Reliable and Hybridized Trust Based Algorithm to Thwart Blackhole Attacks in MANETs using Network Preponderant Determinants

https://doi.org/10.3991/ijim.v14i19.16391

M. Thebiga (✉), R. Suji Pramila
Noorul Islam Centre for Higher Education, Kumaracoil, India
theebs.m@gmail.com

Abstract—This Mobile adhoc networks is a perpetual and autogenous organization without framework, and the mobile nodes are coupled cordlessly. Owing to the deficiency of framework assistance, reliable data distribution is a demanding process in mobile adhoc networks and this mobile adhoc network is unguarded to many categories of attacks. A black hole attack in Mobile Adhoc networks cites to an attack by the malevolent node which strongly get hold of the path from sender to the receiver, by means of perversion of subsequence word. With regard to diminish the menace from the malevolent node, the authors encompass the notion of trust in mobile adhoc networks. In this paper, we cope with a packet dropping misconduct named Black hole Attack and we propounded a new hybrid trust based secured algorithm hinged on four new parameters to scrutinize, whether the transitional nodes are transmitting the packets correctly to the adjacent nodes and to pinpoint the malevolent node hinged on the computation of trust value. Using ns2 simulator, we analyse the performance of our proposed method and proved the detection efficiency. The investigated results show that our proposed work can precisely diagnose the malevolent nodes and assure a good packet delivery ratio and network throughput.

Keywords—Mobile adhoc Networks, Blackhole Attacks, Trust, Malevolent node, Packet Dropping

1 Introduction

The Mobile Adhoc Networks is said to be a self-patterning network, in which it was encompassed with assorted mobile nodes. With present day advancement in wireless type automation and in Movable devices, Mobile Adhoc Networks [1] have turned favoured as a leading transmission technology in military judicious background like organization of transmission networks acclimated to organize military positioning among the combatants, automobiles and command centres [2]. Mobile adhoc networks are universally employed in practice, for instance, personal area network, entertainment, disaster recovery and mainly military applications, vehicular networks, robot networks [3, 4]. Dissimilar reliable procedures such as cryptographic

techniques, corroboration, secretiveness, and message integrity have been suggested to evade safety menaces like packet snooping, message rebroadcasting and Prevarication of messages.

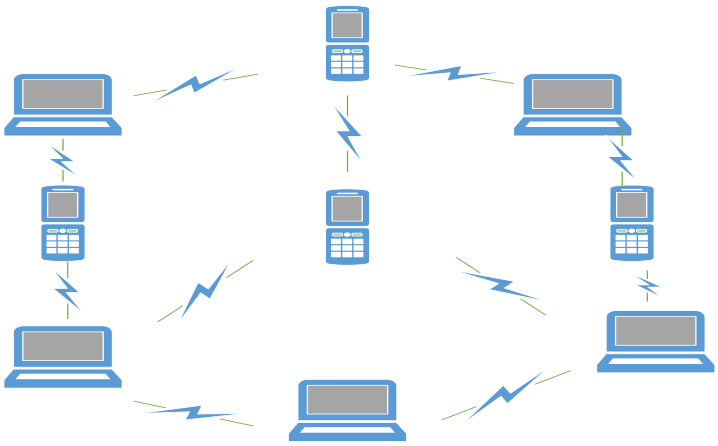

Fig. 1. MANETS ARCHITECTURE

Despite that, these practices are nevertheless abiding from security susceptibilities such like node seize attack and denial of service attacks. Contrarily, the mobile adhoc networks are endangered to dissimilar threats on every layers. Accustomed reliable methods such as encryption and authentication techniques will not deliver an absolute defence, thus trust-based approaches are employed to protect the mobile adhoc network. Attacks in mobile adhoc networks can be categorized into two divisions, based on the guidelines whether they distort the performance of the network or not: active assaults and passive assaults. In apathetic type of attacks, the intruder strives to disclose the most beneficial information without distorting the performance of the protocol. Active attacks are a system utilization, in which the intruder seek to fabricate variation in data, which incorporates activities such as data reorganization and data evacuation. [5]. To organize a reliable and secured transmission, it is required to confirm that every transmission nods are trusted. Traditional reliable methods incorporate enciphering and authentication methods which are incongruous, because it can defy only extrinsic attacks and not intrinsic attacks created by internal malevolent nodes which may results in consequential impact on protection, secretiveness and circuition of the network. Trust Management techniques was contemplated to be an efficacious method to crack those issues [6]. Trust can be elucidated as personalized belief that an individual had about someone else forthcoming performance hinged on chronicle of their experience [7]. From the survey, we can observe that in present day investigation, the rating of trust values is predominantly premised on eminent interaction and ineffectual interaction perspective. In consideration of only the transmission character, we are not able to conclude, that the mobile nodes are trusted or not. In our proposed work, in addition to the interaction factor, other trust measures like forwarding potential ratio, self-forwarding potential ratio, Holdup time and energy are taken

into consideration to compute the reliability of mobile nodes. In this paper, we have propounded an efficient and hybrid trust-based model for thwarting the black hole attacks in Mobile Adhoc Networks. Here we use the undeviating and deviating perception to figure out the trusted value of a specific node in a network. The undeviating perception is premised on the straight forward interoperations which includes forwarding potential ratio, self-forwarding potential ratio, hold up time and delay to compute the undeviant trust and the deviating perception is contingent on the commendation from the third person. Despite that, not every third parties are trustworthy and not every commendation from the third person are faithful [8]. As a result, a scrupulous investigation regarding the third party and their commendation is indispensable.

The contribution of this work can be summarized as

1. We propounded and examined a new revelation and hindrance technique for black hole attack based on new hybrid trust-based concepts.
2. Undeviant trust can be computed using new four network parameters which analyse the causes for packet drip, such like forwarding potential Behaviour ratio, Self –forwarding Potential Behaviour ratio, Hold up time and energy level.
3. Deviant trust can be calculated by using recommendations from the honest recommenders. The honest recommenders are perceived based on two factors called deflection level and Euclidean distance.
4. We implement and exhaustively analyse the detection and hindrance mechanism through a comprehensive set of simulation using NS2 simulator. We equate our proposed work with earlier existing solution and exhibit that our proposed work exceeds them in form of packet delivery ratio, detection precision, packet drip ratio, computation expenses, energy consumption and communication overhead.

2 Related Works

Jian [9] et.al suggested a technique named CBDS which effectually exposes the malevolent nodes that endeavours to initiate synergetic black hole attack or greyhole attack. In this method, the location of a contiguous node is employed as entrap target address to fascinate the noxious node to convey a respond message and finally the malevolent node is discovered by reversal tracking method. Identified malevolent nodes are preserved in a black hole register and every other node is cautioned to cease transmission with every node involved in the register. This method harmonizes the merits of both proactive and reactive technique to accomplish the target.

Kumari [10] et.al propounded a new resistance against creation of multiple phony identities and verification for unidentified site dependent routing in Mobile adhoc Networks. Every arbitrary redirector maintains a table with RSS values which is measured from former message interchange. The discrepancy in RSS ratings of two adjoining nodes is calculated premised on what sort of the nodes appearance position into the region is noticed. Based on appearance position, the nodes region is organized into Secured region and alert region. The messages that are interchanged in-between the originator and arbitrary redirector are guarded by way of group signatures.

