Anomalous Node Detection and Removal in Ad-hoc Network using Enhanced Prime Product Scheme

Tariq Siddiqui
M. Tech. Scholar
CSE Dept

Tanveer Farooqui
Asst. Prof.
CSE Dept

ABSTRACT
In Associate in Nursing Ad-hoc network may be a assortment of mobile nodes dynamically forming a short lived network while not the employment of any existing network infrastructure or centralized administer. attributable to restricted communication vary among mobile nodes in ad-hoc network, many network hopes is also required to deliver a packet from one node to a different node within the wireless network. Many users want to save its resources like battery power, processing and capability for only their personal use hence such nodes become misbehaving in nature and not co-operate do selfish activities. The security of MANET is manipulated by malicious node attack. In such type of attach, a malicious node insert a fake route reply claiming to have the shortest and freshest route to the destination. However, when the data packets arrive, the malicious node discards them. To avoid malicious attack, this work gives behavior analysis with PPN (Prime Product Number) scheme for detection and removal of malicious node.

Keywords
MANET, Malicious Node, bad Nodes removal, Selfish Nodes detect, Network Monitoring.

1. INTRODUCTION
A mobile ad-hoc network (MANET) could be a self-configuring communications less network of mobile devices connected by wireless links. Ad-hoc is Latin word which implies "for this purpose". It's the dynamic set of nodes wherever nodes could also be any machine that ready to send knowledge or share knowledge with all different machines. MANETs are a gaggle of wireless ad-hoc system that usually incorporates a routable networking atmosphere on prime of a Link Layer impromptu network. A painter is associate degree freelance assortment of movable users that exchange knowledge over moderately painter increasing interactions between communication and computing, that is dynamical data access from "anytime anywhere" into "all the time, everywhere." at this time, an oversized kind of networks exists, starting from the well-known infrastructure of cellular networks to non-infrastructure wireless ad-hoc networks. Ad-hoc networks are fitted to use in things wherever associate degree infrastructure is out of stock or to deploy one isn't price effective. MANETs are broadly speaking employed in a variety of military state of affairs, like armed forces switch data on the sphere, investigate groups direct in combat investigate and save exertions, and period enemy uncovering within the order of a troop location. In ancient networks, MANETs are additional susceptible to cruel attacks and accidental breakdown owing to their exclusive options like forced node energy, erring communication media, and dynamic configuration. Therefore, security could be a important for MANETs.

A mobile impromptu network (MANET) is associate degree infrastructure less network of mobile devices. In painter mobile devices communicate on network path for routing messages from one system to a unique. In painter all devices are unengaged to move in any direction, and thus modification its links to different devices often. Each device ought to send traffic unrelated to its own use, and need to be a router. The most challenge in building a painter is mobilization each device to ceaselessly maintain the info required to properly route traffic. These MANETs could operate by themselves or might even be connected to the larger web. MANETs are a type of Wireless impromptu network that usually includes routable networking surroundings on prime of a Link Layer impromptu network. Several analyses have been applied in comparison painter protocols victimization utterly totally different parameters. These are centered on rising performance of painter networks to consume energy efficiently and routing additional economical. In impromptu networks, nodes are not conversant in the topology of their networks. Instead, they have to seek out it: a novel node announces its presence listens for announcements broadcast by its neighbors. Each node learns regarding totally different shut nodes and but to achieve them, associate degreed build an announcement that it may reach them. In MANETs, the nodes ar mobile and battery operated. Because the nodes have restricted battery resources and multi hop routes are used over a dynamical network surroundings owing to node quality, it needs energy economical routing protocols to limit the ability consumption, prolong the battery life and to boost the hardiness of the system [1].

