Novel Routing Protocol for Secure Data Transmission in Wireless Ad Hoc Networks

Arage Chetan S, Satyanarayana K V V

Abstract*: The crucial requirement in MANET is to establish the efficient path among destination and source nodes based on the cooperation among the mobiles nodes. The routing protocols trust the mobile nodes for data transmission. However, MANETs are vulnerable to various security threats. The attacks like grayhole, blackhole, Denial of Service (DoS) attacks etc. performed on MANET. The presence of such malicious nodes in network may lead to serious concerns related to network security. The most of existing security methods for MANET consider the packet delivery rate (PDR) parameter to detect malicious nodes. However, the node mobility, frequent link breaks, queue overflow etc. may be the other reasons for less PDR in MANET. For any security method, detecting the main cause of packet loss is vital. Therefore, along with cooperative security solution, methods required to correctly identify the reason of packet losses. In this paper, we proposed hybrid cooperative bait detection system (HCBDS) in which the reverse tracing and correct identification of packet losses algorithms proposed to correctly detect the malicious node in network. Using the network parameters the accurate reason of dropped PDR determined. The results presented in this paper show that our security model achieves significant improvement in performance under the presence of malicious nodes.

***Index Terms*: Cooperative bait detection, HCBDS, Mobile ad hoc networks, Packet losses analysis Packet loss parameters**

I. INTRODUCTION

The mobile specially appointed system implies MANET is the impermanent system in which the mobile nodes gathered autonomously on other nodes in a similar remote system. These nodes in such systems are moving subjectively everywhere throughout the total system. MANET systems [1] [2] are essentially assembling brief remote systems and they are not requiring any sort of foundation for conveying just as brought together organization. The communication among these nodes relies upon the sort of routing instrument utilized called multihop routing protocols.

Each mobile hub in the mobile system is working as the both sending hub implies routing tasks and host hub. Therefore as such we can say that, routing protocols for the mobile specially appointed system are presented for building the correspondence courses just as remote correspondence organize.

Working of dynamic correspondence a course in the whole system is done among the source hub to destination hub for correspondence reason on interest way and consequently this is the center usefulness of MANET routing protocols. The mobile impromptu systems are not having the settled system topology because of the reason that mobile nodes are much of the time changing their positions and development. System topology for the MANET systems isn't settled in view of the incessant nodes development in the system. Mobile specially appointed systems having diverse sorts of routing protocols like responsive, half and half, and proactive protocols kind of routing protocols. We can utilize these protocols with various system situations and versatility designs. The responsive protocols, for example, DSR (Dynamic Source Routing) protocol and AODV (Ad hoc on interest Distance Vector Routing) protocol are much of the time utilized MANET protocols. Aside from this, DSDV (Destination Sequenced Destination Vectoring) just as OLSR (Optimized Link State Routing) are instances of responsive protocols. Zone Routing Protocol (ZRP) is one sort of half and half protocol for the mobile impromptu systems.

Because of the breaking down, malignant and egotistical nature of mobile nodes are come about into acting up nodes. Any sorts of programming or equipment disappointments are in charge of the breaking down nodes. The narrow minded nodes are just tolerating the contributions from other mobile nodes in the system however not sending it to other sending nodes and simply dropping those parcels. Vindictive nodes in the system bringing other mobile hub into a misguided course as opposed to the planned heading by publicizing data that he has most brief way for the expected beneficiary of data. This assault is called of DoS assault. All the got bundles are dropped by the noxious nodes. If there should arise an occurrence of dark gap hub assault, getting rowdy conduct of the nodes came about into the specifically droppings of bundles. Along these lines because of this sorts of assaults, MANET organize turns into the valunearable for the poor execution treats of utilized routing protocols. There are numerous arrangements are presented for tending to this remote systems assaults and still the inquires about are going on. Be that as it may, in the event that we include the routing instrument for this system, it came about into the execution debasements and lower throughput for those systems.

As the interchanges in MANET perform agreeably, cooperation is normal by all nodes so as to guarantee a legitimate usefulness of the MANET. Be that as it may, numerous intrinsic limitations, for example, continually changing topology and completely circulated design, make these systems powerless against different assaults by making trouble nodes. Instances of such assaults are: (an) a

Revised Manuscript Received on March 02, 2019.

Arage Chetan S, Departement of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur – 522502, Andhra Pradesh, India.

Satyanarayana K V V, Departement of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur – 522502, Andhra Pradesh, India

hub drops information packets because of malevolent conduct; (b) a hub gives misrepresented routing data to different nodes so as to upset the system, and (c) a hub does not take an interest in routing operations so as to spare its own vitality [1]. To distinguish and separate non-agreeable nodes in MANETs, a scope of trust-based security plans [3–8] have been proposed. In MANETs, trust can be characterized with respect to what degree a hub can satisfy the desires for another hub [9]. In trust-based plans, every hub inside the system deals with a free trust table to figure and store the trust estimations of different nodes. Routing choices are then founded on such processed trust esteems.