Ultimately, Misdirected packet drip attack is recognized and abolished by ant colony enhancement approach with forward and backward ant agent. The demerits over this procedure is usage of group signature is an extravagant procedure.

Shu [11] et.al suggested a meticulous algorithm to diagnose the choosy packet drip created by intrinsic attackers. This approach also issues a reliable and openly checkable decision numeric to assist the detection. Great spotting precision can be accomplished by utilizing the association between the dropped packets, and they are estimated using auto association function of bitmap. We are not confident that the information presented by the nodes are trusted or not. The truthiness of information given by the nodes can be checked using public auditing method hinged on Homomorphic Linear authenticator cryptographic procedure. This approach issues high transmission overhead, memory overhead and calculation overhead. To diminish calculation overhead, block-based procedure is proposed. The demerits of this approach are its peculiar to motionless and quasi motionless wireless networks. Active changes in network configuration and bonding features are not contemplated.

Baadache [12] et.al recommended a new technique to diagnose the black hole attack in mobile adhoc networks. It is a substantiated stem to stem acceptance dependence technique and it obviously inspect whichever the transitional nodes are conveying the packets flawlessly or not. This approach can be capable of diagnosing Bothe individual and combined black hole attack, reoccurrence attack and alteration attack. In this approach, prior to conveying the message, the originator set up an arbitrary number, and encipher that given number. Subsequently, the originator estimates the hashed value and encipher that fabricated hashed value by means of a publicly open key and convey that enciphered value to the receiver (MGE, H, and e). Once the message meets the terminus node, it equates the hashed value. If the hash values are unequal, further we conclude that conveyed message is adjusted and if both the hash values are equal, then we conclude the conveyed messages are not adjusted. Ultimately, the receiver will encipher the function and send back to originator. The originator will decipher the message and estimates the function $x=f^{-1}(d)$ and finally the value of x is equated with value of r. If both values are unequal, then no messages are redirected to the next node and after that the precise node is isolated as malevolent node.

Muhammed [13] et.al suggested a new method to notice the malevolent node by diagnosing the real grounds of packet drip. The author suggested a new technique that can be accurately diagnose the malevolent node using the network basic criteria to judge that the packet drip such like, MAC layer information, queue congested or nodes motility in networks. A trust dependent technique is recommended to diagnose the malevolent node depending on the fine-grained examination of packet drip. This method is applicable only for small subsets of nodes and not for other routing protocols.

Priya [14] et.al presented a revised model of Dynamic Source Routing for diagnosing and eradicate the critical black hole attack in Mobile adhoc Networks. In this approach, Irruption recognising System nodes are positioned in a relaxed style to diagnose some instantaneous adjustment in the usual character of a node. If there is any variation in the usual character, the contiguous Irruption Recognising System node would convey a caution report with information about the hostile nodes to all its

accessible nodes. When the total count of accepted packets is below the total count of posted packets, then we need to initiate the diagnosing process. If the variability in number of posted packets in-between the contiguous nodes run over the preset threshold value, subsequently that particular two contiguous nodes are labelled as fishy nodes and the knowledge regarding the fishing nodes are conveyed to all its accessible nodes. If this fishy node wilfully drops the packets, then that particular nodes are termed as hostile nodes and its secluded from the network.

The [15] et.al recommended a new statistical dependent procedure to diagnose the black hole attack and greyhole attack in Delay Tolerant Networks. By employing the given concept, the author can able to diagnose both single and combined attack. By employing the forwarding metrics, the single hostile nodes are diagnosed and that can discriminate the demeanour of assaulter from the ordinary node. To unremittingly drip the packets and to support the forwarding measures simultaneously, the assaulters will construct a bogus encounter registers habitually and with high bogus number of posted messages. The author utilizes this eccentric pattern of arrival frequency and the count of posted messages in bogus encounters to depict a procedure to diagnose the combined attack.

Rajesh [16] et.al suggested a new probabilistic dependent technique with honey pot approach is employed to pinpoint and to obstruct the Blackhole attack in mobile adhoc networks. In this approach, the architecture has three stages. Detection stage, Routing consulting stage, and lastly sequestration stage. In the first stage of Revelation stage, the originator conveys a sham Route Request packet and if any one node riposte to the request packet, that node will be labelled as hostile node. In the second stage, the routing consulting table would examine either the reply is for the bogus request. In this fashion, the proposed approach will perform as honey pot to fascinate the attackers by despatching the bogus route request. In the last stage, Isolation stage, the hostile nodes are diagnosed and their recognition are conveyed to all transitional nodes.

3 Blackhole Attacks in Manets

The Black hole attack is a kind of active attack, in which the malevolent nodes asserts that it comprises the quickest track path to the craved target node, even though it doesn't have path to that target node. In computer networking, the black hole attack is a sort of denial of service attack, where the router will get rid of packets in place of conveying them. Therefore, every packet will be directed to that node and this will empower the black node to drip the packet or to redirect the packet [18]. In other words, the hostile nodes publicize the non-legitimate path as legitimate paths to the initiator at the time routing process. Initiator node trust the nodes which send fake replies. Normally the standard nodes will keep faith on every reply for every request and the hostile nodes make use of this and replies to all requests, informing that it contains the quickest path to the craved destined node. The usual nodes initiate the route exploration process for the purpose to seek the route to the destined node. The provenance node conveys a Routing Request to the destined node, any of those nodes

accepting this Route Request will examine if it has any new route to the target address. When the black node accepts this Route Request, it instantaneously responds that it comprises the quickest path to the destined node. The initiator presumes that response, because of the fact that there is no other means to confirm that the response is from non-malicious node or from black node. The originator initiates transmitting packets to the hostile Node, having a belief that the forwarded packets will be delivered to the target address, but the malevolent node initiates dropping packet. The two types of black hole attack are individual black hole attack and combined black hole attack. In the individual black hole attack, only there will be the presence of one malevolent node and in combined black hole attack, multiple malevolent nodes combine together to downgrade the system performance and important functionalities of the nodes in the network.

