IT in Industry, vol. 9, no.3, 2021 Published online 18-May-2021

"DETECTION AND PREVENTION OF COOPERATIVE BLACK-HOLE ATTACK FOR SECURING THE NEXT GENERATION MANET USING HBCD IN DSR"

Mr. Ganesh D. Dangat ,
ganesh.dangat@kbpcoes.edu.in Research Scholar, Sathyabama University
Dr. S. Murugan. ,
snmurugan@gmail.com Sathyabama University, Chennai India

Abstract
Localized mobility management executives is a terrific test in Wireless Networking that means to create design for quick and effective handover in an administrator's organization to augment the presentation of the portability the board in general. Right now, worldwide portability the executives is utilized to keep up confined versatility the board while it is perceived that a committed limited convention is fundamental for productive handover measure. Transparently open correspondence signals raise a high security hazard in cell Networks that are Ad hoc. Organizations that are Ad hoc are especially defenseless to arrange layer assaults like DoS. The summed up assaults on network which is Ad hoc are Cooperative blackhole attacks. Here, by communicating inaccurate data on steering, the hubs that are malignant disturb information transmission on the organization. An acknowledgment of these assisted us with tending to the subject of information security from an alternate perspective in remote organization which is Ad hoc to give a correspondence way, liberated from all security dangers recently recorded. To guard the organization from outer dangers, numerous incredible and stable arrangements have been recommended. They additionally need awesome methods of distinguishing and forestalling inside dangers, in any case. The objective of this work is to utilize HCBDS to carry out a compelling convention Distance Vector Routing (DSR), that dispenses with by separating the hubs that are noxious, consequently guaranteeing correspondence wellbeing. The hubs that are moderate getting mistaken data on steering from their neighbor hub are arranged to see the hub as noxious and keep the data in the table to achieve this reason. As an Ad hoc network, anytime, hubs will join or leave. Thus, it needs a suitable assurance structure. Through utilizing the proposed HCBDS, genuine malevolent exercises can be isolated from communicating mistakes and the hubs that are vindictive can be effectively found. The calculation proposed utilizing secure steering convention acquires the most extreme throughput with least energy usage.

Keywords- WSN, malicious node detection, Network Simulator 2(NS2), Mobility.

I. Introduction:

An Ad hoc network is a wireless network of a clustered kind. It has no set infrastructure and the nodes are able to connect directly with each other [1][2]. It consists of different nodes that are related by connections. Since they are unsecured and wireless in nature, protection in network which is Ad hoc is a big concern. [4]. The nodes must only exchange a key that is private to the authenticated neighbor nodes in order to provide encryption, so that we can meet the various security objectives such as secrecy, honesty, non-repudiation, availability and authentication. The primary benefit of the network which is Ad hoc is its affordable and simple construction. Network which is Ad hoc are very vulnerable to network layer attacks by Dos.

The generalized attacks on network which is Ad hoc are Cooperative blackhole attack. Nodes that are malicious disrupt network data transfer in a sybil attack by sending incorrect information on routing [2]. Nodes that are malicious relay incorrect information on routing in an attack called the black hole and tell the adjacent nodes they have the smallest path to the node which is the destination. The source sends packets via these nodes that are malicious after receiving this false information, and the nodes that are malicious drops the packets. The

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

packets will not, however, enter the node that is the destination on the network. It is said that the attack Grayhole is an expansion of the attack Blackhole, since the existence of the nodes that are malicious cannot be expected. The Sybil assault is like the transient perception of creating new nodes or creating new network entities and transmitting fake information to another network node. It might behave like nodes that are malicious a few of the times and like regular nodes on the others. Both these attacks interrupt the route discovery mechanism and decrease the ratio of throughput and packet distribution.[3]

The CBD approach in [2-3] detailed the efficiency of the platform measured on the basis of the Packet Distribution Ratio or PDR of halfway source and destination link nodes. In case of any event, there are situations in which protection procedures of MANET struggle to fix alternative explanations for a dropped PDR situation in the state of workmanship. In comparison, this finding has since improved the positive rate falsely by separating the nodes that are real as less effective and malevolent in identifying the original nodes that are pernicious. The aim behind such insufficiencies is to agree that prolonged packet misfortunes or dropped PDR occur in consequence to malevolent exercises by having nodes that are out of hand from certain present security plans. Behind the falling PDR in MANET, there are a few distinct reasons, such as high data rate, blockage or over the top load, high portability, etc. For example, under the criteria of flexibility and data volume being high, the usual methods will take us to false estimates of nodes that are malevolent [1-3].