In [8], the CBDS approach detailed in which the dependability of hub assessed dependent on Packet Delivery Ratio (PDR) of halfway nodes of source and destination hub. In any case, there are conditions in which condition of-workmanship MANET security techniques neglect to address alternate reasons for a dropped PDR occasion. Also, henceforth this outcomes to expanded false positive rate by distinguishing the real nodes as malevolent and less exactness in recognizing the genuine pernicious nodes. The purpose behind such inadequacies is that those present security plans accept that dropped PDR or expanded packet misfortunes emerge as a result of malevolent exercises by getting out of hand nodes. There are a few different purposes behind the dropping PDR in MANET, for example, high portability, over the top load or blockage, high information rate and so on. Under the parameters, for example, high versatility and high information rate, the customary techniques may lead the bogus estimations of malevolent nodes [10– 13].

In this paper, we proposed cross breed answer for alleviate the difficulties of distinguishing the noxious nodes and checking the pernicious nodes identification procedure to convey the more hearty execution for MANET correspondences. The proposed methodology HCBDS is two phase security technique. In initial step, as indicated by CBDS [8], the procedure of malignant hub location is performed in which nearby hub address abused as snare destination deliver to lure malevolent nodes to send an answer RREP message. After the malevolent hub recognized, in second stage, we play out the fine grained examination on distinguished hub so as to check that whether hub is genuinely malignant dependent on packet misfortunes parameters. In second stage, if the causes of packet losses determined other than the computed packet losses parameters, then node is marked as malicious, otherwise marked as trusted node and the process of finding the more stable route initiated. In section II, the brief review of recent MANET security solutions presented. In section III, the proposed HCBDS method discussed. In section IV, performance evaluations and discussions presented. In section V, the results concluded.

II. RELATED WORK

Number of methods investigated to solve the problem of malicious node detection in MANETs since from last two decades. Most of those solutions agitate the detection of one malicious node or need huge resource in terms of your time and value for police work cooperative blackhole attacks. additionally, a number of these ways need specific environments [5] or assumptions so as to work.

The malicious node detection techniques mainly grouped into three categories such as proactive detection methods, reactive detection methods and hybrid detection methods. The proactive detection methods [14]-[20] required to frequently monitor the nearby mobile nodes to detection malicious nodes. Therefore notwithstanding malicious nodes existence, the overhead of detection is consistently created, and also the resource used for detection is consistently wasted. However, one among the benefits of those forms of schemes is that it will facilitate in preventing or avoiding associate attack in its initial stage. The reactive detection strategies [21]–[23] initiated the method of malicious nodes detection only if the numerous packet drop reportable at destination node. The hybrid findion strategies [1] [8] mix the each proactive and reactive strategies to detect the malicious nodes effectively. These strategies exploited the benefits of each proactive and reactive routing protocols.

In [17], Liu et al. proposed a 2ACK plan for the discovery of routing bad conduct in MANETs. In this plan, two-jump affirmation packets are sent the other way of the routing way to demonstrate that the information packets have been effectively gotten. A parameter affirmation ratio, i.e., Rack, is likewise used to control the ratio of the got information packets for which the affirmation is required. This plan has a place with the class of proactive plans and, thus, creates extra routing overhead paying little respect to the presence of noxious nodes. n [21], Xue Associate in Nursingd Nahrstedt planned an anticipation part known as best-effort fault-tolerant routing (BFTR). Their BFTR conspire utilizes begin to end affirmations to screen the character of the routing method (estimated relating to packet delivery quantitative relation and postponement) to be picked by the destination hub. On the off probability that the conduct of the method goes wide from a predefined conduct set for deciding "great" courses, the supply hub utilizes another course. one in all the disadvantages of BFTR is that malignant nodes might nowadays exist within the new picked course, and this set up is inclined to rehashed course revelation forms, which can prompt vast routing overhead.

The method reported in [8], shown that hybrid approach outperformed the proactive and reactive security methods; however they relied on only PDR parameter to mark node as malicious node and this may lead to degrade the performance of correctly detecting malicious node. In this method, if the PDR dropped below the threshold, then reverse tracing algorithm used to locate malicious node. However, in MANET, there are various reasons for packet losses hence the correctness of packet losses should be verified before detecting that node as malicious. Our proposed HCBDS methods perform the two-stage detection process to accurately marked node as malicious in MANET. We considered CBDS method [8] as benchmark technique for performance comparison purposes in this paper along with the DSR based security method.

