International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Hybrid Mobile Ad-Hoc Delay Tolerant Network for Optimum Routing in Wireless Sensor Networks

C R Rathish, Prakasam P

Abstract: ***Due to some misbehaving nodes in Mobile Ad-hoc networks (MANETs), data is lost or false data is delivered. In order to detect and re-configure the path from the source to terminal, Ad-Hoc On- Demand Distance Vector (AODV) routing protocol is used. In existing method the black holes are generated due to the Ad-Hoc On-Demand Distance Vector (AODV) routing protocol. Hence a Delay Tolerant Network (DTN) is proposed to cope up with the black holes. In this paper, it is proposed to operate by forming hybrid network with MANET and DTN as MADT Network is to deliver the correct data with increased bit rate and low delay. The proposed Hybrid MADT network has been verified and the results show that the throughput of the proposed network is increased by 0.7%, the packet transmission rate is enhanced by 7% and the end-to-end delay is reduced by 4%.***

Keywords : AODV, Black Holes, DTN, MADT Network, MANET.

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) [1], [2] is a self-organized network in which the ambulant routers are interconnected by wireless means. Every individual node in MANET changes its link frequently to other devices as it can move freely in any particular direction [3]. MANETs usually have a networking environment that performs routing on the top of the link layer of the Ad-hoc network. Communication in MANET is carried out via multiple techniques [4] - [7]. Various challenges are faced by MANET that contains multiple resource network topology changes unpredictably and connection breaks are pretty frequent. Depending upon the application, the mobility of the host and the node requirement varies. The nodes in MANET are not assigned manually, instead every individual node in the network acts as a router and forwards the data packets to the other nodes of that network. There are two protocols to determine whether the data traffic is properly processed. In Table-driven routing protocol compatible and contemporary routing statistics are perpetuated. Since it involves high data transfer it isn't preferred mostly. The Hello Messages RREQ, RREP, RERR are also used to monitor the network topology. These messages have their specific algorithms.

Manuscript published on 30 September 2019.
*Correspondence Author(s)
C R Rathish, Electronics and Communication Engineering, United Institute of Technology, Coimbatore, India. Email: r.rathish87@gmail.com
***Prakasam P**, School of Electronics Engineering, Vellore Institute of Technology, Vellore, India. Email: prakasamp@gmail.com

Since data or information in MANET are much sensitive, there are always several threatening to the network topology. They may be active or passive and MANET doesn't have specified infrastructure so any node can join or leave anytime, which is rather an advantage and disadvantage. The AODV [8] attack is exposed as various attacks which may lead to breakdown of network connectivity and many more. There are several attacks like black hole, wormhole, byzantine, rushing attack etc in AODV. These may vary but their main objective is to collapse the network topology.

During Black Hole attacks [9], [10] the malicious node plays the major role in destroying the network traffic. The node sucks the data or information, responds with false RREP messages. It also responds faster than other nodes. Main objective of this node is to collapse or breakdown network between other nodes. This attack is referred to as black-hole attack which is caused by RREP and RREQ messages [11]. Black hole attacks cannot be completely avoided and hence it can be coped with Delay Tolerant Network (DTN) using Bundle protocol. The Bundle protocol stores the message/ information until the neighbor node is ready for transfer of data. It categorizes the information into bundles, then by using the store-and-forward technique it transmits the data. It is the technique which connects the multiple subnets into a single network. In this paper, we have suggested to introduce a hybrid network which is a combination of both **AODV with DTN** which will enhance the productivity of the networks.

II. RELATED WORKS

In the previously proposed methods, the concept of Mobile Ad hoc network, its impact of black hole and coping up using delay tolerant network was carried out by many researchers. This section describes the selfish node detection by AODV protocol.

Ahmad A. Hadi, Zulkamain Md. Ali and Yazan Aljeroudi [12] presented the Ad-hoc On Demand Distance Vector (AODV) routing protocol which is used to detect and avoid the misbehaving nodes. This scheme improves the performance such as the Packet Transmission Rate thus minimizing the delay caused during data packet transmission. However, the proposed scheme is vulnerable to multiple types of attacks. FIHRI Mohammed, OTMANI Mohammed and EZZATI Abdellah [13] presented the paper with Ad Hoc network which is independent without central management, easily configurable and cost effective but is vulnerable to the impact of black holes which are the most intrusive attacks of its kind on the MANET that causes higher amount of packet loss compared with normal AODV situation.

