Of Manet: Characteristics, challenges, application and security attacks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 252-257, 2013.

[11] J. Hoebeke, I. Moerman, B. Dhoedt, P. Demeester, "An overview of mobile ad hoc networks: applications and challenges", Journal- Communications Network, vol. 3, no. 3, pp. 60-66, 2004.

[12] Vijaya Bhaskar.ch, Dr. D.S.R.Murthy, " A reliable Routing Approach in Mobile AdHoc Network based on genetic Algorithms" International Journal of Research in Computer and Communication Technology, (IJRCCT) ISSN(o) 2278-5841, ISSN(P) 2320-5156, www.IJRCCT.org, Vol 2, Issue 10, October- 2013, SJIF impact factor 3.751. Corpus ID: 2427122.

[13] S. Umang, B. Reddy, M. Hoda, "Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption," IET Communications, vol. 4, no. 17, pp. 2084-2094, 2010.

[14] N. Arya, U. Singh, S. Singh, "Detecting and avoiding of wormhole attack and collaborative black hole attack on MANET using trusted AODV routing algorithm," IEEE International Conference on Computer Communication and Control, IC4 2015, pp. 6–11, 2015.

[15] S. Tan, K. Kim, "Secure route discovery for preventing black hole attacks on AODV-based MANETs," Proceedings - 2013 IEEE International Conference on High-Performance Computing and Communications, HPCC 2013 and 2013 IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2013, pp. 1159–1164, 2014.

[16] I. Ullah, S. Rehman, "Analysis of Black Hole attack on MANETs Using different MANET routing protocols," 2010.

[17] R. Glabbeek, P. Höfner, M. Portmann, W. Tan, "Modelling and verifying the AODV routing protocol," Distributed Computing, vol. 29, no. 4, pp. 279–315, 2016.

[18] I. Woungang, S. Dhurandher, M. Ge, R. Peddi, "A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," Security and Communication Networks, 2013.

[19] V. Singla, P. Kakkar, S. Lecturer, "Traffic Pattern-based performance comparison of Reactive and Proactive protocols of Mobile Ad-hoc Networks," International Journal of Computer Applications, vol. 5, no. 10, pp. 975–8887, 2010.

[20] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks," IEEE International Multi-Topic Conference, Lahore, Pakistan, pp. 28-30, 2001.

[21] A. Khatkar, Y. Singh, "Performance Evaluation of Hybrid Routing Protocols in Mobile Ad Hoc Networks," 2012 Second International Conference on Advanced Computing & Communication Technologies, pp. 542–545, 2012.

[22] S. Marti, T. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.

[23] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," World Congress proceedings on engineering and computer science, pp. 22-24, 2008.

[24] L. Tamilselvan, V. Sankaranarayanan., "Prevention of black hole attack in MANET," The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications IEEE, p. 21, 2007.

[25] R. Jhaveri, S. Patel, D. Jinwala, "Improving route discovery for AODV to prevent black hole and gray hole attacks in MANETs," INFOCOMP Journal of Computer Science, vol. 11, no. 1, pp. 1-12., 2012.

[26] R. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs," IEEE Third International Conference on Advanced Computing & Communication Technologies, pp. 254-260, 2013.

[27] C. Bettstetter, H. Hartenstein, X. Pérez-Costa, "Stochastic properties of the random waypoint mobility model," Wireless Networks, vol. 10, no. 5, pp. 555-567., 2004.

[28] R. Jain, "The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling," John Wiley & Sons, 1990.

[29] Vijaya Bhaskar ch, Dr. D.S.R.Murthy, "Create Communication Model For Manet Routing Protocol" - Make in India – A new initiative for IT and Business Excellence –October 27-28, 2016, SNIST.

[30] Vijaya Bhaskar Ch, Dr. D.S.R.Murthy, Dr. V. Kakulapati, "Alternative Reliable routing for Reactive based routing used on recovery management in AODV route optimistic properties." Proceedings of the 12th INDIACom; INDIACom-2018; IEEE Conference ID: 42835 2018 © INDIACom-2018; ISSN 0973-7529; ISBN 978-93-80544-28-1. IEEE Conference ID: 42835.

[31] P. Goyal, V. Parmar, R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," IJCEM International Journal of Computational Engineering & Management, vol. 11, pp. 32-37, 2011.

[32] X. Liu, Z. Fang, L. Shi, "Securing Vehicular Ad Hoc Networks. 2007 2nd International Conference on Pervasive Computing and Applications, vol. 15, no. 1, pp. 424–429, 2007

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5772
Article Received: 12 August 2022 Revised: 25 September 2022 Accepted: 08 October 2022

[33] F. Tseng, L. Chou, H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences, vol. 1, no. 1, 2011.

learning and depression discrimination." IEEE Access 8 (2020): 30332-30342.