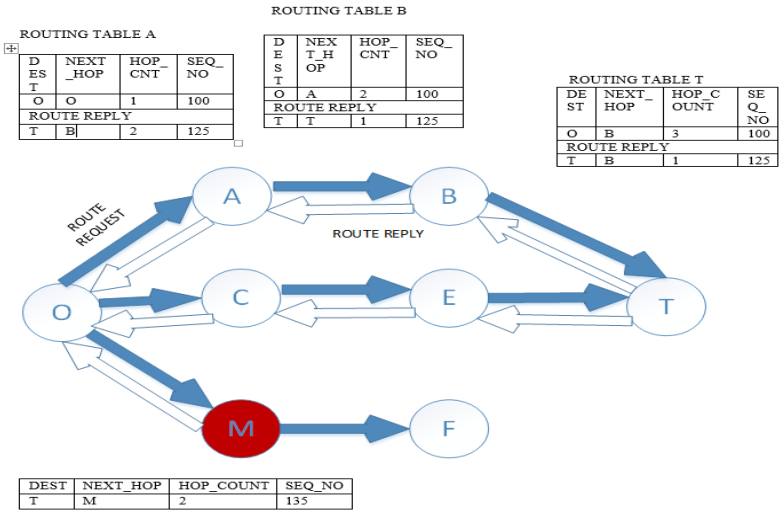

Fig. 2. Blackhole Attacks in Manets

The fig 2 expounds that how the black hole issue occurs, here node 'O' is the originator which wants to interact with the target node 'T' and initiates route determination process by conveying Route Request data packets to all of its nearby nodes A, C and M. The Route Request contains fields such as Source Identifier (SRC_ID), Destination Identifier (DEST_ID), Source Sequence Number (SR_SEQ_NO), Destination Sequence number (DEST_SEQ_NO), Broadcast Identifier (BR_CA_ID) and Time to Live field (TI_LI.).Every node creates a routing table once it receives the Route Request packet. Node 'M' is the malevolent node and it will fabricate a hoax Route Reply packet with less skip count and declare that it contains the quickest track path to the destined node, immediately after accepting the Route Request from the originator node 'O'. It will respond with Route Reply to the originator node 'O', before any other node responds. In this manner, the originator node 'O' presumes that it was the fresh, dynamic and active path and it snubs all other responds from other nodes and

initiates data transmission to the malevolent node 'M'. At last all the packets forwarded to the malevolent nodes will be dropped or consumed. From the routing table of A, we get the information that to reach the destination O the next hop is O from A with hop count 1 and from the route reply we know that to reach the target node 'T', the next hop is 'B' from 'A'.

4 Proposed Work

Routing is considered as a crucial action in every categories of network, and it has a remarkable significance in mobile adhoc networks. Consequently, any interrupt in the routing procedure has an unmediated crash on the working accomplishment of this network. This is exactly why the routing process is purports in different categories of attacks in mobile Adhoc Networks, specifically, Black hole attack. Here, the proposed technique is created to descry and to defy the black hole attacks by postulating a secured hybrid trust-based concepts. In this paradigm, trust is composed of two constituents called Deviant trust and undeviant trust. In Undeviant Trust, a perceiver evaluates the trust value of its one skip neighbor depending on its personal persuasion which includes new four parameters. It is equivalent to the First-Hand details. If we take into consideration only the undeviant perception, then there would exist predilection in computing the trust value.to acquire least bigoted trust values, we also take into account, other perceiver nodes persuasion. Combining the undeviant trust and deviant trust, we are able to achieve a genuine and meticulous trust value for a node in Mobile Adhoc Networks.

$$\boldsymbol{Tru_{Val}}\text{=W1 *UD\_Tr (i) + W2*DEV\_Tr (i)} \quad (1)$$

4.1 Energy level trust

Energy is considered to be a prime factor in mobile adhoc networks because the mobile nodes involved in the network contingent on the volume of energy they have. The malevolent node will habitually engross untypical energy to initiate malevolent attacks. For instance, the malevolent nodes which initiate the attacks will engross more volume of energy whereas the self-seeking nodes engross less volume of energy. Consequently, the energy is employed as a quality measures to check whether that particular mobile nodes is a self-seeking node or caustically debilitates extra energy. By means of energy prophecy model, Energy Exhaustion (EY_{EXH}) of every mobile node can be calculated at various intervals are monitored. When the Left_Over Energy (EY_{LEFT}) Value of mobile node is beneath than the preset threshold value, then that specific node is not proficient to execute its given task. From this, the energy trust value can be taken as '0'. The Energy Trust (EY_{TRU}) Value can be estimated, in accordance with the energy exhaustion rate [0, 1].Greater the energy exhaustion rate is lesser the left over energy which may results in less potential for the nodes to finish the mission. The energy trust [19, 20] can be given as

$$EY_{TRU} = \begin{cases} \mathbf{1 - EY_{EXH}\ EY_{LEFT}\ \geq Thr_{EY_{LEFT}}} \\ \mathbf{0\ elsewhere} \end{cases} \quad (2)$$

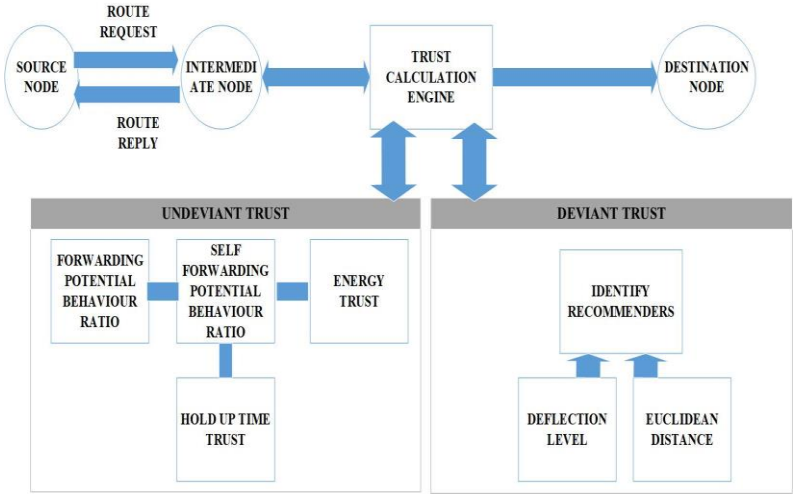

Fig. 3. System Architecture

Where Energy Exhaustion rate of node 'A' during conveying and accepting message can be given as

$$CV\_Cost = Ey\_Con * No\_Bits + Ey\_Snr * No\_Bits * (DIST)^2 \quad (3)$$

$$Accpt\_Cost = Ey\_Con * No\_Bits \quad (4)$$

CV_Cost is the conveying cost, Accpt_Cost represents the accepting cost, Ey_Con represents the unit energy exhaustion while conveying message, No_Bits represents the number of bits in message, Ey_Snr represents the energy required to accomplish determined signal to noise ratio, and DIST represents the distance between specified nodes.

Then Total Energy Exhaustion rate for a node 'A' can be given as

$$\mathbf{EY_{EXH}} = 2 * Ey\_Con * No\_Bits + Ey\_Snr * No\_Bits * (DIST)\ 2 \quad (5)$$

If the starting energy status of a node is Ey_start and the left-over energy status (EY_{LEFT}) for a node 'A' can be given as

$$(EY_{LEFT}) = Ey\_start - \mathbf{EY_{EXH}} \quad (6)$$

This specifies that precise node has the competence to collaborate with another nodes as energy filled nodes, when the left-over energy is beyond the preset threshold value, or else it cannot be involved in the transmission process.

4.2 Forwarding potential behaviour ratio

The assaulters may accept an abundance of messages, but it conveys only a diminutive fraction of messages and the remaining have been dripped. Out of that messages transmitted by the self-seeking assaulters, a huge part of messages is fabricated by itself and they drip others messages but reserve their own messages. Depending on this perception, two important measures such as Forwarding potential ratio and self-forwarding potential ratio has been elucidated.

Forwarding Potential ratio can be elucidated as the fraction of total count of packets perceived and already conveyed by a particular node and the total count of packets accepted and Forwarding potential ratio has been given as

$$\text{FPB}_{\text{ratio}} = \frac{T_{PRF}}{T_{PER}} = \frac{\textbf{Total no of packets received and forwarded}}{\textbf{Total number of packets received}} \tag{7}$$

To be a normal node the FP ratio must be greater than the preset threshold FPB ratio $\geq THR_{FPB}$.