Node wrongful conduct is such a class of security threat for Mobile unexpected Networks (MANETs). In general, misbehaviors may be conducted at each layer in MANETs, like malicious flooding of the Request-To-Send (RTS) frames within the waterproof layer, dropping, modification, and misroute to the packets within the network layer, and deliberate propagation of faux observations relating to the behaviors of alternative nodes within the application layer. Moreover, node misbehaviors might vary from lack of cooperation to active attacks aiming at Denial-of-Service (DoS) and subversion of traffic [25]. as an example, due to the restricted resources (such as battery power and information measure, etc) that every node will presumably possess, a stingy node might select to not work with alternative nodes thus on preserve its own resources [2]. In alternative words, once a stingy node is requested to forward some knowledge packets for alternative nodes, it would drop a section or all of the incoming packets. By this implies, it will save the battery power and transmit some further packets for the sake of itself. On the opposite hand, some malicious nodes aim to disturb the network services, and that they might by choice drop, modify or misroute packets whereas it's not a priority for them

to save lots of battery lives [3]. Despite the intents by that the node misbehaviors ar iatrogenic, they're clearly harmful to a presently healthy Manet..

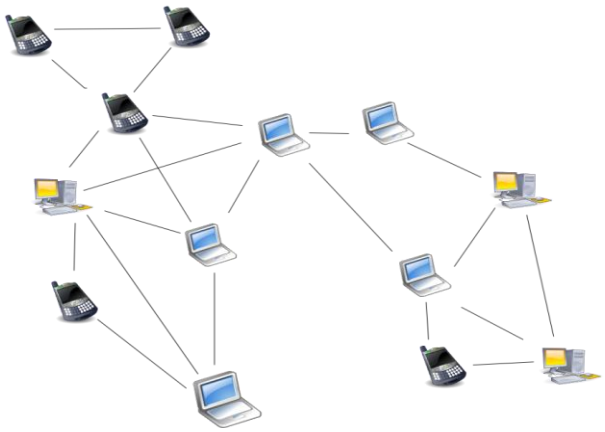

Fig 1. MANET Architecture

To address the safety vulnerabilities caused by numerous node misbehaviors in Mobile unexpected Networks (MANETs), varied security solutions are planned to discover and mitigate those misbehaviors from distinctive views, like the mechanisms mentioned consequently in [4], [5], and [6]. as a result of it's quite helpful to assess a node's behaviors and verify if it's trustworthy in terms of however cooperative it's, trust management mechanism has become an influence tool to address node misbehaviors. a spread of trust management mechanisms are studied throughout the past decades, like the mechanisms mentioned in [6], [7], and [8]. Most of those trust management mechanisms model the trust of a node in one dimension, i.e., all on the market proof and observations are utilized to calculate one, scalar trust metric for every node. However, one trust metric might not be communicative enough to adequately describe whether or not a node is trustworthy or not in several difficult eventualities.

Intrusion Detection is associate degree action with the intention of resolve whether or not a procedure or shopper is efforts for somewhat unexpected. It's operating as distinct by Michael G male monarch and microphone Chappel [20] on the muse of investigatory action on a specific device or network with decides whether or not the action is common or leery. It will more compare recent action to recognized attack image or simply raise associate degree alarm circumstance whereas elaborate measurements reassess specific standards.

There are lots of techniques for intrusion recognition in MANETs. The preliminary categorizations are found on validation based mostly systems. These admit the popularity of nodes through associate degree solely symbol. Build use of secret writing keys comes into this class, likewise as they need been sincerely deliberate. The next approach is activity base algorithms by this intrusion are often distinct supported nodal behaviors, instead of its symbol. This, consistent with USA, is associate degree increased approach for the given reasons:

1. Node individualism are often merely tolen, Behavior is more durable to duplicate.

2. Individuality based mostly actions involves storage of symbol databases or judgment.

3. Each contemporary node must be given a novel symbol, construction the procedure of preparation extra costly (time and cost).