There are numerous different strategies detailed for MANET security, for example, trust based techniques. To

gauge the packet misfortunes there a few procedures exhibited in later past. To assess the packet misfortune rate over connection, De Couto et al. [24] proposed a plan which utilizes expected transmission tally measurements. Such plan effectively processes the packet misfortune rate, yet it can't distinguish the real reason for packet misfortune. Shebaro et al. [25] proposed a fine-grained investigation plan to examine the packet misfortune reasons in remote sensor systems (WSNs). In such a methodology, the parameters utilized for connection profiling are the gotten flag quality marker (RSSI), the connection quality pointer (LQI), and the packet gathering rate (PRR). This methodology is exceptionally compelling for WSNs which have a generally static topology yet the profiling parameters utilized by this methodology can't be effectively connected to MANETs which are exceedingly dynamic conditions.

Parker et al. [26] recommended an interruption recognition conspire that requires the observing nodes to catch traffic in their transmission ranges. They contended that such traffic catching can prompt effective discovery of message dropping and alteration assaults. Be that as it may, assaults, for example, mis-routing assaults (for example the assailant advances packets to the wrong next jump) can't be recognized. A community oriented notoriety based arrangement, called CORE, was proposed by Michiardi et al. [27] to assess the notoriety of a hub. They proposed that community notoriety is the mix of emotional, circuitous, and practical notorieties. A notoriety table is kept up at every hub to record the notoriety of different nodes and to decide if a hub is noxious or not.

The methods discussed above failed to achieve the trade-off between the detection rate performance and QoS (Quality of Service) performance as most of the techniques based on dropped PDR or packet losses as key parameter to marked node as malicious. There is no single security method that conducts the two stage verification to correctly detect the malicious nodes by considering the other causes of packet losses. Hence this can lead to erroneous malicious detection performance under the high mobility and data rate network conditions. In this paper, we proposed the hybrid solution to solve the state-of-art methods problem in which two stage methods designed to prevent the erroneous trust estimation and improve the network performance under the presence of malicious nodes. The key contributions of this paper are:

Designed the novel two stage hybrid cooperative bait detection system for MANETs based on reverse tracking function as well as fine grained analysis.

In first step, we exploited the CBDS method effectively to improve the security performance for various network conditions. If the PDR performance dropped significantly and below the threshold, then the reversed tracing method used to detect the malicious node.

In stage 2, if any node detected malicious in step 1, then it cannot be immediately marked as malicious, it can further pass through the fine grained analysis to estimate the other reasons for packet losses and correctly verify the node marked in step 1 is malicious or not.

The performance evaluation presented in terms of detection accuracy and other routing QoS parameters.

III. RESEARCH METHOD

In this paper, we proposed the malicious node detection method called the hybrid cooperative bait detection system (HCBDS). This method designed to solve the problems of all previous detection methods which are mainly based on packet losses is only parameter for malicious node detection. The proposed HCBDS is two stage detection process in which not only the MANET security provided but also reduced the malicious node detection errors. Accurate detection of malicious nodes is ruled out by many security solutions. Figure 1 shows the functionality of HCBDS.

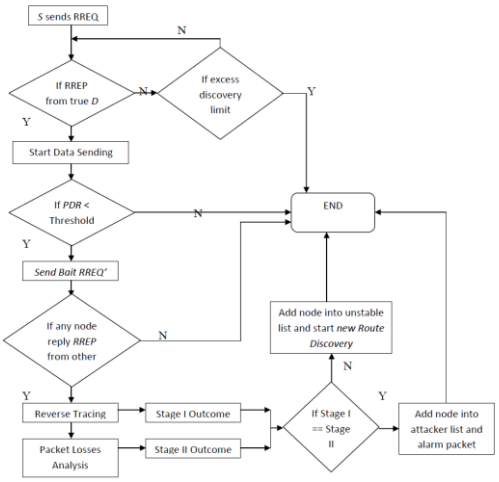

Figure 1: Proposed Method Functionality

As observed in figure 1, initially source node S start the route discovery by broadcasting the RREQ message to its neighbour nodes. The received RREP checked whether it's from true destination node D. Once the route discovered the data transmission process begins. At each interval, the PDR is measured and compared against the dynamic threshold value. If at any interval, PDR dropped below threshold, then source node sends the new RREQ type called Bait RREQ' and check if it received the RREP from any node other than current route, then reverse tracing operation performed to detect the partial malicious node. Once the partial malicious node detected, in second phase we start performing the fine grained analysis on detected node by extracting the other parameters such as mobility, congestion etc. Based on the extracted parameters, the fine grained analysis estimate the extract reason of packet losses. If the partial detection outcome and fine grained analysis outcome is similar, then node is marked as malicious, add to the attacker list and alarm packet sent to other nodes. Else, if we detect the other reasons of packet losses, then we marked that node as unstable temporarily, discard current route, and discovery new route except the recently marked unstable node. The list of unstable node is periodically updated at each round based on their fine grained analysis outcomes. These approaches not only improve the detection rate, but also minimize the packet drops and excessive overhead due to the high mobility and congestion in network.