4.3 Self -forwarding potential behaviour ratio

The second metric Self-forwarding potential ratio [SFP ratio] can be elucidated as the ratio of total count of packets produced by a node by its own and conveyed to the total population of packets forwarded by a particular node and it can be expressed as

$$\text{SFPB}_{\text{ratio}} = \frac{T_{POF}}{T_{PF}} = \frac{\textbf{Total number of packets genertaed by its own and forwarded}}{\textbf{Total number of packets forwarded by particular node}} \tag{8}$$

To be a normal node the SFP ratio must be lesser than the preset threshold SFPB ratio $\leq THR_{SFPB}$.Owing to the dripping mischief, the malevolent node has lesser forwarding potential ratio and larger self-forwarding potential ratio when compared to the normal nodes. Once these measures are calculated, the particular node will equate them the preset threshold values [15]. If the forwarding potential ratio is less than the threshold value, the grade of the node is diminished and if the self-forwarding potential ratio is superior to the preset threshold value, the status of the node is further diminished. And finally, for the nodes whose status exceeds the threshold value (THR_{ACPT}) are considered as trusted node. All the threshold values are preferred analytically using simulations.

4.4 Hold-Up trust

The HOLD_UP time is a predominant pattern and achievement attributes in computer networks. Delay in Mobile adhoc networks is comprised of various categories such like Processing Delay, Media Access Delay, End to end Delay, Propagation Delay. The expansion of hold up time, can be the result of hindrance or contention and some other causes such like distance of the path, intercession. At the same time, it

is very predominant for the mobile adhoc networks to evade the network hindrance and contention for the purpose to maximize the performance and yield of the network. The packet in a network can be vanished, so some trustworthy techniques needed to verify the reason for packet drip. On account of this delay, buffer overrun transpires, when an exit link from a node has a burden factor that outperforms 1.0. that is, the data entering into the queue is quicker than the data get conveyed. As a result, the queue span gets expanded and there will be no lacuna in the queue.at that moment, there would be no option, but the packet will be renounced. Finally, the delay will also be one of the main grounds for packet drip. And it should be minimized.

Node hold up time can be defined as the time exhausted at every node for accepting and conveying the packets to the up-line router after waiting and it can be given as [21,22].

$$(HLD_{trust}) = HL_{proc} + HL_{queue} + HL_{trans} + HL_{prop} \tag{9}$$

Where the HL proc is the Processing Hold up time which can be elucidated as the time demanded for working on a packet and it is literally imperceptible with other phrases. HL queue is the Queuing hold up time which can be explicated as the time demanded for a packet to expend in a queue at a node, in the time expecting for another packet to be conveyed. It is something related to transmission hold up time.

$$HLqueue = HL_{trans} * Que_{Len} \tag{10}$$

HL Trans is the transmission hold up time which can be expounded as the time demanded to put a whole packet in to the transmission media and it can be given as

$$HL_{Trans} = \frac{PKT_{size}}{D_{rate}} \tag{11}$$

Where PKT_{size} the packet size and D_{rate} is the data rate in bits per second. HL prop is the propagation hold up time is the time required for a message to reach the target address and it can be given as

$$\boldsymbol{HL_{prop}} = \frac{\boldsymbol{Dist_{Route}}}{\boldsymbol{Link_{speed}}} \tag{12}$$

Where $Dist_{Route}$ is the distance of the path and $Link_{speed}$ is the link speed.

4.5 Work flow diagram of proposed work

Fig 4 describes When an originator node ‘O’ needs to convey a packet to the target node ‘T’, the originator node initiates a Route Request (RO_REQ) packet to all its adjacent nodes. The precise nodes that are having path to the target node will responds with the Route Reply (RO_REP) packet. The originator node should wait for ‘t’ seconds, until receives reply for all other neighbour nodes. After’s’ seconds, the originator node will enter into the initial phase and it will check the prevalence pattern ($PREV_{pattern}(k_b)$) for all the replied nodes, starting from first replied nodes to last. Prevalence pattern can be elucidated as the product of the number of time that particu-

lar Node is chosen as neighbor node and the number of messages sent between the two nodes.

$$\boldsymbol{PREV_{pattern}(k_b)} = \boldsymbol{OFTEN_{times}(m_i\ k_b) * NOM_{node}(m_i\ k_b)} \quad (15)$$

$OFTEN_{times}(m_i\ k_b)$=number of times choosing the node as neighbour node
$NOM_{node}(m_i\ k_b)$ = number of messages send between the two nodes

If the computed prevalence pattern is beneath the predefined threshold value(THR_{prev}), then that particular node is normal node and transmits the route request packet to the next node. If the calculated prevalence pattern is beyond the predefined threshold value, then that node should be added to the suspicious list. The nodes that are added to the suspicious list will enter into the second phase called trust computation, to check whether that node is trusted or not.

In the trust computation phase, the trust for the particular node is calculated using undeviant trust and deviant trust. If the computed hybrid trusted value is greater than the preset threshold value, then that particular node is a legitimate node and it is authorized to convey the packet to the succeeding node and if the computed hybrid trust value is less than the predefined threshold value, then that node is added to the black hole list and isolated form other node and information about the black node is broadcasted to all neighbouring nodes in the network. The hybrid trust value can be calculated as

Trust Value =W1 *UD_Tr (i) + W2* DEV_Tr (i)