2. RELATED WORK

In the past decade, several analysis efforts are created to deal with the safety desires for MANETs by suggests that of trust management [9]. The most goal of trust management is to gauge the actions of alternative nodes, and builds a name for every node supported the node analysis result [30]. The name will then be accustomed verify the trustiness for alternative nodes. The trustiness is utilized to create decisions on those nodes to collaborate with, or perhaps take action to penalize Associate in shady node if necessary. Trust is split into express trust and indirect trust [10]. Express trust stems from the first-hand observations regionally obtained by a node itself, whereas indirect trust refers to the secondhand observations free by alternative nodes. In MANETs, express trust cannot invariably offer comprehensive analysis of the target node thanks to exterior circumstances like channel conditions, temporary inaccessibility, interference, etc. At this point, indirect trust is employed to supply secondary info to assist judge the particular trustiness of the target node.

Due to its dynamic nature and quality of nodes, mobile adhoc networks are additional susceptible to security attack than typical wired and wireless networks [27]. One in every of the principal routing protocols AODV utilized in MANETs. The safety of AODV protocol is influence by malicious node attack. During this attack, a malicious node injects a faked route reply claiming to own the shortest and freshest route to the destination. However, once the information packets arrive, the malicious node discards them. To preventing malicious node attack, paper [13] presents PPN (Prime Product Number) theme for detection and removal of malicious node.

The paper [14] proposes to use an applied math logical thinking technique, namely, belief propagation (BP), to estimate the likelihood of peers being malicious. The detection algorithmic program is travel by a group of trusty monitor nodes that receives notification messages (checks) from peers whenever they get a bit of data; these checks contain the list of the chunk up loaders and a flag to mark the chunk as contaminated or clean. Peers are able to sight if the received chunk is contaminated or not however, since multiparty transfer is used, they're powerless to spot the source(s) of counterfeit blocks.

To find out malicious nodes among a WSN with mass detector nodes, this paper [15] presents a malicious detection methodology supported multi-variate classification. Given the categories of a number of detector nodes, it extracts detector nodes' preferences connected with the famous varieties of malicious node, establishes the sample area of all detector nodes that participate in network activities. Then, per the study on the type-known detector nodes' samples supported the variable classification algorithmic program, a classifier is generated, and every one of the unknown-type detector nodes are classified.

The sensitivity of Wireless detector Networks makes them at risk of attacks that cause extraction or injury of info or information that flows between distinct nodes [33]. the most objective of paper [16] is to construct an efficient detector security sightion system that is adaptation to the behavioral changes of the nodes and therefore the knowledge flowing between varied detector nodes and thence detect the malicious node in our surroundings supported its skeptical behavior.

Preventing or detection malicious nodes launching grayhole or cooperative blackhole attacks may be a challenge. This paper [17] makes an attempt to resolve this issue by coming up with a dynamic supply routing (DSR)-based routing

mechanism, that is cited because the cooperative bait detection theme (CBDS), that integrates the benefits of each proactive and reactive defense architectures. Our CBDS methodology implements a reverse tracing technique to assist in achieving the expressed goal. Simulation results ar provided, showing that within the presence of malicious-node attacks, the CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols (chosen as benchmarks) in terms of packet delivery quantitative relation and routing overhead (chosen as performance metrics).

Ad hoc on-demand distance vector routing (AODV) may be a very talked-about routing protocol [31]. However, it's susceptible to the well-known region attack, wherever a malicious node incorrectly advertises smart methods to a destination node throughout the route discovery method. In paper [18], a defense mechanism is given against these region attacks during a Edouard Manet. This methodology makes use of the mackintosh address of the destination to validate every node in its path thereby providing an instantaneous negotiation for secure route.

Paper [19] planned model uses the mixture of trust and energy price primarily based routing protocol known as Energy and Trust primarily based AODV routing protocol (ET-AODV) to ascertain a most trusty routes by providing modification to AODV protocol [32]. In planned technique every node estimates its neighbor's trust price and energy price that's one node has for one more node throughout communication dynamically. Adding trust price and energy price new root price is calculated and maintained in each neighbor table. Victimization root price trusty routes are established by 2 ways that are single price routing and multiple price routing and isolate the malicious nodes from the network. This method solely considers the region attack which may simply interrupt the communication path.

