IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 11, 2020, accepted November 25, 2020, date of publication December 15, 2020,
date of current version December 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3045004

Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-Hoc Networks

OSAMAH IBRAHIM KHALAF[1], F. AJESH[2], ABDULSATTAR ABDULLAH HAMAD[3], GIA NHU NGUYEN[4,5], (Member, IEEE), AND DAC-NHUONG LE[5,6]

[1]Al-Nahrain Nonrenewable Energy Research Centre, Al-Nahrain University, Baghdad 70030, Iraq
[2]Musaliar College of Engineering and Technology, Malayalappuzha 689653, India
[3]Department of Mathematics, Tikrit University, Tikrit 14022, Iraq
[4]Graduate School, Duy Tan University, Da Nang 550000, Vietnam
[5]Faculty of Information Technology, Duy Tan University, Da Nang 550000, Vietnam
[6]Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam

Corresponding author: Dac-Nhuong Le (ledacnhuong@duytan.edu.vn)

ABSTRACT Security and correspondence happening between network central point will be an instance for principal issues in Mobile Ad-hoc Networks (MANETs). Due to some ideas created by the organization leading to avoid attacks but may end in failure due to inappropriate way and thus attacks need recognized and cleared. The Dual-Cooperative Bait Detection Scheme (D-CBDS) is one of the ways that is in the stake for the discovery of MANET-dark/dim opening assailants. The current CBDS calculation consolidates the intensity of proactive and responsive security advancements to characterize lure mode assailants as proactive and receptive engineering. In CBDS, an adjacent source node is randomly selected as a bait target for searching. By reverse tracking as a reactive method, the attackers are identified. However, in some time, the chosen bait destination node may be an intruder that is not handled in the current CBDS approach. This paper therefore reinforces the CBDS with the dual mode of selecting two nearby nodes as two bait destinations. Dual reverse tracking enables effective collaborative assailants in MANET. Finally, when we analyze D-CBDS with respect to Routing overhead, End-End delay and throughput it gives much productivity than other methods like DSR, CBDS.

INDEX TERMS Dynamic source routing (DSR), black/ gray hole attacks, mobile ad-hoc networks (MANET), malicious nodes.

I. INTRODUCTION

A. MANET OVERVIEW

The Mobile Ad-hoc Network (MANET) is a typical and distinct field of innovation for dynamic examination. A feature point transmission association MANET that works with all the hubs that are associated with and are connected either in remote way having control, similarity and routing association. Self-managed and self-configuring nodes with a dynamic network topology model. The packets are distributed in a complex network from one node to another, with nodes quickly entering or leaving. The nodes must believe the neighboring node because they play a role in routing the data [1]. The choice of an omni-directional node flow without a central base station enables the MANET to function without infrastructure. In addition to decentralizing the nodes, battery power and bandwidth minimization make routing more complex. The network is ideal for sensitive applications such as combat activities and emergency operations. The high effect of these applications ensures that routing, data traffic and network topology have tighter security measures.

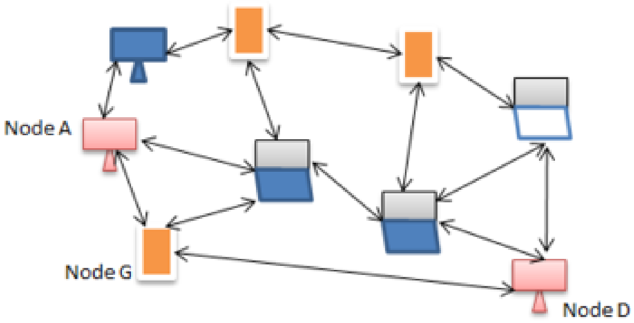

FIGURE 1. Wireless ad-hoc network.

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

The MANET hubs can advance the information parcels using the protocol. Major steering conventions are comprised of four sorts: proactive directing, responsive steering, crossover directing and progressive directing. Proactive steering courses the parcels over the organizations by giving directing tables intermittently and restoring the objective records. Instances of proactive directing are the Optimized Link State Routing Protocol (OLSR) and the Destination Distance Sequence Vector (DSDV). Responsive directing courses parcels. For this type of directing convention, dynamic source routing (DSR) and specially appointed on-request separation vectors (AODV) [2] are the models. The courses are proactively examined and bundle flooding is accomplished by receptive flooding. The ZRP (*Zone Routing Protocol*) is an illustration of this calculation. Various leveled steering can be chosen from useful to responsive directing. CBRP (*Cluster Based Routing Protocol*) and FSR (*Fisheye State Routing Protocol*) are instances of this calculation.

There are some nodes that may create some interruption while routing packets and they are malicious and that attacker node may be a black hole, a gray hole. A black hole typically indicates the shortest route to reach destination, but the path shown is not a true path. The black hole node does not send the packet. The grey hole is selfish and because of overload or congestion, it may lose packets. Collaborative black holes are cooperating and hiding from the process of detection [3]. Nodes that are not in the network or internal nodes that belong to the network may challenge routing protocols. To tackle this issue, several research projects have been conducted. Several techniques have been used and those fail to detect the presence of malicious node. In order to detect more nodes, the work should be further enhanced, which will result in a collective attack that is more distressing for the MANET [4].