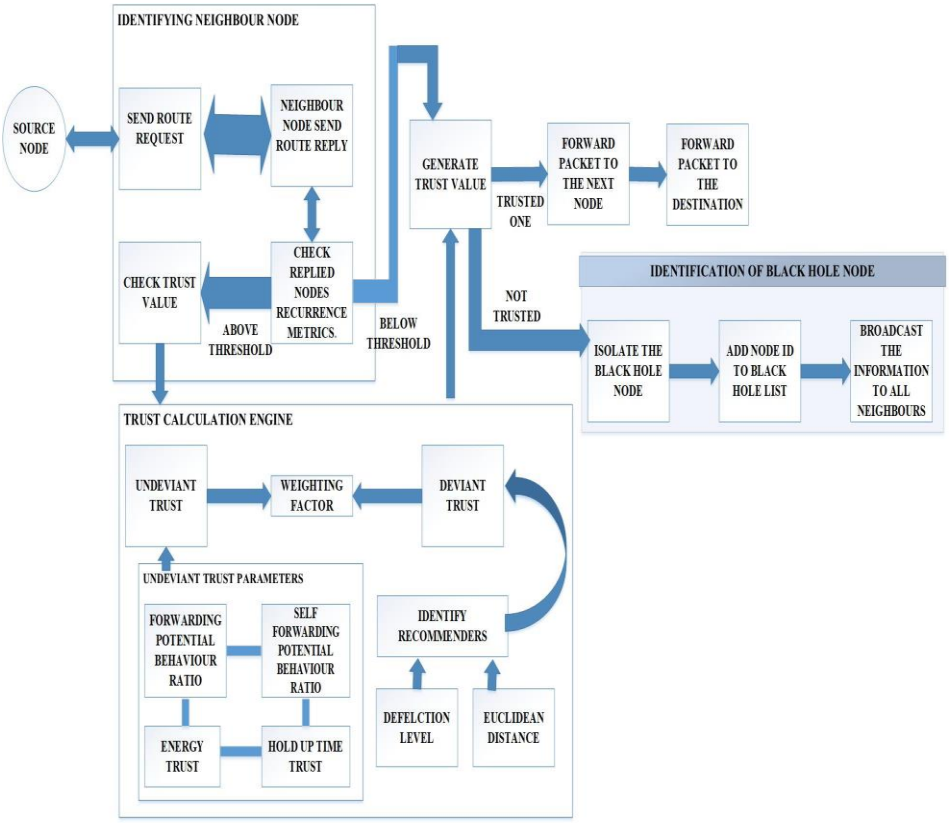

Fig. 4. Work flow diagram of Proposed Work

5 Undeviant Trust

Undeviant trust is computed from a nodes personal perceptions of its contiguous nodes. In our proposed work, the undeviant trust can be calculated using new four network parameters such like forwarding potential behaviour ratio, self-forwarding potential behaviour ratio, hold _up time trust and finally the energy level trust.

$$\text{UD\_ Tr (i)} = \frac{1}{4}[\text{FPB}_{\text{ratio}}] + \frac{1}{4}[\text{SFPB}_{\text{ratio}}] + \frac{1}{4}[EY_{TRUST}] + \frac{1}{4}[HLD_{TRUST}] \quad (16)$$

6 Deviant Trust

Recommendation from the contiguous nodes performs an imperative part in evaluating the trustiness of a perceived node. Despite the fact that, undeviant perception from the perceiver is predominant in reckoning the trust value of the perceived node, the evidence from the contiguous node are also valuable in assessing the trustiness of

the perceived node. Accumulation of contiguous nodes persuasion, can assist in exculpating whether a node is malevolent or not. This process may diminish the bias from the perceiver. Inorder to get proper and correct persuasion from the nodes, the honest recommenders should be chosen. In our work, the honest recommenders are selected based on two criteria's: deflection level and the Euclidean Distance. If the selected node has deflection level lower than the predefined threshold value and the Euclidean distance between the two nodes should be lower than the predefined threshold, then that nodes are chosen as good recommenders and their persuasions are taken into consideration to calculate the deviant trust.

6.1 Euclidean distance

Euclidean Distance estimates the physical distance in-between the perceived node and the suggesting nodes. The utilization of familiarity between the nodes enriches this proposed work, the reason is, the nearest nodes are more likely to acquire similar quality and working criteria's and similar environment for a specified duration. Likewise, the familiar persons may have more communications, associations for the period of friendship. As a consequence, the trusted value for the familiar neighbours may intersect to nearly similar level. This may assist in diagnosing the untrusted suggestion nodes where suggestions are greatly varied from the close suggesting node [23].

$$\boldsymbol{DIST^{a}_{b(NODE)}} = \sqrt{(\boldsymbol{X^{a}_{POS}} - \boldsymbol{X^{b}_{POS}})^{2} + \boldsymbol{Y^{a}_{POS}} - \boldsymbol{Y^{b}_{POS}})^{2}} \quad (17)$$

Where $\boldsymbol{DIST^{a}_{b(NODE)}} \leq \boldsymbol{THR_{DIST}}$

$DIST^{a}_{b(NODE)}$ Represents the Physical distance in-between the perceived node 'a' and the suggesting node 'b'. $X^{a}_{POS}, X^{b}_{POS}, Y^{a}_{POS}, Y^{b}_{POS}$ represents the location of the node a and the b at time 't' sec.Recommenders are chosen if the Euclidean distance between the perceived nodes and the suggesting nodes should be less than the distance threshold value.

6.2 Deflection level

The deflection Level portrays to what augment, the accepted suggestion is harmonious with the personalized participation of perceiving node. Every node equates the accepted suggestions with its personal unmediated details and approve only those nodes that not devious bit much from its own perception [24]. In this propounded work, the deflection level is employed as an auxiliary parameter to drain out any suggestions deflecting over the preset threshold value. The node estimates the deflection level as the difference between the accepting suggestions and unmediated perception of the observed node. The resultant is equated with the preset deflection threshold and we rule out any suggestions that vary from the perceiving nodes self-details.

$$\boldsymbol{D\_LEVEL^{i}_{j}} = \left|\boldsymbol{D\_TRST^{i}_{j}} < \boldsymbol{TRUST^{k}_{j}}\right| \leq \boldsymbol{THR_{D\_LEVEL}} \quad (18)$$

The honest recommenders are chosen based on two criteria's such as low deflection level and short distance and the deviant trust is calculated for that particular node. The deviant trust can be calculated as

$$\boldsymbol{DEV\_TRUST}_j^i = \text{Init}_{\text{Trust}} + N * \left[\frac{\sum_{i,j=1}^{N}(\boldsymbol{NOGR}_{j(NODE)}^i * \boldsymbol{REscore}_{j(NODE)}^i * \boldsymbol{BLF}_{j(NODE)}^i)}{\sum_{i,j=1}^{N}(\boldsymbol{DIST}_{j(NODE)}^i * \boldsymbol{Max}_{\boldsymbol{LRE}} * \boldsymbol{Tot\_RE\_rcvd})}\right] \quad (19)$$

$\text{Init}_{\text{Trust}}$ is Initial Trust, N is Number of Recommenders, $NOGR_{j(NODE)}^i$ is the Number of good recommendations received, $REscore_{j(NODE)}^i$ is the Recommendation Score $BLF_{j(NODE)}^i$ is Belief Factor $DIST_{j(NODE)}^i$ is Distance between the perceived node and suggesting Node. Max_{LRE} is Maximum Limit for Response, Tot_RE_rcvd is the Total No of Recommendation received. Recommendation score can be given as the ratio of total count of good recommendation and total count of both Good and Bad recommendation and it can be given as

$$\boldsymbol{REscore}_{j(NODE)}^i = \frac{\boldsymbol{G_{REC}}}{\boldsymbol{G_{REC}} + \boldsymbol{B_{REC}}} \quad (20)$$

Where G_{REC} Represents Good Recommendation received from the nodes, B_{REC} Represents Bad Recommendation received from the nodes. $BLF_{j(NODE)}^i$ Can be given as ratio of number of successful interaction between the nodes and the total count of interactions between the nodes and it can be given as

$$\boldsymbol{BLF}_{j(NODE)}^i = \frac{\boldsymbol{SUC_{INTR}}}{\boldsymbol{SUC_{INTR}} + \boldsymbol{UNS_{INTR}}} \quad (21)$$

SUC_{INTR} Represents the successful interaction between the nodes, UNS_{INTR} Represents the failure interactions between the nodes.