3. PROPOSED WORK

The PPN scheme is based on AODV and it can efficiently avoid malicious node attacks during path setup between source and destination. PPN scheme uses Adhoc On-demand Distance Vector (AODV) [4] to form path during path discovery. In PPN scheme, every Cluster head node maintains the neighbor table which is used to keep information about all the nodes in the path discovery of PPN scheme, an intermediate node will attempt to create a route that does not go through a node whose replied information is wrong and PPN is not fully divisible [26]. Therefore, malicious nodes will be gradually avoided by other non-malicious nodes in the network. Compared with AODV, the proposed PPN scheme has the following differences in message format and type.

3.1 RREQ Packet

RREQ in PPN scheme is same as the AODV shown in Figure 2.

Types	J	R	D	G	U	Reserved	Hop Count
RREQ ID							
Originator IP Address							
Originator Seq Number							
Destination IP Address							
Destination Seq Number							

Fig 2. RREQ Packet format

3.2 RREP Packet

In the proposed scheme RREP has additional Node ID, Prime Product Number and Cluster Head Node ID of NRREP fields shown in Figure 3. Node ID field is used to store ID of NRREP, Prime product number is used to store the prime product of all the nodes from destination to source inthe path and cluster head node ID of NRREP field contains the cluster head NodeID of the node which originates the RREP.

Types	R	A	Reserved	Prefix Size	Hop Count
RREQ ID					
Source IP Address					
Destination IP Address					
Destination Seq Number					
Life Time					
Node ID	Prime Product Number			Cluster Head Node ID of Nrrep	

Fig 3. RREP packet in PPN

3.3 Neighbor Table

In PPN scheme each cluster head maintains a neighbor table which is used to keep information about all the nodes as shown in Table 1. Neighbor table contains two fields Node ID and Cluster Head Node ID. Each node in the network has a specific prime number which acts as Node Identity and this identity must not be changed. Every node is associatedwith a Cluster Head into the network. Each node's ID and its Cluster Head ID are stored into the table.

Table 1. Neighbor Table

Node ID	Cluster Head Node ID

3.4 Node Behavior data Collection

All the nodes choose to observe the behaviors [28] of packet drop, modification and misroute, then packet drop rate (PDR), packet modification rate (PMOR) and packet misroute rate (PMIR) can be defined as follows, respectively.

PDR = Number of Packet Dropped/Total Number of Incoming Packets

PMOR = Number of Packet Modified/Total Number of Incoming Packets

PMIR = Number of Packet Misrouted/Total Number of Incoming Packets

Behavioral Data Collection on each node first observes and records the behaviors of their neighbors [29]. These behaviors check while route discovery step, if any node finds abnormal behavior then node may be removed by calling Removal of malicious node method.

The proposed scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. The algorithm for the proposed mechanism is depicted in Fig. 4 and Fig. 5. In the changed protocol, the supply node (SN) broadcasts a RREQ message to get a secure route to the destination node. The intermediate node (IN) that generates the RREP needs to offer [22] info relating to its cluster head and merchandise of all prime numbers from destination to supply node within the type of Prime Product variety (PPN). Upon receiving the RREP message from IN, atomic number 50 with the assistance of its cluster head (CH) can divide the PPN with the Node IDs keep in neighbor table at CH to envision whether or not IN is its reliable node. If SN finds that IN replied information is right and PPN is fully divisible, then IN

is a reliable node for SN and SN starts routing data through IN. Otherwise, IN is unreliable and thus SN calls the malicious node removal process and Subsequently SN ignores any other RREP from the malicious node.

In the malicious node removal process respective CH add malicious node to the malicious list and broadcast this list to the whole network. All nodes of the network when obtaining the malicious list finds the Node IDs of the malicious nodes in their table and every node flushes all the entries associated with these Node IDs from the various tables.