B. CHALLENGES

The self-managed existence of MANET insists on creating a host node and finding the way its packet wants to be passed on. This leads to enormous attacks due to the wavering topology, lack of infrastructure and lack of trustworthiness between the nodes. Attacks that may happen can be said as 2 ways, on the basis of behavior it can be of active or passive and for the case of source of attack it can be of internal. External attackers are nodes outside the network that may involve a denial-of-service attack. Firewalls are best for solving external problems. Internal attackers are more powerful than external attackers because they are part of normal packet transmission and it will be difficult to identify those nodes. The active attacker usually has easy access to the network and may take hold of any internal node and involve the rejection of false packets and the denial-of-service attack. The passive attacker will be a silent listener until he captures the necessary information and slowly starts the attack on the network [3].

II. RELATED WORKS ON ATTACKS

An ongoing MANET creation challenge is the Black Hole Attack. A dark opening hub is a childish hub that professes to have the ideal course to the hub that it needs to assault. At the point when the solicitation is gotten, it sends some unacceptable data with the most limited course. After getting to the connection, the bundles can do everything, including dropping it [2]. The assault on the dark opening might be interior or outside. After Hongmei Deng's 'next jump information work, the dark opening assault turned into a functioning examination field.

L. Tamilselvan *et al.* [5] proposed work dependent on the table of unwavering, which measures for each taking an interest hub, the proportion of hub dependability. Hiremani *et al.'s* work depended on information steering data (DRI) table [6], where a DRI table was kept up on every hub to examine past directing data. Further correspondence will be founded on the table of the DRI. Numerous scientists have utilized progressed DRI tables. Another work assigns discretionary qualities for various boundaries in every hub. Measures, for example, rank, solidness factor and trust assessment of every hub are determined based on these qualities. Wahane *et al.* proposed a plan for a dark opening assault dependent on a trust-based recognition framework. AACK plot which is like two-ACK joins a similar plan with the finish of the ACK conspire [7].

William Kozma *et al.* proposed another technique called Resource Efficient Accountability (REAct) utilizes that as the setting off specialist to distinguish a vindictive hub and in this way diminishing the exhibition of organization [8]. A further examination called Best Effort Fault Tolerant Routing (BFTR) was proposed by Y. Xue and K. Nahrstedt [9], which gives better effectiveness of bundle steering even within the sight of a pernicious hub. Inside another plan called the Cooperative Bait Detection Scheme (CBDS), proactive and receptive assurance frameworks are joined and collaboration with neighboring hubs is made. The guard dog procedure recommended by Marti *et al.* depends on two guard dog and way appraising plans [10]. The previous is utilized to help the productivity of the organization, while the last is utilized to recognize interruption [1]. The plan proposed by A. Agalya [11] consolidates a proactive and open obstruction engineering with a stochastic neighboring hub. Group head Gateway Switch Routing (CGSR) convention recognizes a threatening hub dependent on a missing proportion.

Navdeep Kaur *et al.* proposed a CBDS-based plan that mixes productive and delicate protection wonders [12], [13]. Manjeet Singh *et al.* suggested a refreshed type of CBDS conspire known as the ECBDS [14]. Muskan Sharma *et al.* [15] improved CBDS by focusing on parcel conveyance proportion, start to finish dormancy, and throughput. As a result, the proposed plan could limit the deficiency of bundles that might be brought about by pernicious hubs and have a superior throughput [16]–[38].

III. CHARACTERISTICS OF ATTACKS IN MANET

Regardless of the customary geography move, MANET can deal with any hub mistakes. MANET has no concentrated organization or framework set up. Connections may

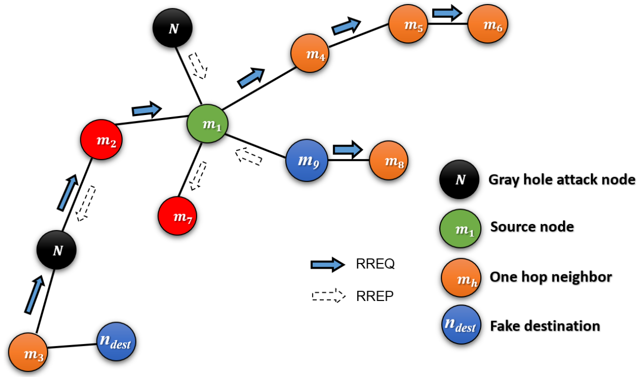

FIGURE 2. Collaborative black hole and gray hole attack in MANET.

inaccessible because of some harm and can be reestablished with new way when solicitations come. Course revelation is finished by source node (SN). The course demand (RREQ) is submitted to its neighbors for course recognizable proof [17]. When a middle hub (IN) gets this RREQ, it examines the way to the objective in its steering table. In the event that accessible, a course reaction (RREP) will be shipped off the source hub. In the event that the directing table doesn't contain the data, the RREQ is sent to its neighbors. In the event that the connection fizzles, the message of Route Error (RERR) is sent.

When a dark opening hub gets RREQ, it sends the malevolent RREP right away. The vindictive RREP would have the more modest bounce check and by and large objective grouping number (DSN), accordingly guaranteeing the briefest objective course. In many occurrences, noxious hubs will be the first to react in light of the fact that they won't test their steering table. Subsequent to accepting the RREP, the parcels will be steered to the guaranteed course. The malignant hub will drop bundles when it gets [15].

In Figure 2, m_1 is the source hub and n_{dest} is the destination hub. At the point when the m_1 attempts to advance the data to n_{dest}, three sorts of assaults may happen.

a) In the event that goes about as the dim opening hub aggressor, it might drop the parcel in startling time by going about as a typical hub till at that point.
b) On the off chance that N goes about as the dark opening hub assailant, drop the parcel.
c) On the off chance that two N_{bs} (different dark openings) are accessible, they may begin the community assault and drop the parcel.