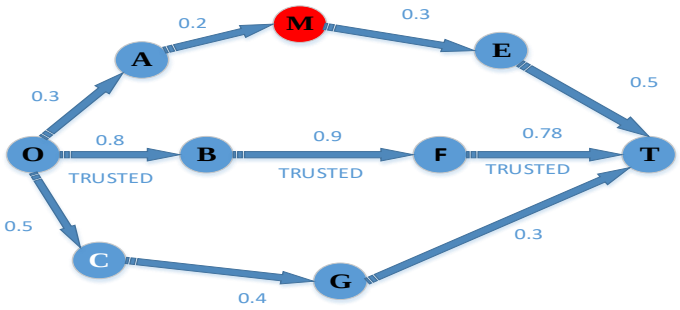

Fig. 5. Trusted Routing of Proposed work in Manets

Table 1. Algorithm 1 Initial phase

1	Source node(S) send ROREQ to all neighbour node 'm_i
2	If node k_b has route to destination
	Send ROREP
	End if
3	For each neighbour node 'm_i
	(i)Check $PREV_{pattern}(k_b) = OFTEN_{times}(m_i\ k_b) * NOM_{node}(m_i\ k_b)$
	$OFTEN_{times}(m_i\ k_b$=number of times choosing the node as neighbour node
	$NOM_{node}(m_i\ k_b)$ = number of messages send between the two nodes
4	If $PREV_{pattern}(k_b) > THR_{prev}$
5	Isolate node as suspicious node (ID)
	Calculate Trust Value COMPUTE TRUST()
	Else
6	Transmit the packet to the next node until it reach Destination
	End IF

Table 2. Algorithm 2 Compute Trust

	Compute Trust ()
1	For each isolated node (ID)
	(i) Calculate UnDeviant Trust ()
	(ii) Calculate Deviant Trust ()
2	Compute trust
	Trust $_{Value}$ =W1 *UN_DEV_Trust (i) + W2* DEV_Trust (i)
3	IF Trust $_{Value\ ((ID)}$ < Trust $_{Thresh}$
	(i) Isolate the node (ID) as Black Listed node
	(ii) Isolate Attacker (node ID)
4	Display node as Malicious.
5	Transmit the malicious node info to all nodes in the network.
	End if
	Else
	Transmit the packet to the next node until it reach the destination.

Table 3. Algorithm 3: Calculate Deviant Trust value

1	Calculate Deviant Trust ()
2	Collect neighbours list ()
	Based on small distance and less deviation level
	Choose recommenders
3	Compute Deviant Trust.
	$DEV\_TRUST_j^i$ =$Init_{Trust}$ + N * $[\frac{\sum_{i=1}^{N}(NOGR(i) * RE\ Score(i) * BL(i))}{\sum_{i=1}^{N}(Dist(i) * Max_{LRE} * Tot\_RE\_rcvd)}]$

Table 4. Algorithm 4: Calculate UnDeviant Trust value

	COMPUTE UnDeviant Trust ()
1	Calculate FPB $_{ratio}$
	FPB $_{ratio}$ = $\frac{T_{PRF}}{T_{PER}}$
2	If FPB $_{ratio}$ <THR_{FPB}
	Dropping = True
3	Calculate SFPB $_{ratio}$
	SFPB $_{ratio}$ =$\frac{T_{POF}}{T_{PF}}$
4	If SFPB $_{ratio}$ >THR_{SFPB}
	Dropping = True
5	Calculate Hold-up time TRUST
	If HLD_{TRUST}> THR_{HLD_TRUST}
6	Dropping =true
7.	Calculate Energy Level TRUST
	If EY_{TRU} < THR_{EY_trust}
	Dropping =true

8.	Calculate Undeviant Trust
	UD_ Tru (i) = $\frac{1}{4}$[FPB ratio] + $\frac{1}{4}$[SFPB ratio] + $\frac{1}{4}[HLD_{TRUST}]$ + $\frac{1}{4}[HLD_{TRUST}]$

7 Experimental Setup and Analysis

This paper utilized NS2 simulator to substantiate revelation and segregation coherence of the propounded method opposed to the black hole attacks in Mobile Adhoc Networks. With an area of 1000 x 1000 m, 50 standard nodes performing this proposed work are positioned aimlessly. Our proposed work is equated with an existing proposed work PPTDP [11]. In this section, we figure out the efficacy of our proposed work. Network simulator 2(NS2) version 2.34 has been employed to execute and examine the working performance of our proposed work. For this simulation's investigations, we differ the simulation time from 50sec to 250 sec and nodes from 10 to 50. In NS2, every dripped packet will be registered in a trace log file.so that we can investigate the outcomes of our proposed investigation by interpreting the trace log files using an AWK scripts.

Table 5. Simulation Parameters

Properties	Values
Coverage Area	1000 x 1000 m
No of Nodes	10,25,50
Simulation Time	250s
Transmission Range	250m
Mobility	Random Way Point Model
Mobility Speed	20m/s
Traffic Source	CBR
Traffic Source	CBR
Initial Energy	100Joules
Protocol	AODV

In this category of black hole attack model, a malevolent node drips data packet aimlessly with 25% probability. The number of malevolent nodes varies from 5% to 25% of the total count of nodes involved in network

7.1 Packet loss ratio

Fig 6 reveals the packet loss rate with the increasing simulation time for the existing PPTDP and proposed work. The packet loss rate for our proposed work is lesser when equated with the existing PPTDP. In our proposed work more trusted nodes are chosen for routing process, which results in small packet drip and a good packet Delivery Ratio. From the fig, we can figure out that in existing work the packet loss

has been increased from 7% to 9.4%, as the number of nodes expands from 10 nodes to 50nodes, and in the proposed work the packet loss rate has been increased from 0.7% to 2.4% as the number of nodes expands from 10nodes to 50nodes. When compared to the existing work, the proposed Technique has less packet loss rate.

$$\text{PLR}=\frac{\sum NO\ OF\ PKT\ LOST}{\sum NO\ OF\ PKT\ SENT} *100 \tag{22}$$

7.2 Detection rate

The Detection rate has been defined as the percentage of malevolent nodes detected to the total number of malevolent nodes included in the network. Fig 7 reveals the detection rate with increasing number of simulation time for existing PPTDP and proposed work. The detection rate can be referred as count of true malevolent nodes that are diagnosed by the process over the total count of malevolent nodes in the network. The detection rate for existing got increased from 60 to 85% and in the proposed work the detection rate has been increased from 80 to 95%. So the proposed work has higher detection rate even when the count of malevolent nodes increases. In the existing work, when the count of nodes got increased, the count of interactions between the networks got expanded, so more packets will be dripped because of collision and no trusted nodes are identified in the network.so detection rate for the existing PPTDP is less compared to the proposed Technique.