An important safety mechanism is built in this paper to secure contact called HCBD and to avoid attacks using the DSR protocol. In this process, it first tests if there are any nodes that are malicious in the network as the network is formed consisting of several nodes. The method of advanced DSR protocol is used to delete these nodes that are malicious. The nodes that are malicious are thus removed. If a neighboring node receives inaccurate information on routing from any node that is intermediate, the node should be considered a node that are malicious. Via the path answering packet, the node that is intermediate tells the remaining nodes about the nodes that are malicious and any node that receives the information; its routing table is updated to mark the node as malicious. In case an RREQ is sent, node list that are malicious is appended and its routing table is modified by the other nodes. Thus, by detecting incorrect information on routing or reviewing the routing table, the nodes can recognize the list of nodes that are malicious so that they can warn other nodes not to accept the nodes that are malicious' information on routing. The network is made up of many nodes linked by ties. Each node has a specific Id, and the Identity of the corresponding source node is stamped on each packet. At every computer node in the network, this essential knowledge is preserved.

The new MANET or Mobile Ad hoc Networking technology is built on a multi-hop design which is wireless without a rigid infrastructure and previous network node setup. The key aspects of this latest networking model have the following: (I) the mutual sponsorship of simple networking roles, such as routing and data transmission; (II) the absence of hierarchical limits of network nodes; (III) the absence of a central network entity; and (IV) dynamic network node relationships in general. As a consequence, a node is unable to make any conclusions on the trustworthiness of its colleagues, who support the node in its correspondence and do not have their certificates in general. One of the key challenges of networks that are Ad hoc and, in particular, a requirement for stable and QoS or quality-of-service connectivity in environments that are adversarial is maintaining the basic network activity. In the face of adversaries, via an unpredictable, constantly evolving multi-hop wireless network topology, the task is to secure communication and sustain synchronization. Both stages of communication, data transmission and path discovery must be safeguarded to solve this complex issue and provide robust protection. A number of studies have recently suggested protected mechanisms of routing to protect against a number of attacks under varying device requirements and assumptions [1]-[8]. Safe protocols of routing alone, however, which ensure the accuracy of

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the discovery of the path, do not guarantee stable and uninterrupted data transmission. In other words, it is not possible to render a right, up-to - date route immediately free from adversaries. For e.g., an intelligent opponent will obey the route discovery rules, put himself on a path, and then start forging, redirecting traffic or dropping, and data packet injection. Clearly, for a large amount of time, an enemy will mask its deceptive actions and strike when the time is least anticipated. Thus, before their strike, it is difficult to discover such an enemy [1].

Networks that are Ad hoc are self-organizing wireless multi-hop networks in which all the nodes engage in the packet forwarding process. Since they do not require any fixed equipment, such as routers or base stations, Networks that are Ad hoc can quickly be deployed. Also, they are particularly important to natural disasters, emergency deployments, missions of search and rescue and strategic battlefields. In mobile Networks that are Ad hoc, connectivity comprises of 2 phases: exploration of routes and data transmission. Routing protocols that are secure are the cornerstone for reliable data transfer and are thus a significant field research of ad hoc on networks. Many protection methods and measures have been introduced [1-9]. It deals very well with external threats, but they either resolve the problem of an attack that is internal only slightly or merely presume an attack-free environment internally. Apart from their inadequacy in defending the infrastructure from internal threats, certain protection frameworks used in SRPs offer valuable insight into addressing data transmission security concerns. For e.g., Ways to use hash chains, with assumption that the routers have clocks synchronized, to safe routing algorithms is demonstrated in [25]. His programme, however, lacks promptness, as it only can track attacks way beyond the time of their occurrence. In [6] implemented a "leap-frog" method of routing that can predict a failure of router in the algorithm of flooding. A credibility system is suggested in [7] and [8], where the nodes that are malicious are statistically detected and their actions are blocked. The drawbacks to this strategy are that the usage of overhead is high, the method of detection is time consuming, and often the result is incorrect. The author introduced in [9] a stable routing protocol on-demand that is immune to errors Byzantine, consisting of three attacks forms: stop-forwarding attacks, hacking attacks and sniffing attacks. Post log n faults have taken place, the scheme detects malicious connections, where n is the routing path length. Again, this process has many disadvantages associated with it. Firstly, because it only identifies malicious links post a certain error numbers, it does not respond to the malicious activity in time. Second, it is not feasible for the mechanism to determine if a harmful action or the transmission method itself creates an error. Thirdly, it is hard to enforce this process. In this article, for Networks that are Ad hoc based on protocols of Reed-Solomon, we present a SDTP or secure data transmission protocol. It exploits the multi-path routing redundancy and, in spite of an adverse environment suffering from attacks like Byzantine, remains powerful and reliable. With only modest overhead multi-path communication and very rational expectations, the reliability of data transmission is done without intrusion detection schemes [10] being used.

However, there are situations in which modern confidence-based strategies struggle to grasp the precise essence of the causes of an adverse case. This results in several false positives that are deemed malicious by legitimate nodes and poor detection rates for nodes that are malicious. The rationale for such vulnerabilities is because these confidence-based protection mechanisms presume because losses of packet occur only due to of actions that are malicious by nodes which are misbehaving. These are, Anyways, for different reasons, such as failures in the propagation of agility, congestion and wireless connections. Without a fine-grain study of packet losses, traditional detection schemes can lead to erroneous estimates of confidence, especially in the sense of high node mobility and data rates [11].