As an example, let's consider attack scenario. In attack scenario all the trusted nodes behave well consistently throughout. This is the simplest attack scenario in which malicious node does not belong to any cluster. In that case malicious node may send the RREP with its own identity in the Node ID field of the RREP, cluster head node ID of Destination (spoofed) and Primeproduct number.

Algorithm to detect Malicious Node attack in MANETs

Notations
MN: Malicious Node
Nrrep: RREP from an Intermediate Node

1. Begin
2. If (PDR>Th OR PMOR>Th OR PMIR>Th)
3. { Declare N_{RREP} as MN.
4. Call Removal of malicious node();
5. }
6. Else
7. Continue.
8. For(Source Node)
9. {
10. Broadcast RREQ packet to every neighbour node
11. Receive RREP
12. RREP will be choose among various reply having Largest sequence number & Minimum Hop count and all other RREP buffered at originating Node.
13. Process RREP
14. }
15. If (Prime Product term is fully divisible && Replied info is right)
16. Declare node as trustworthy node.
17. Else
18. {
19. Declare N_{RREP} as MN.
20. Call Removal of malicious node();
21. }
22. End.

Fig 4. Modified AODV algorithm to detect Malicious Node

Algorithm to remove malicious nodes from the MANETs

Notations
CH: Cluster Head
MN: Malicious Nodes

1. Begin
2. Respective CH adds MN to malicious list.
3. Broadcast this list to the whole network.
4. All nodes of the network after getting the malicious list find the nodes IDs of the malicious nodes in their table.
5. Each node flushes all the entries related to these Node IDs from the respective tables.
6. End.

Fig 5. Algorithm to Remove Malicious Node

Malicious node replies with higher sequence number because they do not know the exact sequence number of the destination node. Consider the network topology described in Figure 6. Here node 3 is the originator and node 67 is the destination node. Node 3 broadcast RREQ packet to the neighbor nodes. Node M is the malicious node and it responds to originator node 3 with RREP and sends its next hop node, cluster head node and prime product number. Node M RREP is choosing among various replies due to its Largest Sequence Number & Minimum Hop Count. As RREP is processed at originating Node, prime product term is not fully divisible & Replied information is wrong. Source node 3 declares Node M as malicious node and calls the process removal of malicious node.

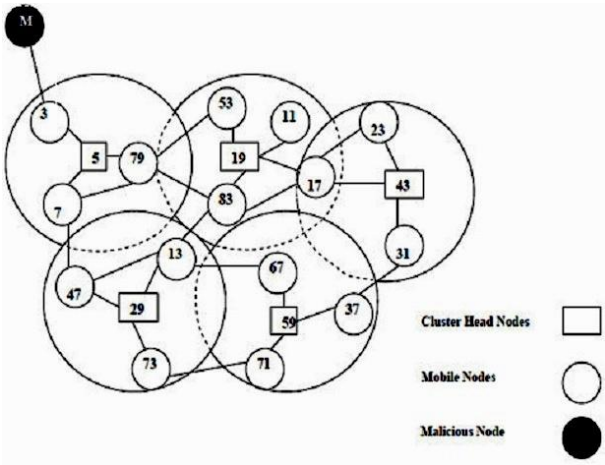

Fig 6. Network Topology for PPN Scheme

3.5 Removal process of malicious nodes

1) Cluster Head Node 5 adds Malicious Node M to the malicious list. Now, Node 5 broadcasts the malicious list to the whole network.

2) All nodes of the network after getting the malicious list find the Node M in their tables and each node flushes all the entries related to Node M from the respective tables.

4. SIMULATION RESULT AND COMPARISON

4.1 Simulation

MATLAB is used for analyzing the performance of the proposed method. Different numbers of nodes are selected for

simulation from 20 to 160 nodes. Numbers of malicious nodes were varied from 2 to 5 through the simulation. The graph of packet delivery rate represents the throughput of standard AODV. The X-axis of the graph represents Number of nodes and Y-axis represents the Network Throughput. The graph demonstrates that AODV routing protocol with proposed method always perform better than standard base method given in paper [13]. The results of the experiments showed that in the presence of 4-10% malicious node,.