A. Stage I Malicious Detection

This step based on the combined properties of proactive and reactive techniques. The process is consist of three main steps such as (1) initial bait step, (2) initial reverse tracing step, and shifted to reactive defence step. As stated in [8], the (1) and (2) belongs to the proactive approach based functionality and (3) belongs to the AODV route discovery start process.

In introductory lure step, the malicious hub force in to send the course answer RREP packets utilizing the snare RREQ' once the PDR unfit beneath the set limit esteem. once the RREQ' gotten by malicious hub, it will publicize itself as having the briefest approach towards the destination hub. this could be potential as indicated by system of irregular selection of agreeable goad address. In beginning converse following advance, the switch following project familiar with acknowledge the practices of malicious nodes through the course answer to the RREQ' message. within the event that a malicious hub has gotten the RREQ', it'll answer with a false RREP. suitably, the spin following operation are going to be diode for nodes obtaining the RREP, with the target to conclude the questionable approach knowledge and also the incidentally confided in zone within the course. It have to be compelled to be accentuated that the planned technique will establish over one malicious hub all the whereas once these nodes send answer RREPs. At long last, once the safeguard step (1) and (2), the DSR course revealing method is initiated. At the purpose once the course is ready up and if at the destination it's discovered that the packet delivery magnitude relation altogether tumbles to the sting, the situation arrange would be activated once more to spot for persistent maintenance and continuous response proficiency. the sting could be a unsteady associate degree incentive within the vary [0.85 to 0.95] which will be balanced by this system proficiency. The underlying edge esteem is set to 0.9. The calculation 1 outlining whole usefulness of helpful snare location which is the initial segment proposed HCBDS technique. As appeared in calculation 1, the edge dynamically registered utilizing when the PDR falls under a similar edge esteem. On the off chance that the If the sliding time is shorter, it accept that malicious nodes are as yet present in the system and subsequently the edge ought to be expanded, else edge will be diminished. The procedure of introductory trap step and starting converse following advance are utilized in Detection () calculation 2 to gauge the Stage I malicious discovery.

Algorithm: Stage I Malicious Detection
Inputs S: source node D: destination node P: current data to transmit γ: discovery hop limit T=0: route discovery timer σ1: store time when the PDR falls below threshold at nth iteration σ2: store time when the PDR falls below same threshold at n+1th iteration P^{sent}=0: total number of sent packets from source node P^{rcvd}=0: total number of received packets at destination node Φ =0.9: PDR threshold value

1. M = Detection () // Initial proactive defense
2. S initiate route discovery
3. S broadcasting RREQ
4. Start timer T to record the current discovery time
5. IF (S Received RREP from True D)
6. Forward (P)
7. $P^{sent}++$
8. IF (ACK)
9. $P^{rcvd}++$
10. END IF
11. ELSE IF (T > γ)
12. STOP
13. ELSE
14. Resending RREQ packets
15. END IF
16. Compute current PDR of nth iteration
17. $(PDR)^n = \frac{P^{rcvd}}{P^{sent}}$
18. IF ($(PDR)^n < \Phi$)
19. M = Detection () // Initial proactive defense
20. σ1 = CURRENT TIME;
21. END
22. IF ($(PDR)^{n+1} < \Phi$)
23. M = Detection () // Initial proactive defense
24. σ2 = CURRENT TIME;
25. END
26. IF (σ1 < σ2)
27. IF (Φ < 0.95)
28. Φ = Φ+0.01
29. ELSE IF (Φ > 0.85)
30. Φ = Φ-0.01
31. END IF
32. ELSE
33. Φ = Φ
34. END IF
35. IF (!M)
36. Stage II Malicious Detection Process (Algorithm 3)
37. END IF

Algorithm 2: Detection ()
Inputs S: source node D: destination node Output M: store the malicious node address at first step

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

1. Start Initial Bait by S
2. S selects the adjacent node nr randomly
3. Generate bait RREQ' in cooperation with nr
4. S send RREQ'
5. IF (RREP && ! nr)
6. Start initial reverse tracing step
7. Store the address of Nodes sending RREP to RREQ'
8. Send test packets
9. Recheck message to estimate the malicious node
10. Store the traced nodes
11. M = {n1…nm}
12. END IF
13. Return M

B. Stage II Malicious Detection

After, completion of Stage I process of malicious node identification, we initiate stage II process (if malicious nodes detected) to verify the correctness of malicious node detected based on packet losses parameters. We used two important parameters to estimate the reasons of packet loss at particular malicious detected node such as Congestion or Queue overflow and nodes mobility. We analyze the congestion and mobility changes parameters of each node to estimate the difference between a PDR dropped due to malicious nodes and said parameters. Using this fine grained analysis, we can able to estimate the actual cause of PDR drop. The range of values taken by each parameter is a decimal value ranging in [0; 1].

C. Queue Congestion:

In MANET, congestion is means the queue overflow which can be caused due to multiple simultaneous tasks performed by nodes. The congestion resulting from an amount of data packets that exceeds the queue length may also lead to packet losses by overflowing the queue. Therefore, we need to track the queue status using the Traffic load intensity (TLI) [28] at the neighboring nodes. The source node periodically computes the traffic load statistics of every forwarding node in routing table. At MAC layer, each forwarding node periodically shares its interference queue length and transmitted to source node via HELLO message. In this paper, we computed the probability of packet transmission using TLI metrics. The TLI estimation of node X computed as following:

$$(\mathrm{TLI})^{X} = \frac{\mathrm{ATL}^{X}}{q^{X}_{max}} \quad \ldots\ldots (1)$$

Where q^{X}_{max} is the length of interference queue of node X. The ATL^{X} is average traffic load at the node X which is computed as following:

$$(\mathrm{ATL})^{X} = \frac{1}{Q}\sum_{i=1}^{N} q^{i} \quad \ldots\ldots (2)$$

Where, Q is the total number of queue length samples and qi is the ith queue length of current time of forwarding node X. Based on the TLI value computed for forwarding node X [30], we estimate the packet forwarding probability of node X related to the queue congestion parameter as following:

$$P^{load} = 1 - \mathrm{TLI}^{X} \quad \ldots\ldots (3)$$

We used P^{load} is the packet forwarding probability with respect to congestion load of node X. Higher the probability, lesser the packets loss at node X.

Mobility: This is another vital parameter that causes the excessive packet drops in network. The mobility of nodes in its neighborhood is determined by computing the neighbourhood link changes rate (LCR) [29]. The LCR used to analyze the reasons of packet losses. The LCR at node X is computed as following:

$$(\mathrm{LCR})^{X} = \frac{\sigma^{X}+\gamma^{X}}{\max(\sigma^{X})+\max(\gamma^{X})} \quad \ldots\ldots (4)$$

Where, σ^{X} is the link arrival rate and γ^{X} is the link breakage rate of node X.

By using the Eq. (4), the probability of successful packet transmission with respect to the mobility is computed as following:

$$P^{mobilty} = 1 - \mathrm{LCR}^{X} \quad \ldots\ldots 5)$$

As observed in Eq. (3) and (5), higher the TLI (high load) and LCR (high mobility) of node X, lesser the chances of successful packet transmission by node X.

We can further compute the final probability for successful packet forwarding as following:

$$P^{final} = \frac{P^{load}+P^{mobilty}}{2} \quad \ldots\ldots (6)$$

The final probability values computed by the source node S and check the current behaviour of every node (detected as malicious) in order verify the correctness of malicious detection. Algorithm 3 presents the second stage II malicious detection process. We keep the threshold value for successful probability of packet forwarding as 0.5, as it is enough to justify the behaviour of analyzed node. If node having the packet forwarding probability more than 0.5, then it is verified as malicious node else it is not malicious node.

Algorithm 3: Stage II Malicious Detection

Inputs
M: set of n number of malicious detected nodes in stage I
S: source node
δ=0.5: threshold value to check the successful packet delivery probability
Output:
M': verified malicious node list

1. FOR i:n
2. S Compute P^{load} (M(i)) using Eq. (3)
3. S Compute $P^{mobilty}$ (M(i)) using Eq. (5)
4. S Compute $P^{final}(M(i))$ using Eq. (6)
5. IF ($P^{final}(M(i)) > \delta$)
6. M'(i) ='true'
7. ELSE
8. M'(i) ='false'
9. END IF
10. END FOR

Finally, both stage I and II returns the set of detected and verified malicious list to source node S respectively. Further one-to-one mapping performed between M and M'. If the outcomes for current node in both set matching, then it is marked as malicious by source node and adds into the blackhole list. The alarm packet broadcast by Source node

to it other nodes to intimate the presence of malicious node/nodes in network. If the outcome of both stages does not match for X node, it means that node not malicious and the causes of packet losses at X are identified as mobility and congestion. Therefore, we discard the current route by marking node X as unstable and restart the process. The nodes added to the unstable list are verified at each interval to check the status of successful packet transmission probability. If packet transmission probability of node X later becomes more than 0.5, then we remove the node from the list of unstable. This approach not only saves the excessive packet drops due to incorrect prediction of malicious nodes but also achieves the load balancing in MANET communications.

IV. RESULTS AND ANALYSIS

We present evaluation of proposed HCBDS protocol for MANET in this section. We compared the performance of proposed HCBDS method versus the benchmark security methods such DSR and CBDS [8]. The NS2 version 2.34 used to implement and evaluate the performance of proposed method. We selected two simulation experiments to evaluate the effectiveness of proposed algorithm such as varying mobility and varying number of malicious users in network. We vary the mobility speed from 5 m/s to 25 m/s. Following performance metrics considered to evaluate proposed method:

Average Throughput: it is average rate successful of data transmission from all source nodes to intended destinations per second.

Packet delivery rate: it is percentage of successful packets received at receiver with respect to total generate packets.

End to end delay: average time required to transmit packet from source to destination.

Detection Rate: the percentage of malicious nodes detected among the total number of malicious nodes within the network.

We implemented the adversary model to estimate the effectiveness of proposed routing protocol. In this attack model, the malicious nodes drops all the packets transmitted to them. We vary in malicious nodes range from 0 % to 40 %.

In section A, impact of varying number of malicious nodes on routing performance presented. In section B, the impact of varying mobility under the presence of malicious nodes presented. Table 1 shows the common parameters used for the simulation analysis.

Table 1: Network Parameters

Number of Nodes	50
Traffic Patterns	CBR (Constant Bit Rate)
Network Size (X * Y)	1000 x 1000
Max Speed	5 – 25 m/s
Simulation Time	500 seconds
Number of Malicious Nodes	0-40 %
Transmission range	250m
Routing Protocol	DSR, CBDS, and HCBDS
MAC Protocol	802.11
Channel Data Rate	2 Mbps
Mobility model	Random waypoint

A. *Malicious Density Evaluation*

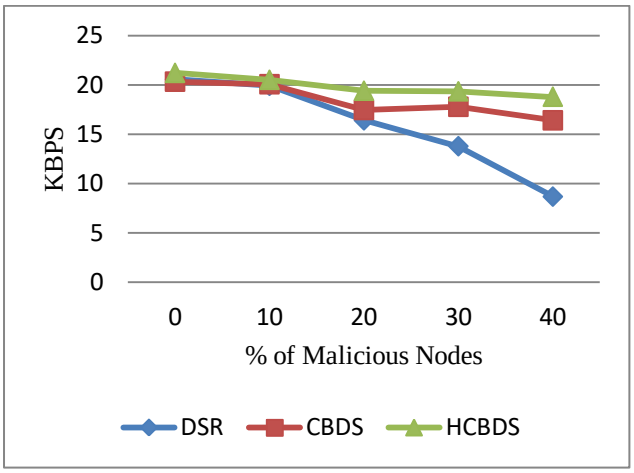

Figure 2: Throughput vs. Varying Malicious Nodes

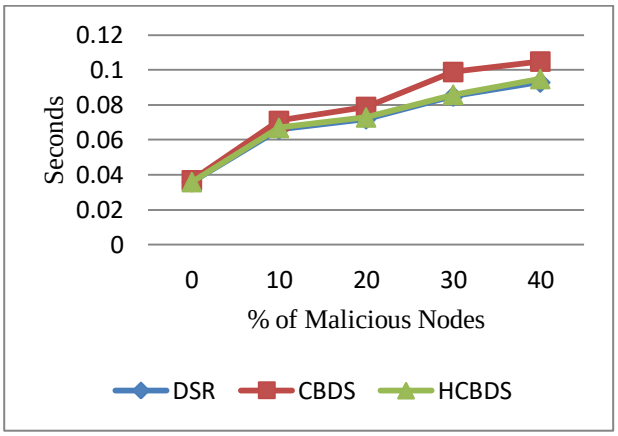

Figure 3: Delay vs. Varying Malicious Nodes

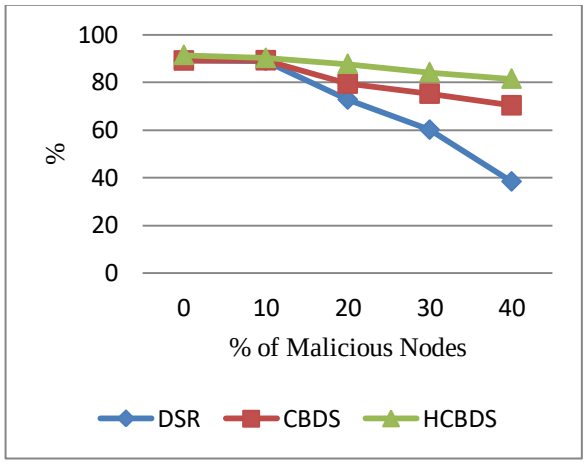

Figure 4: PDR vs. Varying Malicious Nodes

The results observed in figure 2, 3 and 4 for average throughput, average delay and PDR versus the varying malicious nodes respectively. The result captured for throughput and PDR in figure 2 and 4 respectively with maximum moving speed of mobile nodes is 10 m/s. From the result it is noticed that DSR protocol significantly suffered from the malicious nodes attack as the malicious

nodes increases in network. DSR does not have the security method for the detecting the malicious nodes in network. The CBDS method shows the significant improvement in PDR and throughput performance as compared to DSR. CBDS method can manage the maximum throughput and PDR even if the number of malicious nodes increases. However, still the performance dropping steadily in CBDS as the number of malicious nodes increases. This is due to possibility of incorrect malicious nodes detection in CBDS. The figure 5 shows the result for detection rate performance between CBDS and HCBDS. It shows that as the number of malicious nodes increases, the detection rate of CBDS also decreases. It means CBDS detecting the malicious nodes incorrect and hence leads to poor performance for throughput and PDR as compared to HCBDS. Due to dual stage verification, the incorrect detection is reduced as the other causes for the packet losses determined and new healthy path discovered for data transmission. Therefore, the delay performance in figure 3 shows the reduction in delay as compared to CBDS approach.

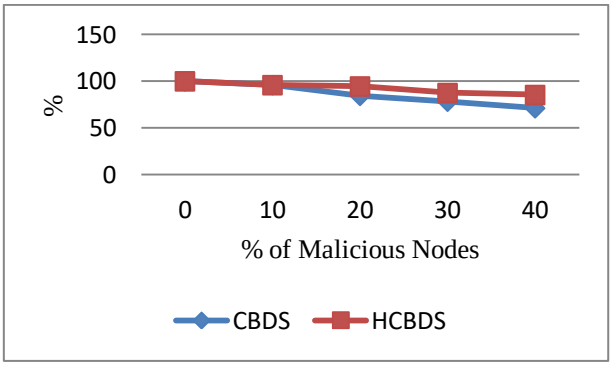

Figure 5: Detection rate vs. Varying Malicious Nodes

In Fig. 3, it can observed that as the number of malicious nodes increases, delay performance also increases due to extra false RREP generated by the malicious nodes in network. The DSR protocol produces the less delay as compared to CBDS and HCBDS. This is attributed to the fact that DSR has no intrinsic security method or defensive mechanism. The CBDS and HCBDS protocols take time to verify and secure the communications in network. The proposed HCBDS protocol achieved the significant trade-off between the network delay and QoS performance as compared CBDS and DSR protocols.

B. Mobility Evaluation

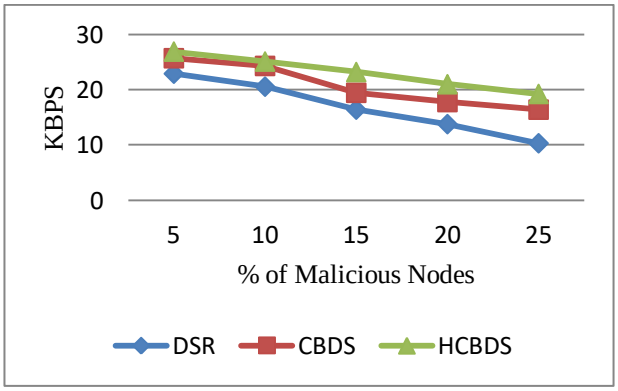

Figure 6: Throughput vs. varying mobility

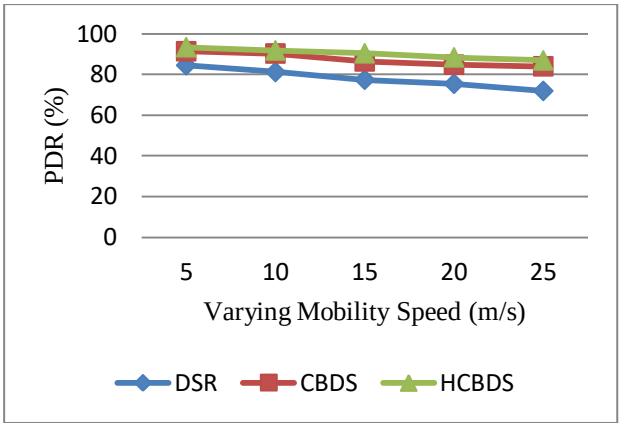

Figure 7: PDR vs. varying mobility

The results observed in figure 6, 7 and 8 for average throughput, PDR, and average delay versus the varying mobility speed respectively. The result captured for throughput and PDR in figure 6 and 7 respectively with maximum number of malicious node is 10 out of 50 nodes. From the results it is observed that as the mobility increases, the performance of throughput and PDR decreases (due to mobility impact) and delay (Fig. 8) increases. The DSR protocol produces the worst performance as compared to the CBDS and proposed HCBDS routing protocol as DSR does not have the security method to detect the malicious nodes in network.

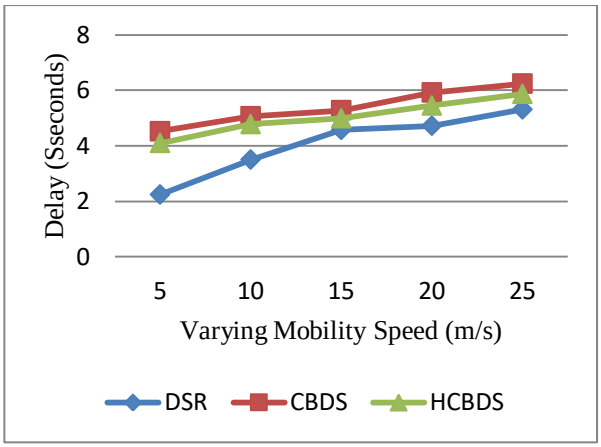

Figure 8: Delay vs. varying mobility

As observed in figure 9, the detection rate performance if higher in proposed HCBDS method as compared to CBDS technique, as the two stage detection technique applied. In CBDS method, as every dropped PDR performance is considered as the malicious performance and the traced node is marked as malicious, more number legitimate nodes detected as malicious. But in HCBDS, we analyzed the other causes of dropped PDR before declaring particular node as malicious which helps to increase the detection rate as well as network QoS performance.

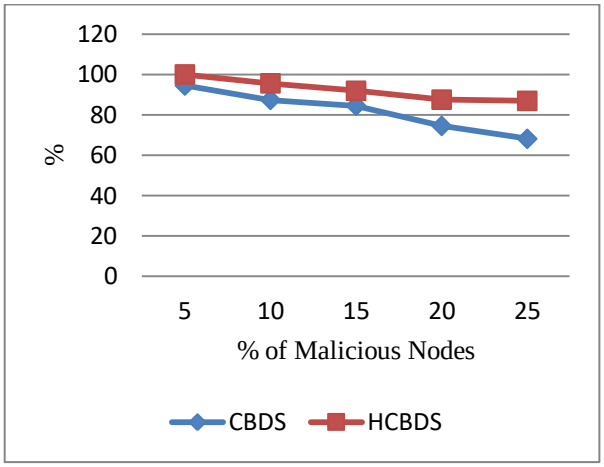

Figure 9: Detection rate vs. Varying Mobility Speed

V. CONCLUSION

In this paper, we proposed novel Hybrid Cooperative Bait Detection System (HCBDS) for the efficient detection and mitigation of malicious nodes in MANET. HCBDS is two stage process to correct detect the malicious nodes in which we first performed the cooperative malicious detection process and then we verified the detected malicious nodes through fine grained analysis of particular nodes using the packet losses parameters such as mobility and congestion. The simulation results claimed that proposed method outperforms the benchmark methods DSR and CBDS in terms of throughput, PDR, and detection rate. The HCBDS outperformed the CBDS in terms of delay performance as well. For the future work, we intend to investigate (1) varying density evaluation, (2) determine and investigate the other parameters of packet losses, and (3) investigate the performance of proposed method under the different security threats.

REFERENCES

1. P.-C. Tsou, J.-M. Chang, 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 Intl. Conf. Wireless Commun.,VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
2. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013).
3. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in proceedings of the 6th annual ACM Intl. conference on Mobile computing and networking, 2000.
4. S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol," in proceedings of the 3rd ACM Intl. conference on Mobile ad hoc networking & computing, 2002.
5. K. Balakrishnan, J. Deng, and P. K. Varshney, "Twoack:preventing selfishness in mobile ad hoc networks," in IEEE Wireless Comm. and Networking Conference, 2005.
6. A. Al-Roubaiey, T. Sheltami, A. Mahmoud, E. Shakshuki, and H. Mouftah, "Aack: Adaptive acknowledgment intrusion detection for manet with node detection enhancement," in 24th IEEE Intl. conference on Advanced Information Networking and Applications (AINA), 2010.
7. E. M. Shakshuki, N. Kang, and T. R. Sheltami, "Eaack— a secure intrusion-detection system for MANETs, " IEEE Transactions on Industrial Electronics, 60(3):1089–1098, 2013.
8. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE SYSTEMS JOURNAL, 2015
9. O. Khalid, S. U. Khan, S. A. Madani,K. Hayat, M. I. Khan, N. Min-Allah, J. Kolodziej, L. Wang, S. Zeadally, and D. Chen, "Comparative study of trust and reputation systems for wireless sensor networks," Security and Communication Networks, 6(6):669-688, 2013
10. M. Zhao, Y. Li, and W. Wang, "Modeling and analytical study of link properties in multihop wireless networks," IEEE Transactions on Communications, 60(2):445–455, 2012.
11. C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against olsr: Distributed key management for security," in 2nd OLSR Interop/Workshop, Palaiseau, France, 2005.
12. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5):536-550, 2007.
13. T. Sheltami, A. Al-Roubaiey, E. Shakshuki,and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Multimedia systems, 15(5):273-282, 2009.
14. A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
15. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.
16. K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.
17. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.
18. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.
19. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.
20. H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.