The remainder of the research is structured in the following manner: Section IV offers the nodes that are malicious identification system in Section II, Similar Work, III Study Process. Simulation consequences in section V.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Finally, in section VI, a brief conclusion of the paper is given.

II. RELATED WORK

Amount of methods learned since the last two decades to address the question of nodes that are malicious identification in MANETs. Much of these strategies agitate the identification of one suspicious node or involve tremendous resources in terms of time and money for coordinated blackhole attacks from police work. In addition, in order to function, a variety of these approaches require unique environments [5] or assumptions. The methods of nodes that are malicious detection are primarily divided into three groups, such as proactive, reactive methods of detection and methods of hybrid detection. Proactive detection methods [12]-[13] are needed to track neighboring mobile nodes regularly in order to identify nodes that are malicious. Therefore, the overhead of detection is continually generated despite the lack of nodes that are malicious, and the resources required for detection are often continually expended. One of the disadvantages of these types of systems, though, is that in the initial stage it can promote the protection or avoidance of related attacks. The process of detecting nodes that are malicious was only initiated by the reactive detection strategies [15]-[17] when the various packets fell reportable at the node that is the destination. To efficiently locate the nodes that are malicious, the hybrid finding strategies [1][8] combine every proactive and reactive approach. The advantages of both constructive and reactive routing protocol have been used by these techniques. A proposal of 2ACK for the finding and identification of routing corruption in MANETs was proposed in [17]. This plan contains, two-jump affirmation packets being sent to the other side of routing to prove that the packets containing information have been effectively received. The proportion of the received packets containing information for which the affirmation is needed is also regulated by a parameter affirmation ratio, i.e., Rack. This strategy has a position in the class of constructive plans and thus generates excessive overhead routing that pays less attention to the presence of dangerous nodes. An anticipation component known as best-effort fault-tolerant routing or BFTR was designed in [21]. Their BFTR conspire uses the beginning of ending affirmations to scan the character of the routing system to be chosen by the destination hub (estimated related to the quantitative relationship and postponement of packet delivery). The supply hub uses another course on the off case that the action of the system goes further from a predefined action collection for evaluating "great" courses. One of BFTR 's drawbacks is that malignant nodes may occur in the current chosen course nowadays, and this configuration is inclined to rehashed course disclosure formats, which can cause massive overhead routing. The method mentioned in [8] showed that the proactive and reactive protection approaches were outperformed by hybrid approach; however, they relied on only the PDR parameter to label nodes as nodes that are malicious, and this could contribute to degrading the efficiency of correctly detecting nodes that are malicious. If the PDR fell below the threshold in this process, then the reverse tracking algorithm used to find the nodes that are malicious was used. However, there are different explanations for packet losses in MANET, so before detecting the node as malicious, the correctness of packet losses should be checked. The two-stage identification method is conducted by our proposed HCBD techniques to reliably identify nodes in MANET as malicious. In this article, we considered the CBD system [8] along with the DSR-based protection method as a comparative methodology for performance comparison purposes. On top of the routing protocol, we have played with FGA scheme implementation. For MANET defense, for example, trust-based techniques, there are various distinct strategies detailed. There were a few techniques seen in later times to calculate the packet misfortunes. To calculate the packet misfortune rate over connection, [24] suggested a strategy that uses planned measures of the transmission tally. The packet misfortune rate is efficiently managed by such a scheme, but the true cause for packet misfortune cannot be differentiated. A fine-grained investigative strategy to investigate the causes for packet failure in wireless sensor

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

systems or WSNs was suggested in [4]. The parameters used for relation profiling in such a technique are the LQI or link consistency indicator and RSSI or obtained signal intensity indicator.

Most of the strategies are focused on packet losses or dropped PDR as the crucial parameter for node identified as harmful, the discussed methods above failed to acquire the tradeoff among the output of the QoS or Quality of Service and detection rate results. In order to accurately identify the compromised nodes by taking into consideration the other triggers of losses of packet, there is an absence of a single protection mechanism that performs the verification in two-stages. This will also result in inaccurate malicious detection results under the constraints of the data rate network and high mobility. In this article, we suggested the approach of hybrid to solve the issue of methods that are state-of-the-art in which two step methods are built to avoid incorrect confidence assessment and increase the efficiency of the network in the presence of nodes that are malicious. This paper's main contributions are: To develop the MANETs new two-stage hybrid cooperative bait detection system based on reverse tracking and fine grain analysis. In the first point, for different network situations, we used the CBD approach effectively to enhance security efficiency. If the PDR output fell dramatically and beyond the threshold limit, after which the form of tracing in reverse obtained to identify the nodes that are malicious was used. As far as stage 2 is concerned, if a node is detected as malicious from step 1, then it will not be automatically identified malicious, therefore it may continue to proceed through the review which is fine-grained to approximate the other causes for losses in the packet and accurately evaluate whether or not the node identified in step 1 is malicious. In terms of detection precision and other routing QoS criteria, the performance assessment was presented.