IV. SCOPE

In this work, the Dual-Cooperative Bait Detection Scheme (D-CBDS) is suggested in which grey hole or blackhole attack can be found in the versatile Ad-hoc network, mainly configured to meet these aims. The new Cooperative Bait Detection Scheme draws inspiration from this work (CBDS). To send the RREP response post, CBDS chooses a neighboring hub. If RREP messages are received from certain separate hubs, the system affirms the existence of a malevolent hub and begins the opposite method of distinguishing the pernicious hub and preventing it from steering further. When the selected contiguous hub itself goes around as the malevolent hub, the CBDS system bombs. To answer this issue, D-CBDS is proposed. Here, two one-bounce neighbors, which are the other way, rather than one, are chosen by the source center. Based on clear source steering, D-CBDS is scheduled and further consolidates the advantages of proactive identification and responsive reaction.

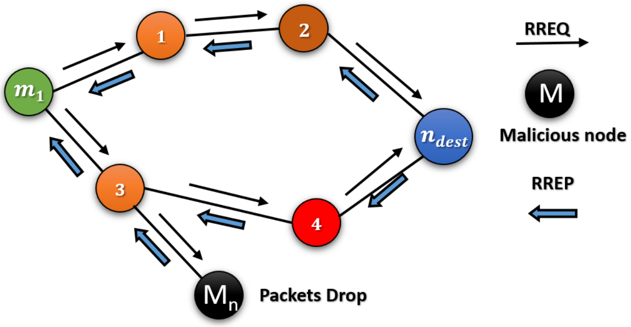

FIGURE 3. Blackhole/gray hole attack in DSR.

V. BLACK HOLE AND GRAY HOLE ATTACK IN DSR

DSR (Dynamic Source Routing) convention brings out 2 cycle for MANET's, for example, course revelation and course upkeep. Course disclosure diagrams a course revelation measure when information needs to send from source to objective hub, where source hub broadcast the RREQ parcel. On the off chance that halfway hub having any directing data, it will answer to the source code a RREQ parcel. So, while RREQ is given to neighbor node then that particular node add address to that packet and thereby identifies nodes along the selected route. For route maintenance, if a failure in connection occurs, the source node is informed by an error packet and thereby different route is served [1], [11], [12]. When coms to attacks on this scheme, it builds some fake RREQ packets and those packets are sent before initiating the actual routing process [14]. This is done for detecting the malicious nodes and avoid in advance. An acknowledgment mechanism is done in such a way that, when an acknowledgment is received as a reply to source node, then only data packets are routed Figure 3.

VI. COOPERATIVE BAIT DETECTION SCHEME (CBDS)

Recognizable evidence of malicious hub is significant to recuperate the organization from any attack. Cooperative Bait Detection Scheme (CBDS) [11], a DSR-based methodology proposed to identify the dark opening assault. This methodology shows valuable distinguishing proof and receptive reaction as the subsequent advance. It is finished by picking the neighboring hub to work together to distinguish the malevolent hub. When the neighboring hub address is sent as the target location for the trap, the malignant hub also sends the RREP response. To accept and group the malicious hub, the converse follow-up method is used. Subsequently, in stage CBDS, baiting, invert follow, and receptive assurance, there are three steps. The CBDS concept is seen in the following Figure 4.

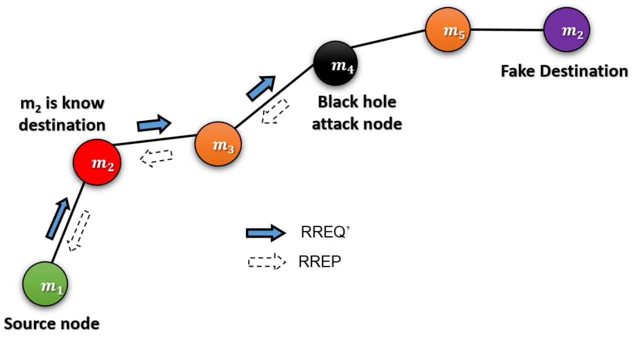

FIGURE 4. Cooperative bait detection scheme (CBDS).

A. BAITING

A neighboring hub that draws near its one-bounce separation is chosen by the source hub and sends RREQ by considering it as the snare objective hub address. In the event that the RREP messages come from non-hubs, we should expect the malignant hubs to be available in the directory response. On the off chance that by itself sends the answer RREP, at that point it shows the nonappearance of any malicious hub in the organization and the course disclosure stage can be started. In the event that doesn't give the answer, we can affirm it as the vindictive hub. Despite the fact that is one among the malicious hub and on the off chance that we get the RREP for RREQ′ of, at that point the converse following advance will be started.

B. REVERSE TRACING STEP

This stage, utilizing the RREP message to investigations the conduct of the vindictive hub, distinguishes the conduct of the noxious hub. The hubs that send the RREP messages are executed. The CBDS was began so that beyond what one malignant hub could be found simultaneously.

The m_r sends the fake RREP with address list L which can be denoted as $\{m_1, \ldots m_k, \ldots m_m, \ldots, m_r\}$. When m_k receives the RREP, the L list is separated by the objective address and it is denoted as $P_k = \{m_1, \ldots, m_k\}$. Where

$$L = \{m_1, \ldots m_k, \ldots m_m, \ldots, m_r\} \quad (1)$$

Thus, we can assemble the data about the objective location from as which is given as

$$P'_k = L - P_k = m_{k+1}P'_k = \{m_{k+1}, \ldots m_m, \ldots, m_r\} \quad (2)$$

S (source address in the RREP), H (next hop address of n_k) and H_1 (one any expectation of n_k) where compared. If H and H_1 are not same as S, then P'_k a forward reversal is carried out. Else, m_k is going to forward back then P'_k. By characterizing F, the questionable way data can be distinguished by

$$F = P'_1 \cap P'_2 \cap \ldots \cap P'_k \quad (3)$$

The set which is been presented can be identified by

$$O = L - F \quad (4)$$

The test packets are sent in this direction to classify the existence of the malicious node in S, and the rechecking of the second node to the last node in set O was performed and thus calculated as the black hole list.