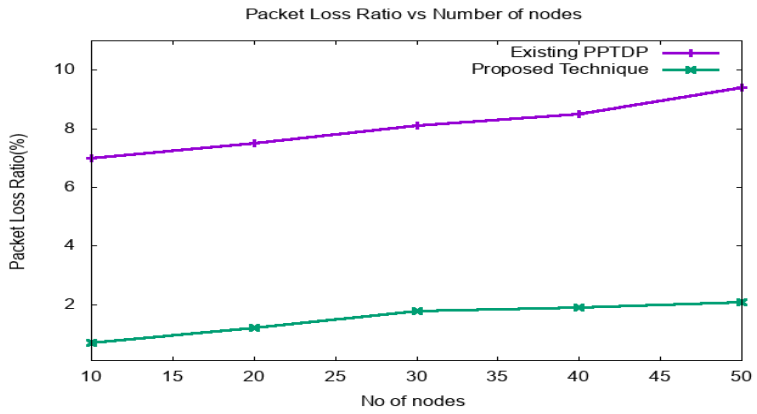

Fig. 6. Packet Loss Rate vs No of Nodes

$$\text{Detection rate}=\frac{No\ of\ malicious\ \_node\ detected}{Total\ no\ of\ malicious\ node} * 100 \tag{23}$$

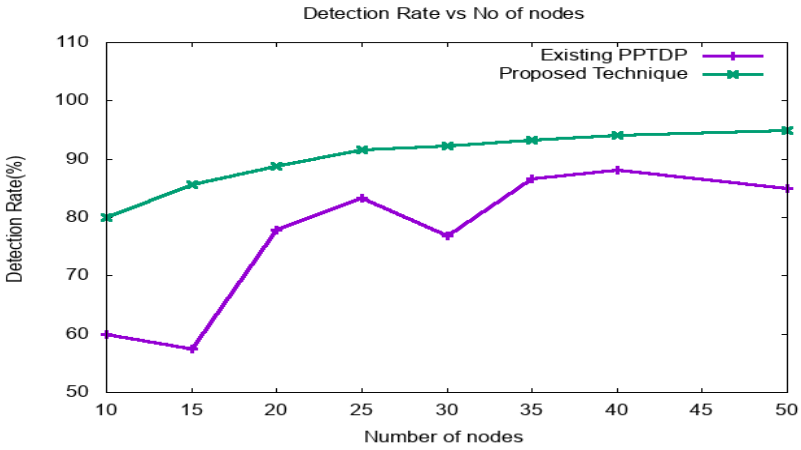

Fig. 7. Detection Rate Vs No of Nodes

7.3 End to end delay

End to End delay has been measured as the time needed by a data packet to reach the target node from the originator node. In the existing work, the trust relationship cannot be fabricated in an efficient manner, so more time is spent in detection process.

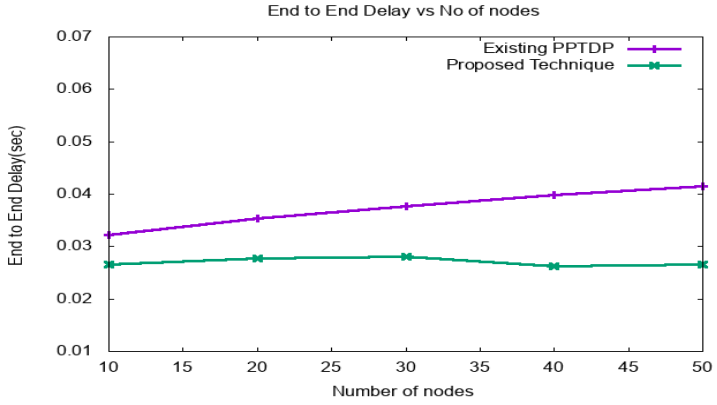

Fig. 8. End to end Delay Vs No of nodes

$$\text{AVERAGE E2E DELAY}=\frac{\sum_{I=1}^{n} Sent\_time - recv\_time}{\sum pkts\_recvd} \quad (24)$$

Fig8 reveals the end to end delay for the existing PPTDP and the proposed Technique. In the existing PPTDP, as the number of nodes increases from 10 t0 50, the delay has been increased from .0322 sec to .0415 sec, because more time is exhausted for the detection of packet drop. In the proposed work, when number of nodes ex-

pands from 10 to 50 nodes, the delay has been increased from .0265 to .028 and then dropped to. 0265.From this comparison, we can conclude that our proposed technique has less delay compared to existing PPTDP.

8 Conclusion and Future Work

In this paper, we have propounded a new-fangled hybrid trust-based concepts to diagnose the malevolent node and to resist the black hole attacks in Mobile Adhoc Networks. Our simulation results disclose that our proposed work outclass the prevailing technique PPTDP in terms of Packet delivery Ratio, Packet loss ratio and energy consumption. As a means of future work, (i) we explore the expediency of our proposed work to tackle with other types of vulnerabilities in Mobile adhoc Networks, (ii) then to apply dynamic threshold values to detect attacks, (iii) explore that combining our proposed Technique with other reliable schemes to provide a more secured routing in Mobile Adhoc Networks. We can further improve our proposed work by including more parameters. The performance of the proposed work is assessed using a simulator NS2 and results reveals that the proposed work diagnose the malevolent node with high accuracy.

9 References

[1] F. R. Yu, (2011) "Cognitive Radio Mobile Ad Hoc Networks." New York, NY, USA: Springer-Verlag.

[2] J.Loo, J.Lloret, andJ.H.Ortiz, (2011) "Mobile Adhoc Networks: Current Status and Future Trends", BocRaton, FL, USA.

[3] Kannhavong B, Nakayama H, Nemoto Y, Kato N, Jamalipour A, (2007) "A Survey of Routing Attacks in Mobile Ad hoc Networks", IEEE Wireless Communications. October, 14(5):85-91. https://doi.org/10.1109/mwc.2007.4396947

[4] Burbank JL, Chimento PF, Haberman BK, Kasch WT, (2011) "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology**".** IEEE Communication Magazine 44(11):39–45. https://doi.org/10.1109/com-m.2006.248156.

[5] Behzad S, Jamali S. (2015) "A Survey over Black Hole Attack Detection in Mobile Ad hoc Network. "International Journal of Computer Science and Network Security (IJCSNS). 15(3)

[6] Pirzada.A.A, McDonald.C, (2006) "Trust Establishment in Pure Adhoc Networks", Wireless Personal Communications, 37(1), pp 39-168.

[7] Miu.L, Mohtashemi.M, Halberstadt.A, (2002) "A Computational Model of Trust and Reputation" Proc.35th Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/hicss.2002.994181

[8] Antesar M. Shabut, Keshav P. Dahal, Senior Member, IEEE, Sanat Kumar Bista, and Irfan U.Awan, (2015), "Recommendation Based Trust Model with an Effective Defence Scheme for Manets", IEEE Transaction on Mobile Computing, 4(10), 2101-2115. https://doi.org/10.1109/tmc.2014.2374154

[9] Abderrahmane and Ali, (2014) "Struggling against Simple and Cooperative Blackhole Attacks in Multihop Wireless Adhoc Networks" in Elsevier, Computer Networks.

[10] Kumari V, Paramasivan.B, (2016) "Defense against Sybil Attacks and Authentication for Anonymous Location Based Routing in MANET", Wireless Network Journal, Springer. https://doi.org/10.1007/s11276-015-1178-7

[11] Tao Shu, Marwan Krunz, (2015) "Privacy preserving and Truthful Detection of Packet Dropping Attacks in Wireless Adhoc Networks", IEEE Transactions on Mobile Computing, 14(4), pp 813-828, https://doi.org/10.1109/tmc.2014.2330818.