In this work, a sybil attack model has been applied to verify the efficacy of the proposed FGA method. The nodes that are malicious output of data packets fall randomly with a 25 percent chance in this type of attack model. The number of fraudulent nodes varies from 5 percent to 20 percent of the total number of nodes installed. So, it impacts the system's efficiency.

III. RESEARCH METHOD

In this article, we have suggested the Hybrid Cooperative Blackhole Detection System or HCBD nodes that are malicious detection tool. This approach is just a parameter for nodes that are malicious identification, intended to find solutions to the issues of all detection systems previously, that are mostly based on the losses in the packet. The HCBD proposed is a detection mechanism which is two-staged in which the nodes that are malicious detection errors were not only provided by the MANET defense, but also decreased. Many protection technologies [20] rule out accurate identification of nodes that are malicious.

As seen in the following figure, by broadcasting the RREQ message to its neighbor nodes, source node S initially begins the route exploration. The obtained RREP tested if it was from the true node of destination D. The data transfer process starts until the path is found. The PDR is evaluated and compared to the complex threshold value at each interval. If the PDR falls below the threshold at any interval, then the source node transmits the new kind of RREQ known as Bait RREQ and checks if the RREP was obtained from any node apart from the existing path, then reverses the procedure of tracing performed to identify the partial nodes that are spiteful. If the partial nodes that are spiteful has been established, the fine-grained analysis on the observed node starts in the second step by absorbing other parameters like latency, mobility, etc. The analysis that is fine-grained determines the cause for packet errors on the basis of the derived parameters. If the partial detection result and the result of the fine-grained review are identical, then the node gets labeled as malicious, added to the attackers list, and the warning packet is sent to other nodes. Otherwise, if we detect other causes for packet losses, we have temporarily marked the node as unreliable, discarded the current path, and discovered a new path several than the recently named insecure node [29]. During each round, the list of unstable nodes is revised regularly

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

based on their fine-grained analysis performance. Not only can these techniques increase the identification efficiency, but they also decrease packet losses and unsustainable overhead due to high network latency and congestion.

The performance review of the proposed device model, namely HCBD, is analyzed and compared with the FGA framework based on the ratio of packet distribution, transmission delay and throughput to check how successful the secure routing protocol applied in the presence of the Sybil attack is.

The node mobility against packet delivery ratio, Throughput & end2 end delay is shown. Packet Delivery Ratio of HCBD is **96.5** %., throughput is 38.37 & end to end delay is 0.34 in the presence of Sybil attack, which is better than FGA approximately. By using proposed system it is possible to improve overall preference of network to get maximum throughput with less time [29].

IV. Malicious Activity Detection:

Using their power, the nodes that are malicious nodes try to undermine other nodes or the whole network by attempting to participate in all existing routes, causing other nodes to use a malicious path under their influence. They trigger severe attacks after being chosen in the requested direction, either by dropping all received packets as in the case of an attack called the cooperative black hole, or selectively dropping packets in the case of a grey hole attack, or by generating a sybil attack picture connection. These nodes that are malicious are referred to as MN nodes for simplicity. Other nodes do not face a major threat, so the routing protocol should easily be overlooked.

On the other hand, routing protocols are much riskier for the SN1, SN3 and MN nodes (defined in section II). These nodes disrupt the data flow by either dropping or refusing to forward the data packets, causing the routing protocol to restart the path-discovery or, if accessible, to pick an alternate route that could in turn contain any nodes that are malicious again, so the new route may also fail. This approach forms a loop that causes the source to assume that it is not possible to further transfer data. The purpose of this proposed work was to detect nodes that are malicious.

The main objective of the research is to provide an idea about MANET's malicious node detection system (mobile ad hoc networks) to improve security and performance. The program is based on the HCBD framework, the hybrid cooperative based bait detection scheme, which has the function to combat various types of MANET attacks. The method of hybrid CBD (HCBD) is required in order to improve end-to-end delay and PDR performance. Proposed work against the current HCBD approaches would result in an increase in PDR and end-to-end performance for a variety of network attackers.

To identify malicious node in a given MANET we use proposed technique to prevent Cooperative blockhole attack [18].

Although it is very difficult to guarantee a stable network and cognitive layer routing and communication mechanism, this work proposes a trustworthy networking framework that not only provides high trust between the nodes, but also provides the CU with accessible legitimate services.

The network environments of 500 m * 500 m with various numbers of nodes are seen in Table 01 below. In addition, the suggested phenomenon was tested against malevolent situations in which the intruders were infected by a variety of legal nodes. In existence, the CUs became movable, where they could at any moment break from their network or combine. The CU mobility rate with a contact range of 30 m was set at 0-10 m / s. In addition, 802.11 was the underlying MAC layer standard, although the routers' contact range was restricted to 120 m. In order to quantify the protection, during the handoff and communication process, the nodes that are malevolent or CUs were inserted into the environment using the probability distribution [14].

Table 01: Parameter use in ad hoc network for simulation

Parameters	Values
Simulation Time	80 s
Grid Facet	500 m × 500m

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Ad hoc Nodes	250
Transmission Range	140m
Data Size	512bytes
MAC Protocol	IEEE802.11

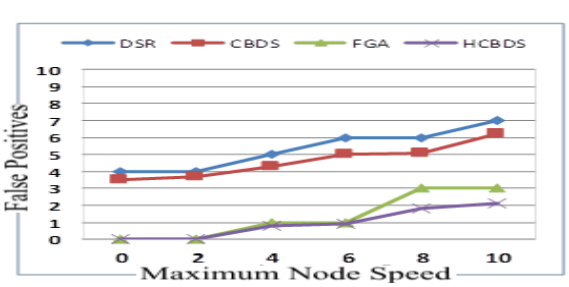
V. Simulation & Results:

Hybrid cooperative blackhole detection system or HCBD performance review of the proposed system model in the Ad hoc Network is tested and contrasted with Boost DSR, CBD, FGA and HCBD routing system based on Packet Delivery Ratio, Processing Latency and throughput to check how successful the stable routing protocol applied in the presence of Sybil attack is.

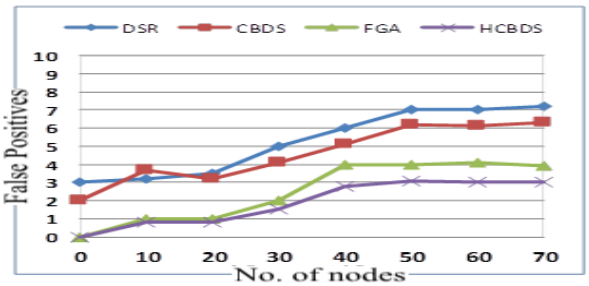
Performance Analysis of proposed system model namely HCBD is evaluated and compared with conventional DSR and CBD, FGA based on parameters like false positives, detection rate, energy consumption, packet loss rate, Packet Delivery Ratio, Processing Delay and throughput to verify, how efficient the implemented secure routing protocol in presence of attack. Following are some Performance analysis of HCBD with proper procedure [27].

1) FALSE POSITIVES

The False Positives Sum is the ratio of legal nodes considered unsafe to the total legal node numbers. We contrasted the architecture proposed with the DSR, CBD, FGA system in the terminology of positives that are false, this time gripping all the frameworks together with our model of optimization, and incorporating nodes that are malicious into the network [12]. The incidence of false positives with increased speed of node movement is shown in Figure 1(a) below. From the diagrammatic representation it is clear that the rate of false positives decreases to a far bigger degree in our HCBD system compared to the other scheme. In reality, our proposed methodology better analyses the overall possible cause of an event of packet drop and then a decision is made on the trustworthiness of the node. Overall, the statistic indicates that with increase in growing node speed the false positive rate increases. This trend has a reason behind it which is that in case nodes move at speeds that are higher, the probability of mis-overhearing at the source node or stale routing information increases considerably, so original nodes are declared when malicious. On similar lines, Representation 1(b) indicates false positive rate along the growing density of the node in the network, keeping the moving speed is 4 m / sec at the node is rigid. With increased count of node in the architecture, the source / destination numbers pairs are also increasing, because due to collisions, more packets are lost in the network. The number of false positives in the HCBD scheme is smaller relative to numerous other schemes, which considers every packet drop as an activity that is malicious, because the frequency of each packet drop is measured before making any judgement on the behavior of nodes [29].



(a)



(b)

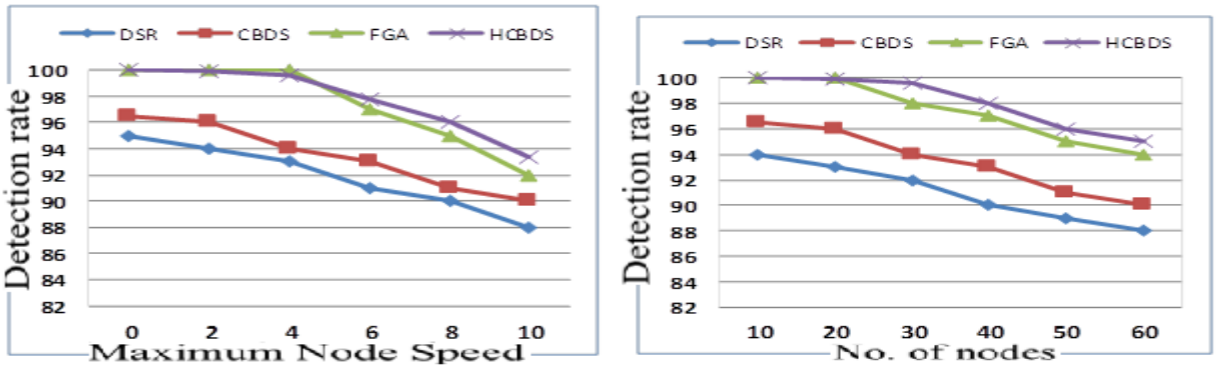
ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Figure 01: Effect of node moving speed and density on false positives. (a) False Positives vs. Node Moving Speed. (b) False Positives vs. Node Densit