C. REACTIVE DEFENSE PHASE

After the two steps described above the finding of the DSR route takes place. After setting the course, the detection scheme will start again if the destination finds a decrease in the delivery ratio. CBDS, fixed portability with moving vindictive hubs and fixed malignant hubs with fluctuating mobility were tested in two cases. Performance analysis indicates favored execution over DSR, 2ACK, and BFTR. As the malignant hub operates with the interference of false RREP, it can also be identified by CBDS. In spite of the fact that the one-bounce neighboring hub picked as the objective location for the RREQ for trapping the malicious node which is remembered by CBDS as malicious hub when RREP has not been intentionally sent. Be that as it may, if this hub sends the RREP, the CBDS considers to be as protected and starts the operation of DSR route revelation. In the end the program comes up short. For this issue, this article proposes another framework called D-CBDS (Dual-Cooperative Bait Detection System).

VII. FRAMEWORK PROPOSED

A. DUAL-COOPERATIVE BAIT DETECTION SCHEME (D-CBDS)

This paper proposes a malicious detection plot, the Dual Cooperative Bait Detection Scheme (D-CBDS), which in the portable Ad-hoc network will recognize dim opening or dark opening attack. To send an RREP response request, the Helpful Bait Detection Scheme (CBDS) selects an adjoining hub. The device will confirm the existence of a malicious node if RREP messages are received from any other nodes and will start a reverse tracing technique to locate a malicious node and prevent further routing. When the selected neighboring node itself behaves as a malicious node, the CBDS device fails. To answer this issue, D-CBDS is proposed. Here rather moving with one hop neighbors, it moves with 2 one hope neighbor. The CBDS definition is inherited by D-CBDS, but it adds two opposite one-hop neighborhood nodes. Even if each of them is a malicious node and sends an RREP message, this will help to identify each other by the interface.

The representation of the D-CBDS nodes is seen in Figure 5. Although knowing the complete position of the hub on the chosen course is conceivable, it is ridiculous to expect to discern data on the middle hub holding the steering data. Absence of data makes the hub malicious.

To resolve this, the HELLO message is also added to the D-CBDS. Table 1 gives the format of the packet. The D-CBDS technique will be sent to two baiting RREQ's. Figure m_{r1} and m_{r2} are the one hope neighborhood nodes that m_1 classify the RREQ for sending. When the machine has an awareness of existence of a malevolent node m_1 send two RREQ requests with the address of the destination m_{r1} and m_{r2}.

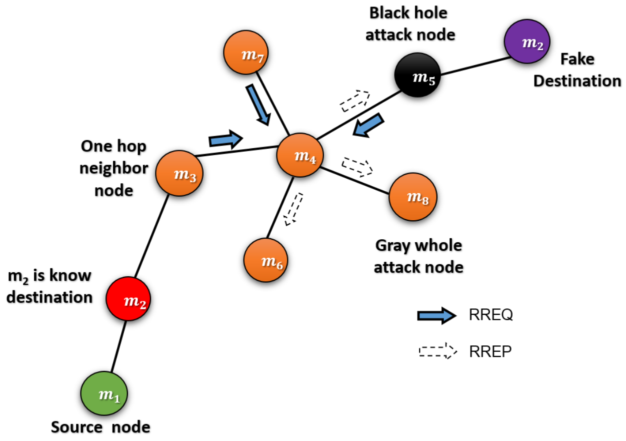

FIGURE 5. Dual-Cooperative bait detection scheme (D-CBDS) model.

TABLE 1. Packet format of RREQ'.

Option Type	Option Data Length	Request ID
Target Address (RREQ': Bait Address)		
Address [1]		
Address [2]		
...		
Address [n]		

The D-CBDS scheme encompasses 3 steps:

1) Dual-Baiting Process
2) Two-order Reverse Tracing
3) Reactive Defense Step.

B. DUAL-BAITING PROCESS

This stage is utilized to entice the RREP to present the vindictive hub or hubs. It is conceivable to recognize the fault through baiting, despite the fact that the anointed one hop neighborhood hub capabilities are the malicious hub and sends RREP. At the point when the lure RREQ is sent, the bedeviling stage will be set off. The development of hubs can affect the goading cycle in light of the fact that the bedeviling is performed arbitrarily.

The source hub at first chooses two one-bounce neighborhood hubs as the objective hubs the other way, at that point the source hub sends two trap RREQ demands by keeping up objective locations as m_{r1} and m_{r2} the answer message should be sent by the objective hubs. Here, RR_1 is the bait RREQ′ response by keeping the destination address as m_{r1} and is the bait RREQ′ response by holding the destination address as m_{r2}. The conditions listed below can occur.

a) The source node can receive from RR_1 and RR_2 itself and from m_{r2} itself.
b) The node of the source can receive from RR_1 and m_{r1} alone and from RR_2 and m_{r2} with m_{r1}.
c) The node of the source can receive from RR_2 and RR_1 alone and from RR_1 and m_{r1} with m_{r2}.
d) The source hub can get and get from a few hubs RR_1 and RR_2, including, or barring, m_{r1} and m_{r2}.

In the event that the source hub is received, at that point the nonappearance of a pernicious hub in the organization can be checked. On the off chance that condition (b) occurs, at that point we can watch that the pernicious hub is m_{r1}. On the off chance that condition (c) occurs, at that point we can watch that the vindictive hub is m_{r2}. In the event that condition (d) happens, the following condition will perform. The DSR should just be begun in the wake of confirming that there are no malicious hubs, as m_{r1} and m_{r2}.

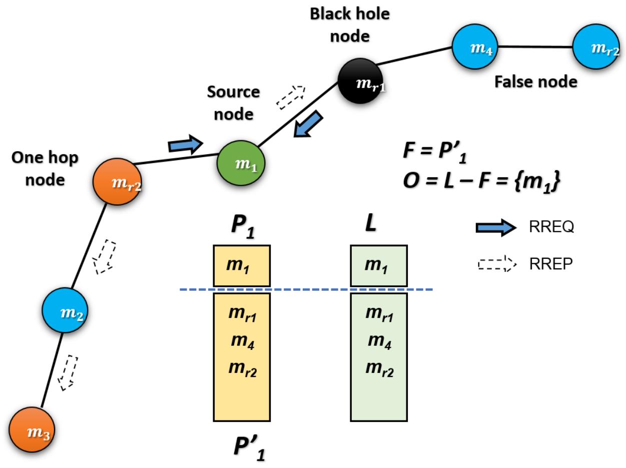

FIGURE 6. Source node identifies the black hole process.

C. TWO-ORDER REVERSE TRACING

When step 2, 3 aims to identify malicious nodes by using RREP to the bait RREQ. When malicious nodes receive RREP, it responds to a false RREQ response. The reverse tracing step is performed to identify the exact malevolent node. Two sets of RREPs are generated from the previous stage RR_1 and RR_2. RR_1 is the RREP created with objective location by the bedeviling RREQ m_{r1} and RR_2 is from the RREP delivered with objective location by the teasing RREQ′ m_{r1}. With the help of using these two arrangements of RREP's we can perform dual-request transition. Double CBDS can recognize numerous vindictive hubs all the while.

Let the address list $L = \{m_1, \ldots, m_k, \ldots, m_m, \ldots, m_{r1}\}$. In node m_k ack the RREP which comes from m_{r1}, m_k will segregate the address list $P_k = \{m_1, \ldots, m_k\}$ by separating the route information from source node m_1 to objective node m_k. And furthermore m_k will discover the data about the course after $m_k P'_k$, which will be put away in the saved field of the RREP. It tends to be characterized as in equation.

$$P'_k = L - P_k \tag{5}$$

$$P'_k = m_{k+1} P'_k = \{m_{k+1}, \ldots, m_m, \ldots, m_{r1}\} \tag{6}$$

When m_k receives the P'_k, it will compare three information.

1) U. The Source Node Address
2) V. Address of the local hub of the following jump in L
3) W. Address of the following hub of the local bounce m_k

When U, V and W are not same, then P'_k back will be subject to forward. Else, m_k going to suspect the L was made by itself. The two-reverse order tracing is shown in Figure 6.

TABLE 2. NS-2 simulation parameters.

Parameters	Values
Network Area	$800m \times 800m$
Node Density	150
MAC Protocol	IEEE 802_11
Beacon Interval	500 Sec
Packet Size	512 bytes
Simulation Time	1200 Sec
Average Vehicle Speed	20 m/s
Data Traffic	15 CBR
Range of Radio	250m
Malicious nodes	0% to 50%

D. REACTIVE DEFENSE STEP

This has been put into effect following the completion of the above procedure. In the case of CBDS, the 2-case appraisal of fixed versatility with various malignant hubs and fixed noxious hubs with various portability brings preferred outcomes over different methodologies. Since the malevolent hub meddles with bogus RREP, it can likewise be distinguished by CBDS, and it is additionally a one-jump neighboring hub that solitary exists on one side, and the issue it faces is that it is unidentifiable when the neighboring hub itself acts as a noxious hub. But the proposed system DCBDS covers that area of issue as it's a dual hope dynamic routing process.

VIII. PERFORMANCE ANALYSIS

A. SIMULATION STEP

Network Simulation (NS) is one of the kinds of reproduction, which is utilized to reproduce the organizations, for example, in MANETs, VANETs and so on, in which it gives reproduction to routing and multicast protocol for both wired and remote networks. NS is authorized for use under adaptation 2 of the GNU (General Public License) and is prominently known as NS-2.The presentation of the D-CBDS model will be assessed utilizing the NS-2 test system. Absolutely 150 hubs are haphazardly conveyed in the $800m \times 800\ m$ reenactment zone. Aggressor hubs are chosen on an arbitrary premise. Subtleties of the recreation boundaries are appeared and for assessment of MANET the below parameters are used and their respective value for this test is shown in Table 2 beneath.

B. PERFORMANCE METRICS

The proficiency of the proposed D-CBDS was much greater than the cutting edge DSR and CBDS [13] plans. For example, execution metrics have been used for examining Message Delivery Ratio, Average End-to-End Message Latency, Routing Overhead and Throughput. Two simulations were performed in this process. According to the case one, malicious nodes varies as mobility is going constant, but for the case two malicious nodes percentage varies in range of 0-50% with fixed mobility.

The following Figure 7 indicate D-CBDS scheme efficiency based on message transmission ratio in two simulation modes. Figure 7 shows that, owing to its lower transmission efficiency, the DSR method suffered severely from the attack. The presence of 50 percent of malicious nodes is more than 95 percent of the distribution ratio relative to the current CBDS system in our proposed D-CBDS process. Node velocity usually reflects the propagation ratio.

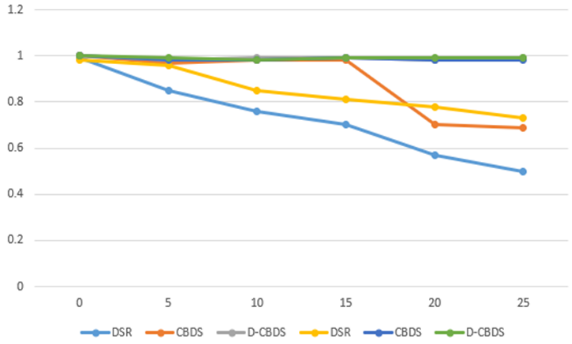

FIGURE 7. Packet delivery ratio versus malicious node and speed.

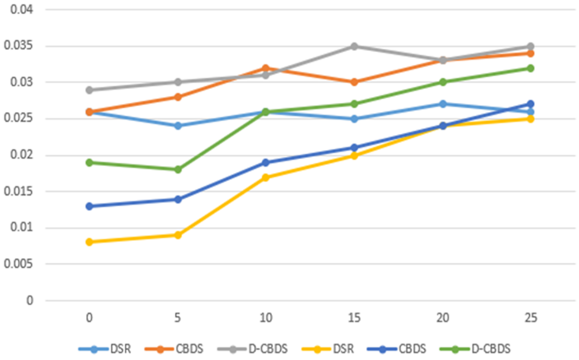

FIGURE 8. Routing overhead versus malicious node and speed.

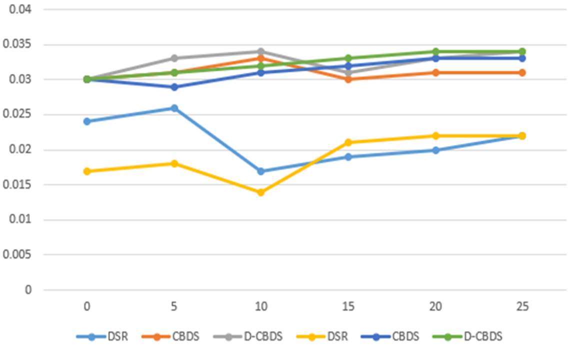

FIGURE 9. End-to-end delay versus malicious node and speed.

It is evident from the above Figure 8 that the overhead routing occurred in D-CBDS due to its two bait methods is marginally more than DSR and CBDS. The reasoning behind this fact is that the parcels are sent intermittently from source to target using reverse methods while applying the two methods of bait calculation. With the D-CBDS technique, the steering overhead is now slightly extended.

In Figure 9, the End-End delay study was led for three strategies. Which shows that because of a similar clarification for the double snare cycle and testing technique, the finish to - end delay in D-CBDS was hardly more than in DSR and CBDS. The D-CBDS strategy additionally accomplished extremely superior contrasted with DSR and CBDS approaches. D-CBDS gadget viably recognizes noxious hubs

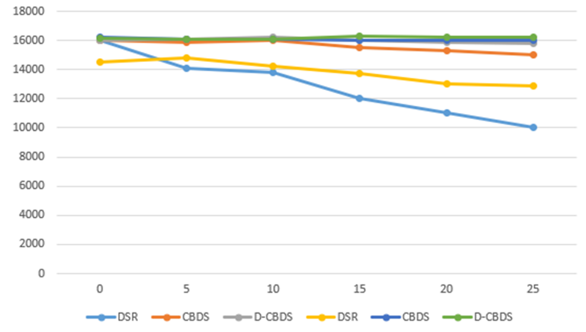

FIGURE 10. Throughput versus malicious node and speed.

as the organization has up to half hubs. The proposed plot got the throughput more than 16000 bit/s while half of malevolent hubs happened in the organization framework [35].

In Figure 10, gives the throughput diagram of the three frameworks in which as we see that the throughput of DSR diminishes as the versatility increments and this is caused because of absence of security issues. When seeing the other 2 techniques gives a lot of fluctuation to the DSR as both goes in expanded way alongside the addition of versatility in which to be more explicit there is a serious presentation on account of D-CBDS than customary CBDS and this happens due to dual bait process and checking process.

IX. CONCLUSION

This paper proposed an improved framework to recognize vindictive hubs in the case of MANET dark and grey hole attacks. The new CBDS conspire consolidates the productive and receptive plan security model. CBDS approach considers the lure target hub address of the haphazardly chosen neighboring hub. Out of all possible way, a chosen malicious hub can be dark/dim hole gatecrasher. Thus, the proposed D-CBDS approach chooses two contiguous hubs as two snare objective hubs to viably distinguish malevolent hubs despite the fact that the chose nearby is one of the pernicious hubs in both converses preparing mode. The proficiency of the proposed double CBDS plot is stood out from cutting edge DSR and CBDS frameworks with worthy reproduction situations. From the exploratory discoveries, it is plainly seen that the proposed plot (D-CBDS) accomplishes better dissemination proportion and throughput execution with generous overhead. The proposed arrangement holds network solidness with up to half of pernicious hubs in the organization.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their valuable comments and suggestions that have improved the quality of the paper in even more better way.

CONFLICT OF INTERESTS

The authors declare no conflict of interest

REFERENCES

[1] J.-M. Chang, P.-C. Tsou, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, Feb. 2011, pp. 1–5.

[2] P. Goyal, V. Parmar, and R. Rishi, "Manet: Vulnerabilities, challenges, attacks, application," *Int. J. Comput. Eng. Manag.*, vol. 11, pp. 32–37, Jan. 2011.

[3] S. K. Prasad, J. Rachna, O. I. Khalaf, and D.-N. Le, "Map matching algorithm: Real time location tracking for smart security application," *Telecommun. Radio Eng.*, vol. 79, no. 13, pp. 1189–1203, 2020.

[4] J. Sen, S. Koilakonda, and A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in *Proc. 2nd Int. Conf. Intell. Syst., Modelling Simulation*, Jan. 2011, pp. 338–343.

[5] O. I. Khalaf and G. M. Abdulsahib, "Energy efficient routing and reliable data transmission protocol in WSN," *Int. J. Adv. Soft Comput. Appl.*, vol. 13, no. 3, pp. 45–53, 2020.

[6] V. A. Hiremani and M. M. Jadhao, "Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET," in *Proc. Int. Conf. Green Comput., Commun. Conservation Energy (ICGCE)*, Dec. 2013, pp. 944–948.

[7] G. Wahane and S. Lonare, "Technique for detection of cooperative black hole attack in MANET," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–8.

[8] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *Proc. Appl. Innov. Mobile Comput. (AIMoC)*, Feb. 2014, pp. 157–164.

[9] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 1, pp. 10–16, 2010.

[10] G. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in *Proc. Int. Conf. Syst. Eng. Technol. (ICSET)*, Sep. 2012, pp. 1–5.

[11] A. Agalya, C. Nandini, and S. Sridevi, "Detecting and preventing black hole attacks in manets using CBDS (cooperative bait detection scheme)," *Int. J. Mod. Trends Eng. Res.*, vol. 2, no. 4, pp. 148–152, 2015.

[12] R. Kaur and J. Singh, "Towards security against malicious node attack in mobile ad hoc network," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 7, pp. 273–381, 2013.

[13] N. Kaur, "Implementing MANET security using CBDS for combating sleep deprivation & DOS attack," *Int. J. Sci. Emerg.*, vol. 16, no. 1, pp. 6–12, 2017.

[14] M. Singh and A. Sharma "Security in MANET using ECBDS on resource consumption attack Byzantine attack," *Int. J. Inf. Technol. Knowl. Manage.*, vol. 8, no. 2, pp. 4–7, 2015.

[15] A. Puran and Ş. T. Imeci, "Design and analysis of compact dual resonance patch antenna," *Heritage Sustain. Develop.*, vol. 2, no. 1, pp. 38–45, Jun. 2020.

[16] M. L. Thivagar, M. A. Ahmed, V. Ramesh, and A. A. Hamad, "Impact of non-linear electronic circuits and switch of chaotic dynamics," *Periodicals Eng. Natural Sci.*, vol. 7, no. 4, pp. 2070–2091, 2020.

[17] N. Kang, E. M. Shakshuki, and T. R. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2011, pp. 488–494.

[18] L. M. Thivagar, A. A. Hamad, and S. G. Ahmed, "Conforming dynamics in the metric spaces," *J. Inf. Sci. Eng.*, vol. 36, no. 2, pp. 279–291, 2020.

[19] B. Durakovic, "Design of experiments application, concepts, examples: State of the art," *Periodicals Eng. Natural Sci.*, vol. 5, no. 3, pp. 421–439, Dec. 2017.

[20] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals Eng. Natural Sci.*, vol. 7, no. 3, pp. 1096–1101, 2019.

[21] O. I. Khalaf and G. M. Abdulsahib, "Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network," *J. Inf. Sci. Eng.*, vol. 35, no. 5, pp. 1099–1112, 2019.

[22] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *Int. J. e-Collaboration*, vol. 16, no. 1, pp. 16–32, Jan. 2020.

[23] O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar, "Optimization of wireless sensor network coverage using the bee algorithm," *J. Inf. Sci. Eng.*, vol. 36, no. 2, pp. 377–386, 2020.

[24] O. I. Khalaf, G. M. Abdulsahib, and M. Sadik, "A modified algorithm for improving lifetime WSN," *J. Eng. Appl. Sci.*, vol. 13, no. 21, pp. 9277–9282, 2018.

[25] G. Abdulsahib and O. Khalaf, "Comparison and evaluation of cloud processing models in cloud-based networks," *Int. J. Simul., Syst., Sci. Technol.*, vol. 19, no. 5, pp. 261–264, Jan. 2019.

[26] A. D. Salman, O. I. Khalaf, and G. M. Abdulsahib, "An adaptive intelligent alarm system for wireless sensor network," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 15, no. 1, pp. 142–147, 2019.

[27] K. A. Ogudo, D. M. J. Nestor, O. I. Khalaf, and H. D. Kasmaei, "A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks," *Symmetry*, vol. 11, no. 4, p. 593, Apr. 2019.

[28] J. Chen, G. Mao, C. Li, W. Liang, and D.-G. Zhang, "Capacity of cooperative vehicular networks with infrastructure support: Multiuser case," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1546–1560, Feb. 2018.

[29] D. Zhang, G. Li, K. Zheng, X. Ming, and Z.-H. Pan, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 766–773, Feb. 2014.

[30] D.-G. Zhang, S. Liu, T. Zhang, and Z. Liang, "Novel unequal clustering routing protocol considering energy balancing based on network partition & distance for mobile education," *J. Netw. Comput. Appl.*, vol. 88, pp. 1–9, Jun. 2017.

[31] D. Zhang, T. Zhang, and X. Liu, "Novel self-adaptive routing service algorithm for application in VANET," *Int. J. Speech Technol.*, vol. 49, no. 5, pp. 1866–1879, May 2019.

[32] D. Zhang, X. Wang, X. Song, and D. Zhao, "A novel approach to mapped correlation of ID for RFID anti-collision," *IEEE Trans. Services Comput.*, vol. 7, no. 4, pp. 741–748, Oct. 2014.

[33] D. N. Le, V. N. Van, and T. T. T. Giang, "A new private security policy approach for DDoS attack defense in NGNs," in *Information Systems Design and Intelligent Applications*. New Delhi, India: Springer, 2016, pp. 1–10.

[34] M. Paul, G. Sanyal, D. Samanta, G. N. Nguyen, and D.-N. Le, "Admission control algorithm based on the effective bandwidth in vehicle-to-infrastructure communication," *IET Commun.*, vol. 12, no. 6, pp. 704–711, Apr. 2018.

[35] A. Nayyar, V. Puri, and D.-N. Le, "Comprehensive analysis of routing protocols surrounding underwater sensor networks (UWSNs)," in *Data Management, Analytics and Innovation*. Singapore: Springer, 2019, pp. 435–450.

[36] J. Yang, M. Ding, G. Mao, Z. Lin, D. G. Zhang, and T. H. Luan, "Optimal base station antenna downtilt in downlink cellular networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1779–1791, Mar. 2019.

[37] T.-G. Zhang, T. Zhang, Y. Dong, X.-H. Liu, Y.-Y. Cui, and D.-X. Zhao, "Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning," *J. Netw. Comput. Appl.*, vol. 122, pp. 37–49, Nov. 2018.

[38] D. Zhang, H. Ge, T. Zhang, Y.-Y. Cui, X. Liu, and G. Mao, "New multi-hop clustering algorithm for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1517–1530, Apr. 2019.

OSAMAH IBRAHIM KHALAF received the B.Sc. degree in software engineering from Al-Rafidain University College, Iraq, in 2004, the M.Sc. degree in computer engineering from Belarussian National Technical University, in 2007, and the Ph.D. degree in computer networks from the Faculty of Computer Systems and Software Engineering, University Malaysia, Pahang, in 2017. He is currently a Senior Engineering and Telecommunications Lecturer with the College of Information Engineering, Al-Nahrain University. He has hold ten years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer science and information technology projects. He has had many published articles indexed in (ISI/Thomson Reuters) and has also participated and presented at numerous international conferences. He has a patent and has received several medals and awards due to his innovative work and research activities. He has good skills in software engineering including experience with.Net, SQL development, database management, mobile applications design, mobile techniques, java development, android development, and IOS mobile development, cloud system and computations, and website design. His brilliant personal strengths are in highly self-motivated team player who can work independently with minimum supervision, strong leadership skills, and outgoing personality. He has overseas work experiences in University in Binary University in Malaysia and University Malaysia Pahang.

F. AJESH received the bachelor's degree in computer science and Engineering from the Cochin University of Science and Technology (CUSAT), Kerala, India, and the master's degree in computer science and engineering from Anna University Chennai, Tamil Nadu, India. He is currently a Professor with the Department of Computer Science and Engineering, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India. His research interests include computer networks, medical image processing, machine learning, and artificial intelligence. He published various international journals and attended many national and international conferences.

ABDULSATTAR ABDULLAH HAMAD was born in Slah Al Deen, Iraq, in October 1987. He received the B.Math. degree in Iraq, in 2014, and the master's degree in India, in April 2018. He is currently pursuing the Ph.D. degree with the School of Mathematics, Madurai Kamaraj University.

GIA NHU NGUYEN (Member, IEEE) received the Ph.D. degree in mathematical for computer science from the Ha Noi University of Science-VNU, Vietnam. He is currently the Dean of the Graduate School, Duy Tan University, Vietnam. He has a total academic teaching experience of 19 years with more than 60 publications in reputed international conferences, journals and online book chapter contributions (Indexed By: SCIE, SSCI, Scopus, ACM, and DBLP). His areas of research include healthcare informatics, network performance analysis and simulation, and computational intelligence. Recently, he has been the technical program committee, review committee, track chair for several international conferences under Springer-ASIC/LNAI Series. Six computer science books published in Springer, IGI Global, CRC, and Wiley Publication. He is currently an Associate Editor of the *IGI-Global: International Journal of Synthetic Emotions (IJSE)*.

DAC-NHUONG LE received the M.Sc. and Ph.D. degrees in computer science from Vietnam National University, Vietnam, in 2009 and 2015, respectively. He is currently an Associate Professor, and an Associate Dean of the Faculty of Information Technology, Haiphong University, Vietnam. He has been involved with academics including teaching and research, since 2005. He has more than 50 publications in the reputed international conferences, journals, and online book chapter contributions (Indexed by: SCI, SCIE, SSCI, Scopus, ACM, and DBLP). He is doing research in the field of evolutionary computation, specialized with evolutionary multi-objective optimization, network communication and security, cloud computing, VR/AR. Recently, he has been the technique program committee, the technique reviews, the track chair for international conferences under Springer-ASIC/LNAI/CISC Series. He also have been served in the editorial board of international journals and he authored and edited more than 15 computer science books by Springer, Wiley, and CRC Press Publishing.

• • •