Pham Thi Ngoc Diep and Chai Kiat Yeo [14] presented the method of developing Delay Tolerant Network to manage even in the case of random connectivity and prolong delay in WSN. In this paper, in order to handle individual as well as collusion attacks they have proposed a method that detects the presence of Blackhole as well as Greyhole attackers based on the statistics. It maintains the network by coping up with almost same efficiency even with delay.

Shesh Kumar Sharma, Ramendra Kumar, Anshul Gangwar and Kamaljeet Pakhre [8] has proposed the knowledge regarding various routing protocol to combine and integrate to keep the network active for a long period of time. The various advantages and the fields where MANETs find their application with many challenges and issues are studied in this paper to establish effective and secure communication.

Waleed S. Alnumay and Uttam Ghosh [15] in this paper described the summary regarding the popular Mobile Ad- Hoc Network (MANET) with the Ad- Hoc On-Demand Distance Vector routing protocol (AODV) and the standard Transmission Control Protocol (TCP). The AODV provides security to the route detection and route conservation.

III. PROPOSED SYSTEM

In the existing system, AODV protocol is employed that establishes connection whenever there is a demand thereby minimizing the traffic while communication along the links. But, as the level of trust in the network cannot be estimated, compromised nodes may interfere with route discovery process and head off the control packets to disturb communication. In Delay Tolerant Network (DTN), these intermittent communication issues are addressed and resolved by enhancing communication over the most unstable and stressed environments where the probability of network disruptions is high. Thus, the sufficiency of DTN copes up the insufficiency of AODV by devising a hybrid network.

In the proposed work, monitoring of misbehaving nodes in MANET and detecting the black hole attack using delay tolerant network has been combined. Thus, a hybrid network (AODV with DTN) is proposed which increases the throughput ratio and packet transmission ratio and decreases the overall delay.

IV. OVERVIEW OF THE SYSTEM DESIGN

In the process of data transfer when the nodes are of particular radio range or nodes which are perfect can directly transfer data. When there is a presence of misbehaving node, the transfer of false data or loss in data takes place. In this case, local repair starts as detecting the misbehaving nodes and finding an alternate route by AODV protocol. In AODV, the procedure of sending RREQ to the destination and receiving RREP from the neighbouring nodes is performed. If the RREP received is appropriate then the data transfer takes place. In other case, if the data received is not original data then the generation of black hole takes place.

The generation of blackhole cannot be completely avoided, it can only be managed by the Delay Tolerant Network. The Delay Tolerant Network uses the Bundle protocol to store and forward the information/data until the neighbouring node is active and ready to transfer the information. Thus, the blackhole attack is coped using DTN and the data transfer takes place successfully. The block diagram given below depicts the proposed system.

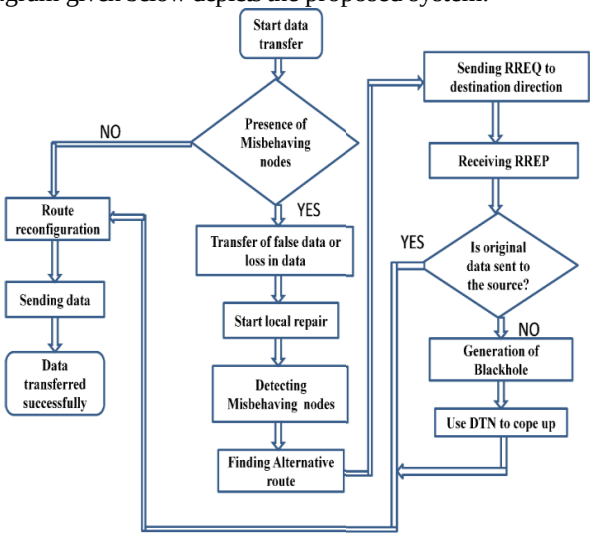

Fig. 1. Block diagram

Hence from all the concepts explained above, the proceedings of the reckon is, the relocation of the data commences until the reckon materialize and when the existence of the node which fail to conduct oneself in an acceptable way is observed then the AODV protocol occur as a supervene to resolve the muddle by sorting an alternate route. Howbeit AODV is the unexcelled; it has the snag of forming black holes. The black holes provoke when the erroneous announcement originate. The black holes cannot be circumvented wholly and so it is coped up using Delay Tolerant Network (DTN). The DTN helps in relocation of data even in case of black holes by managing or coping up with the black holes activities. It originates the route reconfiguration and resettles the data capably.

A. Monitoring Misbehaving Nodes

In MANET, any mobile node can transfer and receive data. Here the mobile nodes transfer data using Distance Vector Routing algorithm. In DVR protocol, every individual node of the network holds the attribute such as the distance or cost of all the other nodes of the network and transmits the information to the immediate neighbouring nodes.

B. Distance Vector Routing

Distance vector routing protocol determines the best possible path for routing based upon the interspace betwixt the source and the target. An illustration of Distance Vector Routing is depicted in the figure (Fig. 2. Example for Distance Vector Routing) and its routing format is illustrated in the table (Table- I Routing table). This routing algorithm measures the interval by calculating the no. of routers a data packet has to pass through, counting one router as one hop. DVR protocol utilizes the Bellman-Ford algorithm as well as Ford-Fulkerson algorithm to estimate the shortest and leading route. The other means of estimating the foremost path is based on the cost of the link, and it is administered through link-state routing protocol.

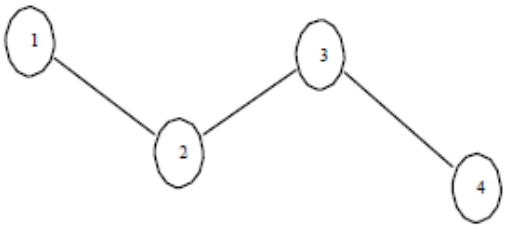

Fig. 2. Example for distance vector routing

Table- I: Routing Table

SOURCE	NEXT HOP	COST	DESTINATION
1	2	18	3
2	3	8	4
3	4	6	4

C. Misbehaving Nodes

Some nodes in MANET deny service to other nodes of the network, such type of nodes are known to be misbehaving nodes [16]. So as to detect and monitor the misbehaving nodes the AODV is used.

D. AODV Protocol

The AODV protocol builds route between the nodes of a network only if it is requested by the source nodes. The AODV routing protocol efficiently informs the network with route failure. The AODV routing protocol is broadly classified into two types. They are:

1) Table-driven routing protocol
2) Source initiated on-demand routing protocol

Table driven routing protocol is also referred to as proactive routing protocol an example is shown is figure (Fig. 3. Example for AODV) and its route allocation for node 1 is shown in the table (Table- II : Routing table for node 1).

In this protocol the nodes in the network need to have the updated routing information. Even after a minor change in the network the node creates routing table to store the information. Thus it is used in high dynamic network as lots of dynamic changes occur and it may cause high congestion. Apart from all its advantages like battery power drain out the major advantage is that there is no initial delay. AODV is a reactive routing protocol, which is employed to find the route betwixt the source and the target. It also allows the movable nodes to get fresh routes for their current destination so as to maintain the network.

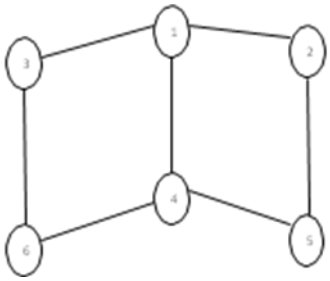

Fig. 3. Example for AODV

Table- II: Routing table for Node 1

DESTINATION	NEXT HOP	DISTANCE
3	3	1
2	2	1
4	4	1
5	2	2
6	3	2

In AODV, there are three types of messages along with a HELLO message, they are Route request (RREQ), Route reply (RREP) and Route error (RERR). The process of RREQ and RREP is explained in the figure (Fig. 4. Example for RREQ and RREP).

- RREQ

This is the first message used to locate the destination. This message is used to locate the target. This message is used to obtain the attributes such as the sequenced number, terminal address and the hop count initiated by zero.

- RREP

The route reply message has the similar fields as in route request message. The message is forwarded in the similar path as RREQ. This message is dispatched from the target to the origin. Once this message reaches the origin, it indicates that the target is prepared to receive the data from the source and the path is operating properly.

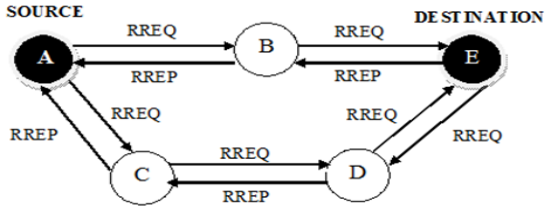

Fig. 4. Example of RREQ and RREP

E. Black Hole Attackers

When the AODV routing protocol finish its repairing process there are chances of creation of black hole attackers. Black hole attackers [17], [18] are invisible nodes which are present within the network and its presence can only be known when the message is lost or part of the message is missing. Thus it is not possible to detect the presence of black hole attackers and destroy them, thus we should use a network which is capable of coping with the black hole attackers and transfer the message correctly to make it reach the destination. The presence of black hole attack will drastically reduce the packet delivery. In our proposed work we use DTN to deal with the black hole attackers and to successfully transmit the data to the destination with more efficiency.

F. Delay Tolerant Network (DTN)

The DTN [19] is employed in order to deal with the black hole attackers which are invisible nodes, whose presence cannot be detected and which cannot be completely destroyed. In our proposed system the protocol used in Delay Tolerant Network is Bundle protocol.

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

G. Bundle Protocol

The bundle protocol [20] is used in order to cope up with the intermittent connectivity which is caused by the black hole attackers. The bundle protocol uses store and forward mechanism. In this protocol the data is stored in the transmitting node until it ensures that the data has reached the destination. In case the information is lost during the communication process due to the presence of black hole attackers, the node which stored the information retransmits it and makes sure it reaches the destination.

The above figure (Fig. 5. Bundle Protocol) explains the bundle protocol in detail. Here, node A stores the data even after it transmits to node B till the information reaches the target. By using this technique, the data can successfully reach the destination by reconfiguring its path.

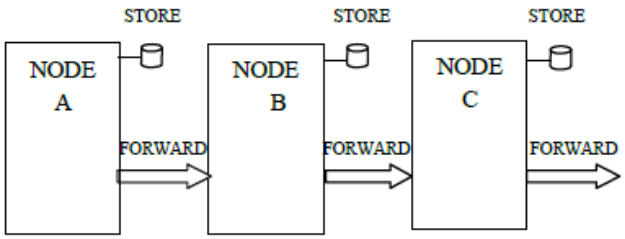

Fig. 5. Bundle protocol

Table- III: Simulation parameters

NETWORK	VALUES
Number of Nodes	59
Topography Area	1000 m X 800 m
Connection Type	UDP
Source Traffic	CBR
Routing Protocol	AODV
Simulation Time	1000 sec
Network Simulator	NS-2

V. RESULT AND ANALYSIS

A. Throughput Ratio

It is the ratio of the total number of data packets delivered to the total simulation time.

$$T = \frac{T(p_{(d)})}{T(s_{(t)})} * 100 \qquad (1)$$

In analysis, the throughput ratio in the form of hybrid network with the AODV and DTN is 8.3% and the throughput ratio in AODV in the existence of Black hole attack is 7.6%. Therefore, it has been shown that the throughput ratio is increased by 0.7%.

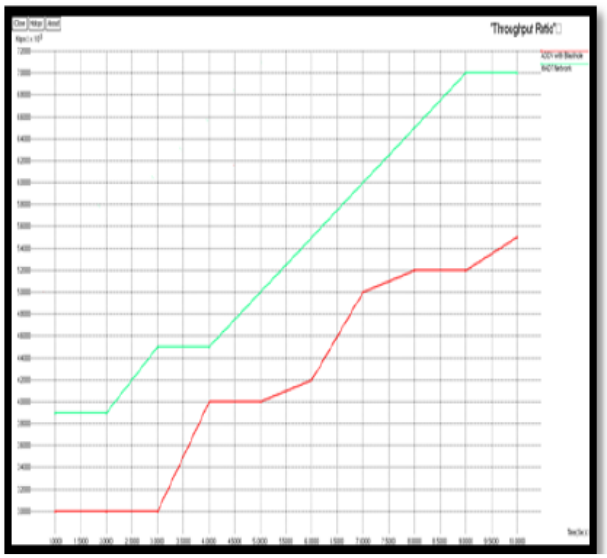

Fig. 6. Throughput Ratio of AODV with Black Hole and Hybrid Network

B. End-To-End Delay

It is the difference in time between the packet received and the packet sent to the total packet count.

$$E2E = \frac{R(ti) - S(ti)}{T(pc)} * 100 \qquad (2)$$

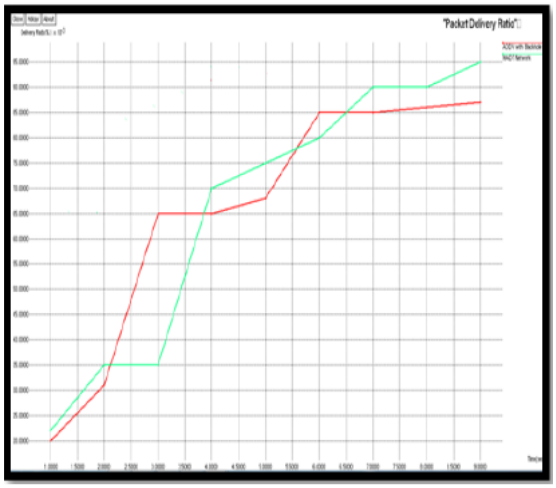

Fig. 7. End-To-End Delay of AODV with Black Hole and Hybrid Network

In analysis, the delay in the form of hybrid network with the AODV and DTN is 4% and the delay in the AODV in the existence of Black hole attack is 8%. Therefore, it has been shown that the delay in the proposed is reduced by 4%.

C. Packet Delivery Ratio

It is the total number of packets received to the number of packets generated or transmitted to the destination from source.

$$PDR = \frac{n(p_{(r)})}{n(p_{(g)})} * 100 \quad (3)$$

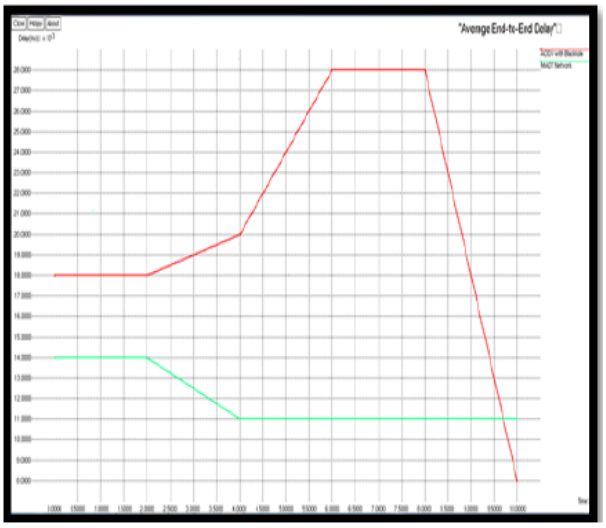

Fig. 8. Packet Delivery Ratio of AODV with Black Hole and Hybrid Network

Table- IV: Comparison table

S. NO	PROTOC-OL	ADVANTAGES & DISADVANTAGES
1	Enhanced Adaptive Acknowledgement Scheme [8] **(EAACK)**	**Advantage:** It is capable of detecting misbehaving nodes and it ensures authentication. **Disadvantage:** It is unsuccessful in detecting the misbehaving nodes when the acknowledgement packets are forged by the attackers.
2	Enhanced Adaptive Acknowledgement 2 [8] **(EAACK2)**	**Advantage:** It is the improved version of the EAACK and provides better detection of false behaviour of nodes [9]. **Disadvantage:** It has higher routing overhead than the EAACK.
3	Mobile Agent Based Acknowledgement Scheme **(MAACK)** [19]	**Advantage:** It reduces the network overhead. It also reduces latency for better performance in MANET. **Disadvantage:** Comparing the existing EAACK model, MAACK is efficient but it does not provide good efficiency in common.
4	Audit Based Misbehaviour Detection **(AMD)** [20]	**Advantage:** It successfully and systematically differentiates continuous as well as selective packet droppers. It undergoes packet evaluation without packet overhead. **Disadvantage:** Sometimes the packets are not forwarded by the network which causes hindrance in data transmission.
5	Dynamic Source Routing [12] **(DSR)**	**Advantage:** It reduces the communication overhead. **Disadvantage:** It enlarges the identification delay. It fails to detect selective attackers due to encrypted flow.
6	Audit Based Misbehaviour Detection and Monitoring Method [20] **(AMDMM)**	**Advantage:** It operates in multichannel networks as well as in networks having directional antenna. **Disadvantage:** Sometimes the packets are not forwarded by the network which causes hindrance in data transmission.
7	Ad-Hoc On-Demand Distance Vector **(AODV)** Routing Protocol [12]	**Advantage:** It is more adaptable in responding to changes that attack the dynamic routes. The data packets do not suffer from any extra overhead [14]. **Disadvantage:** In AODV, due to the effect of Black hole more information is lost.
8	Bundle Protocol in **DTN** [17]	**Advantage:** They have the advantage to easily deal with the network issues like bandwidth, delays and breakups. They hold record of the communication and provide information when requested. **Disadvantage:** It is not needed for the single hop systems. It adds overhead depending on data size.
9	Hybrid AODV and DTN Network	**Advantage:** It copes with the Black hole attack in AODV. It reduces the overhead in the Bundle protocol. **Disadvantage:** It increases complexity with large data transfer.

VI. CONCLUSION

In this research paper, AODV in MANET and its various challenges are presented. The method in DTN to cope with challenges in AODV is also discussed. After detailed review, it is concluded to form the hybrid network with the AODV and DTN, which will tend to get efficient output by enhancing the throughput and data packet transmission rate and by minimizing the overall delay. It has been observed that the throughput of the proposed method is increased by 0.7%, the packet transmission rate is enhanced by 7% and the end-to-end delay is reduced by 4%.

REFERENCES

1. Prakasam P, "Optimal Power Distribution Strategy for Energy Harvesting in Wireless Sensor Networks Using Assymetric Nash Bargaining Algorithm," *Environmental Engineering: Current Perspective*, PP. 322-325, 2017.
2. M. Ghonge, S. U. Nmbhorkar, "Simulation of AODV Under Blackhole Attack in MANET," *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 2, February 2012.
3. Rajaram P, Prakasam P, "Non-Linear Error Identifier Algorithm for Configuring Mobile Sensor Robot," *Journal of Electrical Engineering and Technology*, Volume 10, Issue 3, PP. 1201-1216, 2015.
4. R. Rajasekar, P. Prakasam, "Proposed Coordinating Multiple Sampling Task in Sensor Field Using Geometric Progression Algorithm for Efficient Data Collection in Wireless Sensor Networks," *Springer Science Business Media New York*, Volume 82, Issue 3, PP. 1810-1824, 2015.
5. Rajaram P, Prakasam P, "Data Collection Using Mobile Robot in WSN: A Review," *Journal of Theoretical and Applied Information Technology*, Volume 65, Issue 2, PP. 437-446, 2014.
6. Sathyaprakash Palaniappan, Prakasam Periasamy, "Proposed Energy Efficient Multi Attribute Time Slot Scheduling Algorithm for Quality of Service in Wireless Sensor Network," *Wireless Pers Communication*, Volume 97, Issue 4, PP. 5952-5968, 2017.
7. C R Rathish, A Rajaram, "Sweeping Inclusive Connectivity based Routing in Wireless Sensor Networks," *ARPN Journal of Engineering and Applied Sciences*, Vol. 13, No. 5, PP. 1752 – 1760, March 2018.
8. Shesh Kumar Sharma, Ramendra Kumar, Anshul Gangwar, Kamaljeet Pakhre, "Routing Protocols and Security Issues in MANET: A Survey," *International Journal of Emerging Technology and Advanced Engineering*, Volume.4, Issue 4, PP. 918-924, April 2014.
9. Akanksha Saini, Harish Kumar, "Effect of Blackhole Attack on AODV Routing Protocol in MANET," *International Journal of Computer Science Trends and Technology*, Volume 1, Issue 02, PP. 57-59, December 2010.
10. Monika Roopack., Prof. BVR Reddy, "Blackhole Attack Implementation in AODV Routing Protocol," *International Journal of Scientific and Engineering Research*, Volume 4, Issue 05, PP. 402-406, May 2013.
11. C R Rathish, A Rajaram, "Robust Early Detection and Filtering Scheme to Locate Vampire Attack in Wireless Sensor Network," *Journal of Computational and Theoretical Nanoscience*, Vol.14, PP. 2937 – 2946, 2017.
12. Ahmad A Hadi, Zulkamain Md Ali and Yazan Aljeroudi, "Improved Selfish Node Detection Algorithm for Mobile Ad Hoc Network," *International Journal of Advanced Computer Science and Application*, Volume 8, No.4, PP. 103-108, 2017.
13. FIHRI Mohammed, OTMANI Mohammed, EZZATI Abdellah, "The Impact of Black-Holes on Ad hoc On-Demand Distance Vector Routing Protocol," *International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad hoc Networking and Applications*, PP. 20-24, 2014.
14. Pham Thi Ngoc Diep, Chai Kiat Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," *IEEE Transactions on Mobile Computing*, Volume 15, Issue 5, PP. 1-15, May 2016.
15. Waleed S. Alnumay, Uttam Ghosh, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks," *International Journal of Computer Networks & Communication*, Volume 6, No.1, PP. 111-127, January 2014.
16. Xianghui Cao, Lu Lui, Wenlong Shen, Aurobinda Laha, Jin Tang, Yu Cheng, "Real-Time Misbehavior Detection and Mitigation in Cyber-Physical Systems over WLANs," *IEEE Transactions on Industrial Informatics*, PP. 1-12, 2015.
17. Imad Aad, Jean- Pierre Hubaux, Edward N. Knighty, "Impact of Denial of Service Attacks on Ad Hoc Networks," *IEEE Transactions on Networking*, Volume 16, No.4, PP. 791-802, August 2008.
18. Yuxin Lui, Mian Xiong Dong, Kaoru Ota, Anfeng Liu, "Active Trust: Secure and Trustable Routing in Wireless Sensor Networks," *IEEE Transaction on Information Forensics and Security*, PP. 1-14, 2016.
19. Qinghua Li, Guohong Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," *IEEE Transactions on Informatics Forensics and Security*, Volume 7, No.2, PP. 664-675, April 2012.
20. Rakhi Sharma, Dr D. V. Gupta, "Blackhole Detection and Prevention Strategies in DTN," *International Journal of Engineering and Computer Science*, Volume 5, Issue 8, PP. 17386-17391, August 2016.
21. Otor Samera U., Akinyemi Bodunde O., Adekunle Adeyelu, Akumba Beatrice O., Aderounmu Ganiyu A., "An Agent -Based Approach To Nodes' Misbehaviour Detection In Mobile Ad-Hoc Networks," *International Journal of Scientific and Technology Research*, Volume 6, Issue 02, PP. 44-49, February 2017.
22. Zhang, Lou Kas Lazos, William Jr. Kozma, "AMD: Audit-Based Misbehavior Detection in Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, PP. 1-14, 2012.

AUTHORS PROFILE

C R Rathish is an Assistant Professor in the department of Electronics and Communication Engineering. He pursued his Bachelors' degree in ECE from Maharaja Prithvi Engineering College and Masters' degree in VLSI Design from Karpagam University, Coimbatore. He has presented 4 National Conferences and has published 10 articles in well reputed journals. He has also published a patent. His research interests includes Wireless Communication, Wireless Sensor Networks and VLSI Design.

Prakasam. P has obtained his B.E degree in Electronics and Communication Engineering from Madras University in 1994. He received his M.Tech degree in Advanced Communication Systems from Sastra University, Tanjore, India in 2002. He obtained his Ph.D from Anna University Chennai, India. At present he is a Professor, School of Electronics Engineering at Vellore Institute of Technology, Vellore. He has authored over one hundred and ten research publications in international and national journals and conferences. His special areas of interest are Signal Processing, Wireless Networks, Communication Systems and Applications of signal processing in Mobile Communication Systems. He is an Associate Editor in IEEE Access and an editor-in-chief of Journal of Signal Processing and Wireless Networks. Prakasam. P is a Senior Member of IEEE (USA), life member of ISTE, IACSIT, IAENG and VSI (India).