2) DETECTION RATE

The rate of detection is referred as the percentage of true spiteful nodes above the total spiteful nodes that the scheme detects. The identification rate is higher in our HCBD solution, as each judgement is more aware about malicious activities and network nodes [23]. On the other scheme, when each packet drop is taken as spiteful and the subsequent node is proclaimed as spiteful, more lawful nodes are mis-detected when spiteful nodes. As shown in the statistics,

Our HCBD framework has a bigger identification effectiveness contrasted with the other plan 's rate. Likewise, Figure 2(a) depicts the recognition rate with expanding hub speed under the HCBD technique and the other plan, and Figure 2(b) depicts the location rate with expanding hub thickness [32]. With developing hub thickness, the quantity of information associations in the organization additionally increments, as more bundles in the organization are lost because of impacts. The other framework considers these parcel drops as acting up activities from genuine hubs. Subsequently, in our HCBD cycle, the identification rate is again higher than the rate in the different cycle [34], as found in the figure.



(a) **(b)**

Figure 02: Effect of node moving speed and density on detection rate. (a) Detection Rate vs. Node Speed. (b) Detection rate vs. Node Density

3) ENERGY CONSUMPTION

Figure 3 shows the energy consumed with increasing node speed under the HCBD scheme and the FGA scheme. The purpose of this experiment is to show the overhead incurred due to processing and communication cost in the HCBD scheme with comparison to the FGA & other scheme that ultimately incurs a higher energy consumption. The most of the node energy is consumed by packet sending and receiving. Our HCBD scheme does not increase the number of exchanged messages, but instead leverages existing routing packets (already required by routing protocol standards) To exchange data such as the status of the queue and the status of the path. The only energy that is extra required by our HCBD system is for the processing of information that is different, like MAC layer information, queue information and rate of link shifts, that is negligible [29]. Therefore, as seen in the diagrammatic representation, the energy expended is precisely equal in both the FGA and HCBD & other schemes, suggesting that our system improves greatly the network security without energy consumption.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

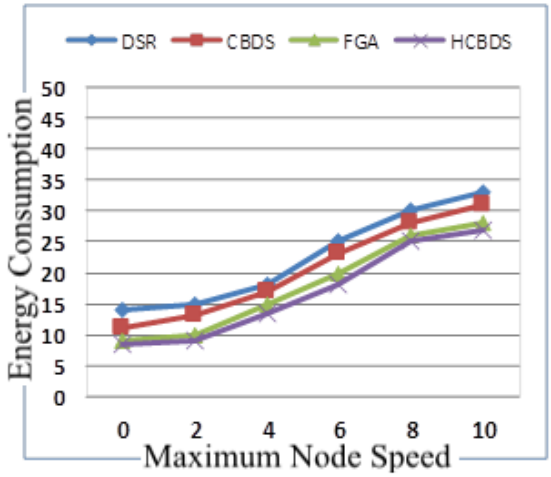


Figure 03: Effect of node moving speed on energy consumption

4) PACKET LOSS RATE

Figure 4 demonstrates rate of packet loss with accelerating node speed under the FGA scheme and HCBD scheme. The loss rate of the packet is lower in our HCBD system, as seen in the figure, than in the FGA system. In the HCBD scheme, more trustworthy nodes are usually preferred for the path of routing, resulting in fewer error packets and a larger transmission ratio of packets. When it comes to FGA & other schemes, valid nodes from the path are isolated, resulting in a higher drop of packet due to the unavailability of forwarding nodes to the destination. Currently, actual nodes that are malicious remain on the path to the network, resulting in more possibilities for them to drop data packets that are valuable [28].

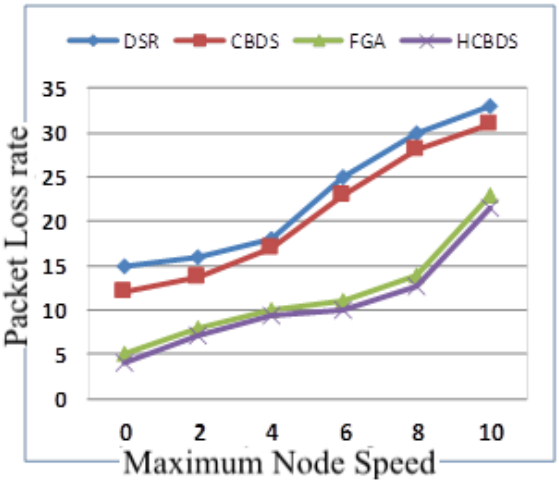


Figure 04: Effect of node moving packet loss rate

5) PACKET DELIVERY RATIO

The malicious nodes against packet delivery ratio are shown in below Graph. Packet Delivery Ratio of Conventional DSR routing protocol is **86.19** %. In the presence of Sybil attack, Insecure CBD & FGA routing protocol is **94.70** % and in proposed HCBD protocol **97.54** %. The percentage data loss in DSR , CBD & FGA under Sybil Attack is increased more than the HCBD routing protocol in all scenarios [35][36].

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

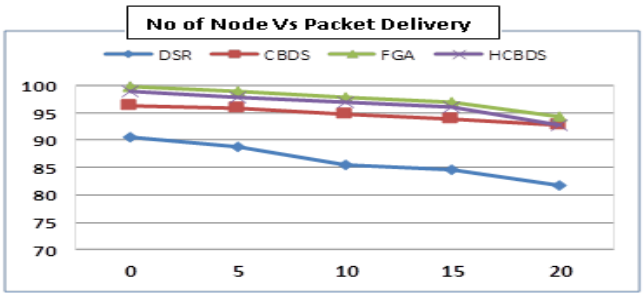


Figure 05: Performance analysis of Packet Delivery ratio using DSR, CBD, FGA & HCBD

6) END TO END DELAY

The end to end delay performance of the conventional DSR, CBD, FGA and HCBD are shown in graph. The CBD, FGA producing over 0.34 % of average end to end delay compared with HCBD produces 0.3 %. From the results, it concludes that the model is flooding minimal delays as compare to other. But at stringent conditions e.g. load increase it may possible to increase the delay in network due to network overhead issue.

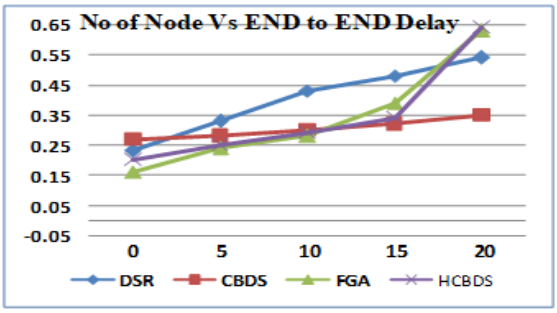


Figure 06: Performance analysis of End to End Delay using DSR, CBD, FGA & HCBD

7) THROUGHPUT

The throughput performance of the conventional DSR, CBD and FGA is given in below table and the results are shown in graph. The HCBD outperformed DSR, CBD & FGA by producing over 38.37 of average throughput. The DSR is the least and its throughput had numerous fluctuations under Sybil Attack.

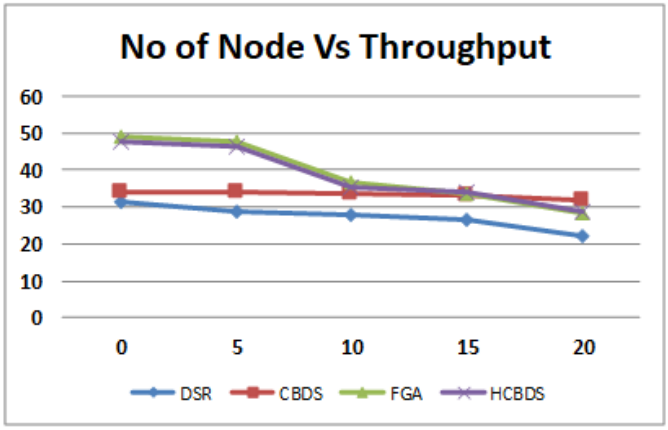


Figure 07: Performance analysis of Throughput using DSR, CBD, FGA & HCBD

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

VI. Conclusion:

Cooperative blackhole attack are known by numerous others to be the most damaging attacks against the Ad hoc network. While there are many methods for protecting Networks that are Ad hoc against such threats, there are significant shortcomings and some drawbacks to conventional preventive approaches in this regard. During the route discovery process, DSR often fails to delete nodes that are malicious and thus does not manage to send all data packets to the destination under Cooperative blackhole attack. Many of the conventional approaches lack sensitivity. In these attacks, the Packet Distribution Ratio or PDR can also decrease throughput as the number of nodes that are malicious increases.

Therefore, a new system HCBD has been suggested for protecting Networks that are Ad hoc.

In conclusion, Cooperative blackhole attack can be avoided as a result of our proposed mechanisms, and the demonstrated improvement in throughput and improved Packet Delivery Ratio is explicitly worthy of consideration. By observing the result, it is concluded that proposed HCBD system gives better performance as compare to FGA method in terms of packet delivery ratio and throughput.

References:

1. H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ‘‘VANet security challenges and solutions: A survey,’’ Veh. Commun., vol. 7, pp. 7–20, Jan. 2017.
2. I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani, ‘‘Overcoming the key challenges to establishing vehicular communication: Is SDN the answer,’’ IEEE Commun. Mag., vol. 55, no. 7, pp. 128–134, Jul. 2017.
3. I. Ahmad, R. M. Noor, I. Ali, M. Imran, and A. Vasilakos, ‘‘Characterizing the role of vehicular cloud computing in road traffic management,’’ Int. J. Distrib. Sensor Netw., vol. 13, no. 5, 2017, Art. no. 1550147717708728.
4. Muhammad saleem khan, daniele midi, majid iqbal khan, elisa bertino, “fine-grained analysis of packet loss in manets”, 2169-3536 2017 ieee.
5. I. Ahmad, U. Ashraf, and A. Ghafoor, ‘‘A comparative QoS survey of mobile ad hoc network routing protocols,’’ J. Chin. Inst. Eng., vol. 39, no. 5, pp. 585–592, 2016.
6. L. Li and G. Lee, ‘‘DDoS attack detection and wavelets,’’ Telecommun. Syst., vol. 28, nos. 3–4, pp. 435–451, 2005.
7. C. Buragohain, M. J. Kalita, S. Singh, and D. K. Bhattacharyya, ‘‘Anomaly based DDoS attack detection,’’ Int. J. Comput. Appl., vol. 123, no. 17, 2015.
8. S. S. Manvi and S. Tangade, ‘‘A survey on authentication schemes in VANETs for secured communication,’’ Veh. Commun., vol. 9, pp. 19–30, Jul. 2017.
9. Srinivasa Rao, Y., & Hussain, M. A. (2018). Dynamic MAC protocol to enhancing the quality of real time traffic in MANET using network load adaptation. Journal of Advanced Research in Dynamical and Control Systems, 10(7 Special Issue), 1612-1617.
10. Suma, P., & Hussain, M. A. (2018). Secure and effective random paths selection (SERPS) algorithm for security in MANETs. International Journal of Engineering and Technology(UAE), 7(2), 134-138. doi:10.14419/ijet.v7i2.8.10345.
11. A. Sinha and S. K. Mishra, ‘‘Preventing VANET from DOS & DDOS attack,’’ Int. J. Eng. Trends Technol., vol. 4, no. 10, pp. 4373–4376, 2013.
12. Boddu, N., Vatambeti, R., & Bobba, V. (2017). Achieving energy efficiency and increasing the network life time in MANET through fault tolerant multi-path routing. International Journal of Intelligent Engineering and Systems, 10(3), 166-172. doi:10.22266/ijies2017.0630.18.
13. Kolagani, P., Aditya, K., Venkatesh, N., & Kiran, K. V. D. (2017). Multi cross protocol with hybrid topography control for manets. Journal of Theoretical and Applied Information Technology, 95(3), 457-467.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

14. K. Verma and H. Hasbullah, ‘‘Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET,’’ Secur. Commun. Netw., vol. 8, pp. 864–878, Mar. 2015.
15. S. A. Ghorsad, P. P. Karde, V. M. Thakare, and R. V. Dharaskar, ‘‘DoS attack detection in vehicular ad-hoc network using malicious node detection algorithm,’’ Int. J. Electron., Commun. Soft Comput. Sci. Eng., vol. 3, p. 36, 2014.
16. Cynthia, C., Saguturu, P. K., Bandi, K., Magulluri, S., & Anusha, T. (2018). A survey on MANET protocols in wireless sensor networks. International Journal of Engineering and Technology(UAE), 7(2), 1-3. doi:10.14419/ijet.v7i2.31.13384.
17. Abdul, A. M., & Umar, S. (2017). Notification of data congestion intimation for IEEE 802.11 adhoc network with power save mode. Indonesian Journal of Electrical Engineering and Computer Science, 5(2), 317-320. doi:10.11591/ijeecs.v5.i2.pp317-320
18. X. Hong, D. Huang, M. Gerla, and Z. Cao, ‘‘SAT: Situation-aware trust architecture for vehicular networks,’’ in Proc. 3rd Int. Workshop Mobility Evolving Internet Archit., Aug. 2008, pp. 31–36.
19. J. Hortelano, J. C. Ruiz, and P. Manzoni, ‘‘Evaluating the usefulness of watchdogs for intrusion detection in VANETs,’’ in Proc. IEEE Int. Conf. Commun. Workshops, May 2010, pp. 1–5.
20. C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, ‘‘A trust model for vehicular network-based incident reports,’’ in Proc. IEEE 5th Int. Symp. Wireless Veh. Commun. (WiVeC), