Performance Evaluation of Routing Protocol Under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms

Swapnil S. Bhalsagar, Manish D. Chawhan, Yogesh Suryawanshi, V. K. Taksande

Abstract: The Mobile Ad-hoc network (MANET) is the most widely used type among all Wireless Ad-hoc networks where the number of moving nodes connecting to each other is not fixed. There is no central management system in MANET. Protocols are designed as per the node handling capacity in proper way by using multi-hop network topology. Sometimes the protocols fail to communicate due to the presence of an external attacking (malicious) node such as Black hole (BH), Gray hole (GH), etc.. This may cause a great loss of valuable data. Therefore, routing security is a major concern now a days. To properly secure routing, changes has to be made in the routing protocols continuously. In this paper, an overview of some conventional protocols such as AODV, DSDV and DSR protocols is given. Different types of malicious attacks such as Black hole, Gray hole, Jellyfish and Wormhole Attack are studied. In this paper, how trust based scheme will help in overcoming the adverse effects due to the presence of malicious nodes is given. The trust based schemes are introduced in a protocol in order to avoid addition of a malicious node in the route by assigning it a trust value. Also a comparative analysis has been done between the preventive Trust Based Protocols that ensure high security and minimize the effects of these malicious attacks. The DSR protocol under Black hole attack is implemented and the performance is analysed with respect to Packet Delivery Ratio, Throughput, Number of Received Packets and Average End-to-end Delay. The improvement in these factors of a protocol will make it more secure and reliable. Thus, it will be applicable to be employed in the fields where security is of utmost importance.

Keywords: MANET, AODV, Routing attack, ESCT, TDSR

I. INTRODUCTION

Recent generation is witnessing an advanced and dynamic form of communication with continuous research in advancement. The Mobile Ad-hoc network (MANET) plays a key role in this advancement of worldwide communication. MANET employs moving (mobile) nodes as its basic elements. Each mobile node has a capability to form its own central management system.

Manuscript published on 30 March 2019.
*****Correspondence Author(s)

Swapnil SunilraoBhalsagar , B. Engg. Electronics and Telecommunication , Rajiv Gandhi College of Engineering and Research, Nagpur Nagpur University, M.tech. Communication Engineering , Department of Electronics and Telecommunication Engineering, YeshwantraoChavan College of Engineering, Nagpur.

Manish D. Chawhan, Associate Professor Yashwantrao Chavan College of Engineering, Electronics & Telecommunication Engineering, Nagpur. BE and M-TECH YCCE, Nagpur, PhD Electronics Engineering , Nagpur University.

Yogesh Suryawanshi, Assistant Professor Yashwantrao Chavan College of Engineering, Electronics Engineering, Nagpur. M-TECH GHRCE, Nagpur. PhD Electronics Engineering Nagpur University.

V. K. Taksande, Head of the Department in Priyadarshini College of Engineering, Electronics & Telecommunication Engineering, Nagpur. BE from N.I.T. Durgapur (W.B.) and M-TECH from YCCE, Nagpur. PhD in Electronics Engineering from Nagpur University.

In MANET, the network management is transparent to the user i.e. the mobile terminals can actively connect or leave the network as per its convenience. These terminals are also capable of sharing resources with each other by forming their own spontaneous ad-hoc network up to a limited range. Due to the presence of multiple users or large number of nodes, it becomes necessary that each node should recognize every other node of concern. To establish connection with a particular node the source node finds the shortest path to that node. If this shortest path is through other node in between, they are connected by hopping (or multi-hop if there are many number of nodes in between) scheme i.e. the nodes in between help the two nodes to connect with each other and maintain the connection. For the establishment of a secure connection, the nodes must follow same routing protocol. The routing protocols are basically the sets of certain rules that must be followed by the nodes to establish a convenient connection. Due to the wireless structure, MANET is prone to malicious node attacks which may lead to packet drops. Therefore, the routing protocol should provide high security. So, we will also discuss the type of malicious attacks and compare their effects on various performance factors before and after attack and also see the preventive measures already used to avoid these attacks.

II. LITERATURE SURVEY

A. *Conventional MANET Protocols[4]:*

i. *Ad Hoc on Demand Distance Vector (AODV):*

In AODV protocol, the route to the destination node is established only when the source node will demand it. That is why it is called as an on demand protocol. When the source have data to send towards the destination node, it searches for the shortest route leading to the destination node (minimum number of hops). Once the connection is established, the route is maintained till the data is sent completely. A single node can also form trees with multiple destination nodes in case of multicast routing. It uses sequence number allotted to each routing node to count the hops. The route request message initiated by the source node is received by its neighbors and then they again broadcast it by adding the hop count thus creating a series of temporary routes. By the time the destination node receives this message for the first time, it is obviously through the shortest route. The destination node will store the route information in the packet and will send it back to the source node via the same temporary route. So now this route will be used by the source for data transmission and all the other routes will be discarded. If a link breaks then a routing error message is passed back to the source node and the process is repeated.

i. Destination-Sequenced Distance-VectorsRouting (DSDV)

DSDV make use of sequence number for each entry in the routing table to solve this flaw of routing loop in Bellman-Ford Algorithm. The sequence number is an even number if the link is present and odd if the link is absent. Usually the destination node generates these sequence numbers and are sent by the generators along with the next update. The routing information is updated in small increments.

ii. Dynamic Source Routing (DSR)

DSR is one of the most important on demand type of protocol. It operates in two phases:

i. Route Discovery and

ii. Route Maintenance

In the first phase, the source node broadcasts a route request message which contains the packet's unique id and source and destination's ID. As the nodes near the source will receive this packet, they will update their ID in it and again broadcast it. The source will identify the packet by its unique id and realize that it is not from the destination node then it will discard it. In this way, all the nodes in between source and destination will update their IDs' and by the time the packet reaches the destination node, it contains the complete path. The destination will send reply through the same route and then the source will establish the connection.

Second phase is executed when the link is broken. DSR is called dynamic because it consistently broadcasts the request message at predefined intervals.

The detailed comparison between these three protocols is given in reference paper no. 4.

The performance of AODV is the best in case if the ability to maintain connection is considered. AODV and DSR perform better than the DSDV as far as Throughput is concerned, for large no. of nodes AODV is a better option whereas DSR is acceptable for smaller no. of nodes. DSDV has minimum average delay for any no. of nodes. In this paper the analysis of these protocols is given. The aim is to evaluate security issues in DSR, study various attack patterns and modify the existing protocol in order to limit those attacks.

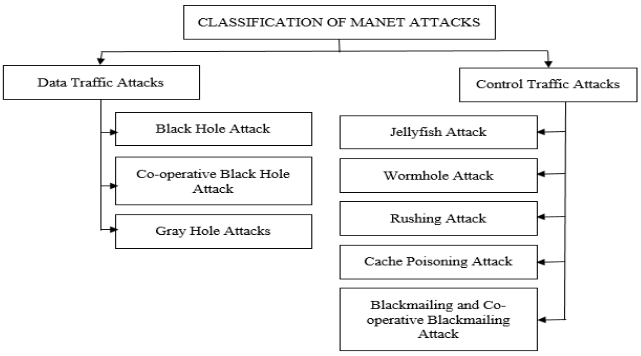

Figure 1: MANET attacks Classification

B. Classification of attacks:

Depending upon the common characteristics and attack targets, the MANET attacks are mainly classified as data and control traffic attacks [6][7]. For example, the Black Hole attack drops data packets. Therefore, it is included in Data traffic attack.

i. Data Traffic Attack:

This type of attack mainly targets the data packets. The attacking node either drops the data packet or delays it before forwarding. This leads to a rise in end-to-end delay and number of packets dropped. Which ultimately disturb the quality of service.

A) Black-Hole Attack: A black hole is a high density body in space, near which all kind of mass and matter disappear. A node can also behave in such manner. This type of node claims that it has the shortest path towards the destination, invites the data packet from the source and drops it silently just like a black hole. When there are many such nodes present in the network, the attack is termed as co-operative black hole attack. This type of attack harms the network at a greater extent. The black hole attack is further classified as

i. Active Black hole attack and

ii. Passive Black hole attack

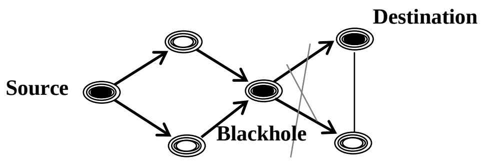

Figure 2: Black-Hole Attack

In Active type, the node drops all the data packets passing through it, whereas in passive type, it helps in forwarding some selected packets towards the destination. A connecting node effectively separates the network into two separate networks.

Here the attacking Black-Hole node is separating the network into two parts.

B) Gray-Hole Attack: Gray-Hole attack either drops the data or forwards them. It generally adapts the following two most common type of behaviour:

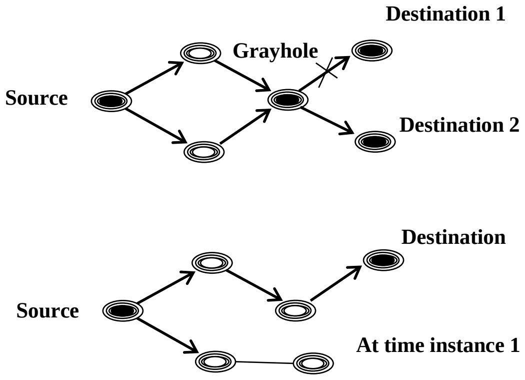

Figure 3: Node-dependent Grayhole attack

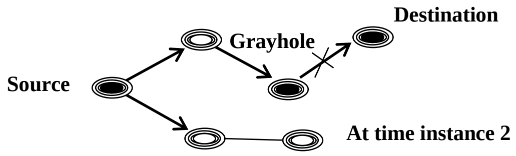

Figure 4: Time-dependent Grayhole attack

(i) Node dependent attack: This type of attack drops information to or from victim nodes in between the path (fig 3 and for non-victims it normally routes the data.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

(ii) Time dependent attack: In this type of attack data packets are dropped depending on some fixed trigger time and when there is no trigger, it forwards the data. (figure. 4)

Detection of this kind of behaviour is arduous. It requires an extensive detection algorithm. The method is similar to that of Passive Black-Hole attack where the presence of Gray-Hole attack might be detected by the feedback of sequence number. If there are many paths between sending and receiving nodes then queued packets may find out active Gray-Hole attack in action.

iii. Control Traffic Attacks:

The primary aim of this type of attack is to manipulate the flow of data packets. It concerns with delay and packets alignment. Thus it affects the control of the protocol over the packet flow. Following are the examples of this type of attack:

a) Worm Hole Attack: The term ‘Worm-hole’ is described as a bridge that connects two physically separated points in space. In the same way in MANET also a malicious node can short circuit the network and disturb the usual flow of packets. If this link claims to have shortest path then this link will be the first choice while sending data. Here the malicious node is capable of monitoring the traffic and also disrupt the flow of packets. In figure 5, the attack is being performed by X and Y.

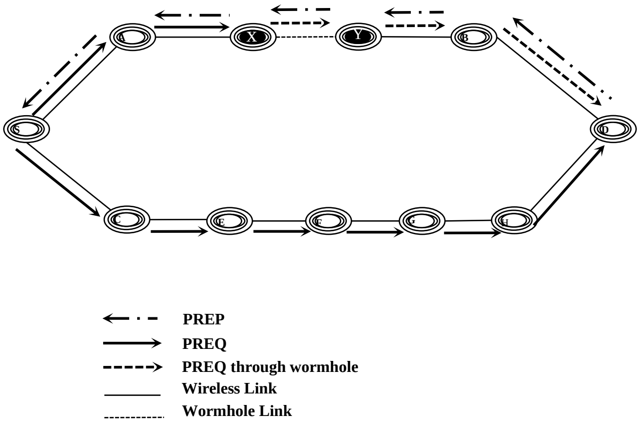

Figure 5: Worm-Hole attack

b) Jellyfish Attack: Unlike the BH and GH attacks, in Jelly-fish attack, some targeted packets are rather delayed than dropped. This leads to random reception of data. The usual sequence of data is disturbed and thus the QoS is affected badly.

III. TRUST BASED SECURITY ENHANCED PROTOCOLS TO MINIMIZE VARIOUS ATTACKS

In trust based scheme, every node in the network maintains a trust table which records the routing history of its neighbour and depending on this history, the node decides whether its neighbour is malicious or benign. Once the node is aware of the behaviour of its neighbour, it will establish the route as per the trust table.

In a trust based scheme if a node is found malicious, its neighbouring nodes will not forward any data to it and it will be avoided while selecting route. A route that doesn’t include the malicious node will be selected.

A. Evolutionary Self-Cooperative Trust Scheme (ESCT)[1][11][12][13]:

The ESCT is a high security protocol over other conventional routing protocols. The mechanism comprises of two stages of detection. During the first stage, every node in the network executes self-detection which evaluates the trust levels of other nodes independently. During the second stage, the self-detection results are shared by each node with their direct neighbours. This helps the peers to execute the co-operative detection to acquire more trust information about the network. The trust information in self-detection results are of utmost importance for the nodes. This information determine the attitude of a particular node towards the network and also affects its decision.

ESCT comprises of the following features:

1) In ESCT, the mobility helps in enhancement of security.

2) The protocol is easy to apply.

3) The trust information is exchanged with the help of direct neighbours at some intervals. But the final trust level (Benign or Malicious) is assigned with the help of no. of voting nodes as well as the attitude of that node.

4) The results of self-detection are trusted more than co-operative efforts.

ESCT acquires trust information in two stages of detection from the neighbouring nodes and compares it with a particular threshold value to distinguish between the benign and malicious node.

B. Trust Based Dynamic Source Routing (TDSR or TBDSR)[3][10]:

The TBDSR Protocol is a trust based modification of the existing standard DSR protocol. With the help of the neighbouring nodes it finds a secure route mainly free of black hole attackers.

IV. COMPARATIVE ANALYSIS

ESCT makes use of human nature to enhance the performance and ensure undisrupted routing in MANETs. It is based on following 3 processes:

1) Self Detection: Thismechanism uses the mobility of device to perform trust analysis. Each node assigns some trust value to its neighbours. This value is later used for reference.

2) Co-operative Detection: The cooperative detection mechanism further improves the performance and also improves the robustness of ESCT. In co-operative detection, two processes occur simultaneously. On one hand, the trust evaluation process is boosted and the remaining trust information is acquired. On the other hand, a voting concept implemented which restricts the increase in the trust value of malicious peers by making use of most benign nodes present in the network. This improves the network performance.

3) In third step, the protocol allows all the nodes to explore different networks in order to tackle the effect of irrelevant information given by the attacking nodes and automatically correct themselves.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

ESCT can improve the Packet Delivery Ratio by more than 90% as compared to DSR in the presence of any type of attack.

No. of Attackers	DSR	ESCT	TDSR	Self-Detection
0	0.98	0.98	0.97	0.98
5	0.59	0.85	0.7	0.62
10	0.49	0.77	0.59	0.52
15	0.35	0.68	0.5	0.45
20	0.29	0.59	0.46	0.4

Table 1: No. of Packets Vs. Packet Delivery Ratio [1]

No. of Attackers	DSR	ESCT	TDSR	Self-Detection
0	0.13	0.14	0.148	0.13
5	0.11	0.15	0.136	0.12
10	0.09	0.155	0.136	0.09
15	0.08	0.2	0.136	0.075
20	0.07	0.21	0.9	0.075

Table 2: No. of Packets Vs. End-to-end delay [1]

In TBDSR [14] protocol, the route is completely secured and found to be repelling the BH nodes. Any BH node, trying to drop the packets, is effectively singled out. There is 42% rise in the PDR as compared to DSR and also 37 % less packet loss rate if observed than DSR. The TBDSR has more merits compared to other related works

V. RESULTS AND ANALYSIS

The network scenario of MANET is made in Network Simulator 2 as shown in figure 6 with the all the parameters as shown in table 4.

A. *Network Scenario:*

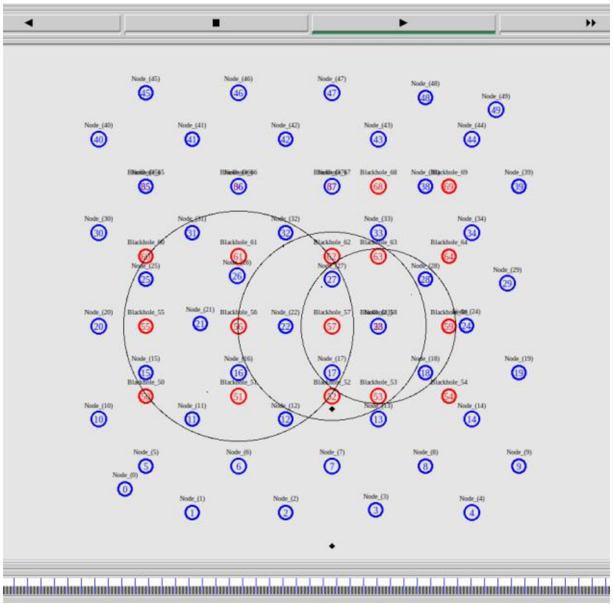

Figure 6: Network Scenario

Then etwork scenario in figure 7 has 70 mobile nodes out of which 20 nodes are malicious black hole nodes. The mobile nodes are moving with different velocities ranging from 1 to 20 m/s. The queue size used is of 20 packets in length. The results and analysis are when routing protocol **DSR** is used in the network.

All the parameters used in the network scenario are as shown in table 3.

Parameter	Value
Total No. of Nodes	70
Default No. of Attackers	20
Routing Protocol	DSR
Sending node(s)	1 to 25
Receiving node(s)	26 to 50
Simulation Area	1000x1000m
Default Maximum Speed	20 m/s
Transmission Range	250 m
Default Traffic Flow pair no.	25
Packet Length	512 bytes
Traffic type	CBR (UDP)
Queue size	20 Packets
Simulation Time	500 sec
Request Frequency	1 sec
Initial Placement	At uniform distance
Movement	Random

Table 3: Network Parameters

B. *Packet Delivery Ratio Vs. Number of Attackers:*

The number of attackers is increased by 5 progressively till the number reaches 20. From the graph of Packet Delivery Ratio Vs. Number of Attackers, it is been analysed that the Packet Delivery Ratio is decreased by 8 to 9% when the number of attackers is increased by 5.

In the absence of attacker, the packet delivery ratio recorded was 97.0143%. When there are 20 attackers the packet delivery ratio is 66.7239%. There is a drop of 30.29% in the presence of 20 attackers.

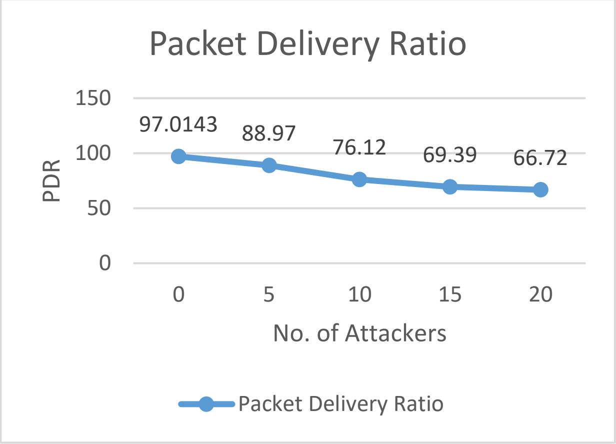

Figure 7: No. of Attackers Vs. PDR

C. Throughput Vs. Number of Attackers:

The graph associated with Throughput Vs. No. of Attackers show that the throughput which is the received data bits per second is decreased by around 100 to 400 Kbps progressively. When there are no attackers the throughput observed is 3035.7874 Kbps. When the no. of attackers is 20, the throughput is observed to be 2088.3253 Kbps. There is a drop of 947.4639 Kbps or 31.2% of throughput in the presence of 20 attackers.

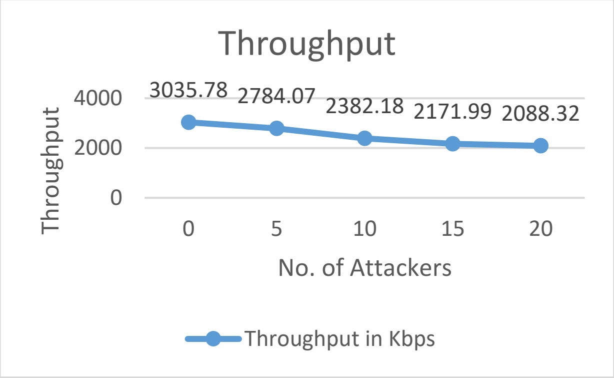

Figure 8: No. of Packets Vs. Throughput

D. Number of Packets Received Vs. Number of Attackers:

From the graph of Packets Received Vs. Number of Attackers, it is been analysed that when the number of attackers is increased by 5 progressively, the number of packets received is decreased by around 800 to 1500. The number of packets received are decreased by 3703 in the presence of 20 attacking nodes. Therefore the packets received are decreased by around 31.22%.

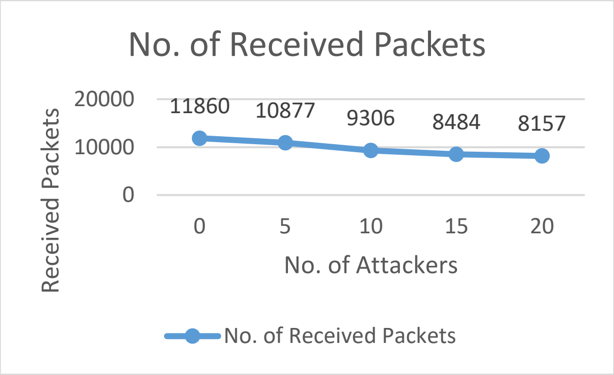

Figure 9: No. of Received Packets Vs. No. of Attackers

E. Average Delay Vs. Number of Attackers:

From the analysis of graph associated with Average Delay Vs. No. of Attackers, it can be observed that the average delay decreases as the number of received packets is decreased when the no. of attackers is increased by 5 progressively. So large number of packets are dropped as we go on increasing the number of attackers by 5. Hence less number of packets are routed and received at destination. So the required amount of delay goes on decreasing for less amount of packets received.

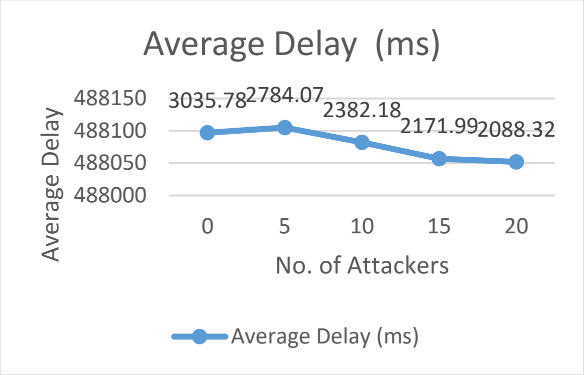

Figure 10: Average Delay Vs. No. of Attackers

VI. CONCLUSION

A comparative analysis has been done between the preventive Trust Based Protocols that ensure high security and minimize the effects of malicious attacks.It is observed that the ESCT protocol is highly effective over all the data traffic attack types. Also it is observed that the ESCT scheme is more reliable than TBDSR or TDSR.

The implementation of network scenario in figure 6 with the parametric specifications shown in table 3 are associated to the black hole attack that has been implemented in DSR Protocol and the results show that the PDR decreases with increase in no. of attackers. There is a drop of 30% in PDR with 20 attackers. The throughput is decreased by around 100 to 400 Kbps progressively. There is a drop of 31.2% in throughput in the presence of 20 attackers. The number of packets received is decreased by around 800 to 1500. The packets received are decreased by around 31.22% in the presence of 20 attackers. The average delay decreases as the number of received packets is decreased when the no.

of attackers is increased by 5 progressively. Hence less number of packets are routed and received at destination. So the required amount of delay goes on decreasing for less amount of packets receive

An Advanced protocol can be implemented[15][16][17] that will focus on having the knowledge of two alternate shortest paths instead of one. When the link is established and the data is transmitted using one of the links, the other link will be idle. Under BH attack, using trust based scheme, the confirmation of BH attack will be done and now, that the second shortest link is available before hand, the data will be routed by that link. So, crucial time will be saved and hence delay will be less, PDR will be high and throughput of the network will be more.

In this advanced protocol, self-assessment and co-operative assessment of the neighbouring nodes can be done to improve data transmission in the network. Having the trust information of the neighbouring nodes will help in establishing better security. This quality of the protocol makes it more reliable and eligible in the sensitive fields where high security is required.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

REFERENCES

1. RuoJunCai,Xue Jun Li,andPeter and Han Joo Chong, “AnEvolutionarySelf-Cooperative Trust Scheme Against Routing Disruptions in MANETs”, IEEE Transactions on Mobile Computing DOI 10.1109/TMC.2018.2828814.
2. Y. A. Suryawanshi, AvichalKapur, M. D. Chawhan, “Analysis of symmetric key cryptosystem in VANET”, vol. 7, no. 2, pp. 3–7, 2012.
3. M. Mohanapriya · IlangoKrishnamurthi,“Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks”, Arab Journal DOI 10.1007/s13369-013-0764-1.
4. V. RAJESHKUMAR, P.SIVAKUMAR, “Comparative Study of AODV, DSDV and DSRRouting Protocols in MANET Using Network Simulator-2”, International Journal of Advanced Research in Computer and Communication EngineeringVol. 2, Issue 12, December 2013
5. R. F. Sophia Pearlin and G. Rekha, “Performance Comparison of AODV, DSDV and DSR Protocols in Mobile Networks using NS-2”,Indian Journal of Science and Technology, Vol 9(8), DOI: 10.17485/ijst/2016/v9i8/87948, February 2016
6. Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose,HimadriNathSaha and DebikaBhattacharjee, “Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques”, Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake.
7. SagarikaKar Chowdhury, Mainak Sen. "Attacks and mitigation techniques on mobile ad hoc network — A survey", 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017.
8. P. Kavitha, RajeswariMukesh. "To detect malicious nodes in the Mobile Ad-hoc Networks using soft computing technique", 2015 2nd International Conference on Electronics and Communication Systems (ICECS), 2015.
9. ElaheFazeldehkordi, IrajSadeghAmiri, OluwatobiAyodejiAkanbi. "Literature Review" Elsevier BV, 2016.
10. Mohanapriya, M., and IlangoKrishnamurthi. "Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks", Arabian Journal for Science and Engineering, 2014.
11. E. Perkins, E. M. Belding-Royer, and S. R. Das, “Ad Hoc On Demand Distance Vector Routing”: IETF RFC 3561, July 2003.
12. T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”: IETF RFC 3626, October 2003.
13. D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”: IETF RFC 4728, February 2007
14. W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K.-Y. Lam, "Trust based routing for misbehavior detection in Ad hoc networks," Journal of Networks, vol. 5, pp. 551-558, 2010.
15. S. Yan Lindsay, Y. Wei, H. Zhu, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, pp. 305-317, 2006.
16. K. Hoffman, D. Zage, and C. N. Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Computing Surveys, vol. 42, pp. 1-31, 2009.
17. S. Buchegger and J. Y. L. Boudec, "Performance analysis of the CONFIDANT protocol " in Proc. of ACM MobiHoc'02, Lausanne, Switzerland, Jun. 2002, pp. 226-236.

AUTHORS PROFILE

Swapnil SunilraoBhalsagar received his B.Engg. degree in Electronics and Telecommunication from Rajiv Gandhi College of Engineering and Research, Nagpur under Nagpur University, currently pursuing M.tech. in Communication Engineering from the Department of Electronics and TelecommunicationEngineering, YeshwantraoChavan College of Engineering, Nagpur year 2018-19.

Dr. Manish DevendraChawhan is working as an Associate Professor in YashwantraoChavan College of Engineering, Department of Electronics & Telecommunication Engineering, Nagpur. He did BE and M-TECH from YCCE, Nagpur. He is PhD in Electronics Engineering from Nagpur University. His area of research is Wireless Communication & Networking. He has a teaching experience of 19 years .He has published & presented 28 papers in various National and International Journals & Conferences. He has been approved a grant from Department of Science & Technology (DST) for research in wireless Communication & Networks. He has also received a grant of from All India Council of Technical Education (AICTE) for Skill and Personality Development of Students. He was a reviewer in The IEEE International Symposium on Signal Processing and Information Technology (ISSPIT) held in Luxor, Egypt and Journal of Communication and Networks published by Korea Informatics and Communication society. He has delivered various expert lectures on Bluetooth technology, wireless communication and networks, optical fiber communication, Cross Layer Design, Microcontroller Architecture and chaired sessions as judge in national and international conferences. He has taken workshops on Signal Processing using Matlab, Bluetooth technology, Optical Fiber Communication. He is an approved supervisor for PhD.

Dr. Yogesh A. Suryawanshi, is working as an Assistant Professor in YashwantraoChavan College of Engineering, Department of Electronics Engineering, Nagpur. He did M-TECH from GHRCE, Nagpur. He is PhD in Electronics Engineering from Nagpur University. His area of research is Cryptography & Network Security. He has a teaching experience of 13 years.He has published & presented 15 papers in various National and International Journals & Conferences. He has delivered various expert lectures on Cryptography & Network Security. He has taken workshops on PLC & SCADA.

Dr.VirendraKeshavTaksande, is working as Head of the Department in Priyadarshini College of Engineering, Department of Electronics & Telecommunication Engineering, Nagpur. He did BE from N.I.T. Durgapur (W.B.) and M-TECH from YCCE, Nagpur. He is PhD in Electronics Engineering from Nagpur University. His area of research is Wireless Communication & Networking. He has a teaching experience of 23 years & industrial experience of 7 years in HMT,Ajmer .He has published & presented 19 papers in various National and International Journals & Conferences. He is a technical consultant for research in wireless Communication & Networks in industry.

He has also received BHARAT VIDHYA RATNA AWARD from International Business council for his contribution in educational field and social field. He is an editorial member of international journal. He has delivered various expert lectures on Bluetooth technology, wireless communication and networks, optical fiber communication, Cross Layer Design, Microcontroller Architecture and chaired sessions as judge in national and international conferences. He has taken workshops on NS2.