[12] Baadache A Belmehdi. A (2014), "Struggling Against Simple and Cooperative Blackhole Attacks in Multi-hop Wireless Adhoc Networks", Computer Networks, 73, 173-184. https://doi.org/10.1016/j.comnet.2014.07.016

[13] Muhammad Saleem Khan, Daniele Midi, Majid Iqbal Khan and Elsa Bertino (2017), "Fine- Grained Analysis of Packet Loss in Manets", IEEE Access, Multidisciplinary, (5), 7798-7807. https://doi.org/10.1109/access.2017.2694467

[14] Mohana Priya M & Krishnamurthi. I, (2014), "Modified DSR Protocol for Detection and Removal of Selective Black hole Attack in MANET", Computers and Electrical Engineering Journal, Elsevier, 530-538. https://doi.org/10.1016/j.compeleceng.2013.06.001

[15] Thi Ngoc Diep Pham and Chai Kiat Yeo, (2016) "Detecting Colluding Blackhole and Grey hole Attacks in Delay Tolerant Networks", IEEE Transaction on Mobile Computing, 15(5) 1116-1129. https://doi.org/10.1109/ccnc.2015.7157982

[16] Rajesh Babu. M, Usha. G, (2016) "A Novel Honey Pot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black hole Attacks in MANETs", An International Journal of Wireless Personal Communications, 90, .831-845. https://doi.org/10.1007/s11277-016-3229-5

[17] C.Siva RamMurthy, B.S.Manoj, "Adhoc Wireless Networks: Architectures and Protocols", Prentice Hall Communication Engineering and Emerging Technology Series, Theodore S.Rappaport Series Editor, ISBN 0-13-147023-X, 2004, Pearson Education.

[18] Joshi, (2016) "A review paper on black hole attack in MANET," International Journal of Advance Research in Computer Science and Management Studies, 4(5)16–21.

[19] P. F. Xu, Z. G. Chen, and X. H. Deng, (2006)," Research on Neighbouring Graphs Based Topology Control in Wireless Sensor Networks. Beijing, China: Publishing House Electronics Industry, 13.

[20] Danyang Qin, Songxiang Yang, Shuang Jia, Yan Zhang, Jing Yama and Qun Ding, (2016), "Research On Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network", May 2016, https://doi.org/10.1109/access.2017.2706973.

[21] Khaja Anwar Ali, Yousof Khan Afroz, (2012) "Minimum Delay Routing Protocol with Enhanced Multimedia transmission over Heterogeneous MANETs", Trends in Innovative computing - Intelligent system Design

[22] Saad M.Adam, Rosilah Hassan, (2013) "Delay Aware Routing Protocol for QOS in MANETs: a Review", Journal of Applied Research and Technology, 11(6), 844-850. https://doi.org/10.1016/s1665-6423(13)71590-6

[23] E. M. Daly and M. Haahr, (2009), "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," IEEE Trans. Mobile Computing, 8(5), 606–621. https://doi.org/10.1109/tmc.2008.161

[24] S. Buchegger and J. Y. Le Boudec, (2004) "A Robust Reputation System for P2P and Mobile Adhoc Networks," in Proc. 2nd Workshop Econ. P2PSyst. http://www.eecs.harvard.edu/p2pecon/program.html.

[25] C.Panos, C.Ntantogian Stefano, and Christos Xenakis, (2017)"Analysing, Quantifying and Detecting the black hole attack in infrastructure Less Networks", Elsevier, Computer Networks, 94-110. https://doi.org/10.1016/j.comnet.2016.12.006

[26] Weizhi, WenJuan, Lam, (2017), "Towards Effective Trust- Based Packet Filtering in Collaborative Network Environments", in Proc. IEEE Transactions on Network and Service Management, 14(1) 233-245. https://doi.org/10.1109/tnsm.2017.2664893

[27] Adwan Yasin, Mahmoud Abu Zant,(2018) "Detecting and Isolating Blackhole Attacks in Manets using Timer Based Baited Technique", *Wireless Communication and Mobile Computing*, https://doi.org/10.1155/2018/9812135.

[28] Arora S.K, Vijan.S and Gaba G.S, (2016) "Detection and Analysis of Blackhole attack using IDS" *Indian Journal of Science and Technology*, Vol 9, No 20, pp 1-5.

[29] Shashi Gurung, Siddhartha Chauhan, (2019) "A survey of Blackhole attack Mitigation techniques in MANET: Merits, Drawbacks and Suitability", *Wireless Networks, springer lin*k, pp 1-19. https://doi.org/10.1007/s11276-019-01966-z

[30] M.Thebiga, R.Suji Pramila (2020),"A survey on assorted subsisting approaches to recognize and preclude Blackhole attacks in Mobile adhoc networks "International Journal of Interactive Mobile Technologies (iJIM), volume 14, No 01, pp 96-108. https://doi.org/10.3991/ijim.v14i01.11329

[31] Chae, Y., DiPippo, L. C., & Sun, Y. L, "Trust management for defending on-off attacks", IEEE Transactions on Parallel and Distributed Systems, 26(4), 2015, pp 1178–1191. https://doi.org/10.1109/tpds.2014.2317719

[32] Christoforos Panos, Christoforos Ntantogian, Stefano's Malliaros, Christos Xenakis, "Analysing, quantifying, and detecting the Blackhole attack in infrastructure-less networks", Computer networks, Elsevier, 113(2017), pp 94-110. https://doi.org/10.1016/j.comnet.2016.12.006

[33] Delkesh, T., & Jamali, M. A. J. "EAODV: Detection and Removal of Multiple Blackhole Attacks through sending forged packets in MANETs". Journal of Ambient Intelligence and Humanized Computing. 10, pp 1897-1914,2018, https://doi.org/10.1007/s12652-018-0782-7. https://doi.org/10.1007/s12652-018-0782-7

[34] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, and Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed systems, Vol 26, No 5,2015,pp 1228-1237. https://doi.org/10.1109/tpds.2014.2320505

[35] Muhammad Saleem Khan, Daniele Midi, Majid Iqbal Khan, Elisa Bertino, "Fine-Grained Analysis of Packet Loss in Manets", IEEE Access, Vol 5, pp 7798-7807,2017, https://doi.org/10.1109/access.2017.2694467

[36] Ndajah, P, Matine A. O, & Hounkonnou M. N. (2018). "Blackhole attack prevention in wireless peer to peer networks: A new strategy", International Journal of Wireless Information Networks, Springer, 2018, 26, pp 48-60. https://doi.org/10.1007/s10776-018-0418-z.

10 Authors

M. Thebiga has received her Master degree in Software Engineering from periyar Maniammai college of Technology for Women, Thanjavur, TamilNadu, and pursuing her Ph.D. in Computer Science and Engineering from Noorul Islam Centre for Higher Education, Kumaracoil, and Tamil Nadu. Her research interest includes Mobile Adhoc Networks, Wireless networks and Security, Quality of Service.

R. Suji Pramila is currently working as an Associate Professor in Noorul Islam Centre for Higher Education, Kumaracoil, and Tamil Nadu. She received her Ph.D. in Computer Science and Engineering from Noorul Islam Centre for Higher Education, Kumaracoil. Her research interests include Mobile communication and Sensor Networks. sujisymon@gmail.com

Article submitted 2020-06-19. Resubmitted 2020-09-10. Final acceptance 2020-09-11. Final version published as submitted by the authors