Figure 7 and table 2 shows the result generated by proposed method experiments results. Comparative graph represents effectiveness of proposed method for every time for selecting different numbers of nodes such as 20, 40, 60, 80. 100, 120, 140 and 160. Proposed method gives minimum 60% thought put with maximum 160 node in network when five nodes are placed as malicious nodes within network environment.

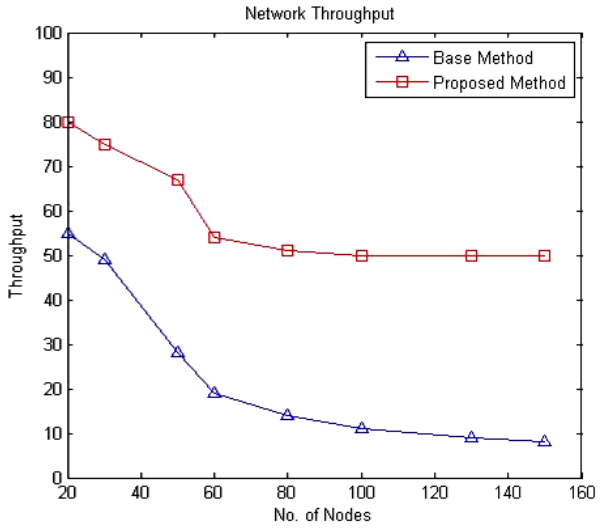

Fig 7. Network Throughput for AODV under Five Malicious Nodes

Table 2: Network Throughput for AODV under Five Malicious Nodes

Nodes	Base Method	Proposed Method
20	55	80
30	49	75
50	28	67
60	19	54
80	14	51
100	11	50
130	9	50
150	8	50

5. CONCLUSION

As the use of Mobile accidental Networks (MANETs) has inflated, the MANETs security has become additional necessary consequently [23]. Little questions the IDS area unit here to stay our systems safe; but, future systems will certainly take a unique kind from our contemporary versions. During this survey analysis, we've got mentioned Classification of selfish nodes detection techniques, varied Intrusion detection techniques, varied Innovated selfish node detection techniques and varied projected selfish node detection techniques for mobile accidental networks.

In this paper, routing security issues in MANETs are discussed in general, and in particular the malicious node attack has been described in detail. A security protocol has been proposed that can be utilized to identify malicious nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the malicious nodes. As next step is to simulate more scenarios in which more complicated misbehaviors exist and other metrics need to be measured such as latency and end-to-end delay.

6. REFERENCES

[1] J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1 –22, 2010.

[2] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 275–283.

[3] Y.-A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 135–147.

[4] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Communications Magazine, vol. 43, no. 7, pp. 101–107, July 2005.

[5] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in Proceedings of the 7th International Symposium on Communication Theory and Applications, 2003, pp. 99–104.

[6] H. Deng, Q.-A. Zeng, and D. Agrawal, "Svm-based intrusion detection system for wireless ad hoc networks," in Proceedings of 2003 IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall., vol. 3, Oct. 2003, pp. 2147–2151.

[7] C.-Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for aodv," in SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. New York, NY, USA: ACM, 2003, pp. 125–134.

[8] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for mobile ad-hoc networks," in Proceedings of P2PEcon, 2003.

[9] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputationbased incentive scheme for ad-hoc networks," in Proceedings of 2004 IEEE Wireless Communications and Networking Conference, WCNC '04., vol. 2, March 2004, pp. 825–830 Vol.2.

[10] S. Buchegger and J.-Y. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in Proceedings of WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003.

[11] Jaya Jacob, V.Seethalakshmi. "Performance Analysis and Enhancement of Routing Protocol in MANET", International Journal of Modern Engineering Research (IJMER) ,Vol.2, Issue.2, Mar-Apr 2012 pp-323-328.

[12] Sandeep Lalasaheb Dhende, Prof. D. M. Bhalerao "Detection/Removal of Black Hole Attack in Mobile Ad-Hoc Networks" International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 6, August 2012.

[13] Gambhir, S. ; Sharma, S., "PPN: Prime product number based malicious node detection scheme for MANETs", IEEE 3rd International on Advance Computing Conference (IACC), Page(s): 335 – 340, IEEE, 2013.

[14] Gaeta, R. ; Grangetto, M., "Identification of Malicious Nodes in Peer-to-Peer Streaming: A Belief Propagation-Based Technique", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, Issue: 10, Page(s): 1994-2003, IEEE, 2013.

[15] Hongjun Dai ; Huabo Liu ; Zhiping Jia ; Tianzhou Chen , "A Multivariate Classification Algorithm for Malicious Node Detection in Large-Scale WSNs", International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Page(s): 239 - 245, IEEE, 2012.

[16] Singh, M. ; Mehta, G. ; Vaid, C. ; Oberoi, P., "Detection of Malicious Node in Wireless Sensor Network Based on Data Mining", International Conference on Computing Sciences (ICCS), Page(s): 291- 294, IEEE, 2012.

[17] Chang, J.-M. ; Tsou, P.-C. ; Woungang, I. ; Chao, H.-C. ; Lai, C.-F., "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, , Volume: PP, Issue: 99, Page(s): 1- 11, IEEE, 2014.

[18] Narayanan, S.S. ; Radhakrishnan, S., "Secure AODV to combat black hole attack in MANET", International Conference on Recent Trends in Information Technology (ICRTIT), Page(s): 447-452,IEEE, 2013.

[19] Amaresh, M. ; Usha, G., "Efficient malicious detection for AODV in mobile ad-hoc network", International Conference on Recent Trends in Information Technology (ICRTIT), Page(s): 263- 269, IEEE, 2013.

[20] Michael G Solomon and Mike Chappel. Information Security Illuminated. Jones and Bartlett, 2004.

[21] Tariq Siddiqui, Tanveer Farooqui, "A Survey on Malicious Node Detection in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, Pages 156-162, December 2014.

[22] Harveen, Vanita singh, "Detection of Non Consecutive Malicious Nodes Under Black Hole Attack In Manet", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3 Issue 11, Pages 3863-3870, November 2014.

[23] Sagar Adiya, Rakesh Pandit & Sachin Patel, "Survey of Innovated Techniques To Detect Selfish Nodes In MANET", International Journal of Computer Networking, Wireless and Mobile Communications, Vol. 3, Issue 1, Pages 221-230, IJCNWMC, Mar 2013

[24] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks" 2011.

[25] Wenjia Li, Anupam Joshi, Tim Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-dimensional Trust Management Approach", Eleventh International Conference on Mobile Data Management, MDM 2010, Kanas City, Missouri, USA, 23-26 May 2010.

[26] Chandandeep kaur, Dr.NavdeepKaur, "Detection and Prevention Techniques for Wormhole Attacks", International Journal of Computer Science and Information Technologies, Vol. 5 (4), Pages 4926-4929, IJCSIT 2014.

[27] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", 2012 International Conference on System Engineering and Technology September 11-12,Bandung, Indonesia, IEEE, 2012.

[28] Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández and Pedro García-Teodor, "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs", 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[29] Humaira Ehsan, Farrukh Aslam Khan, "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs", 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[30] Ruchi Aggarwal, Simmy Rana, "A Comparitative Survey on Malicious Nodes and Their Attacks in MANET", Volume 16, Issue 3, Ver. VII, PP 93-101, IOSR Journal of Computer Engineering (IOSR-JCE), 2014.

[31] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of Cooperative black hole attack in manet", Journal of Networks, Vol. 3 (5), pp.13-20, 2008.

[32] Amos J Paul ,Vishnu K "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" International Journal of Computer Applications, Volume 1–No. 22, Pages 0975 – 8887, 2010.

[33] Saurabh Gupta, Subrat Kar, S Dharmaraja , "BAAP: Black hole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCCT), IEEE, 2011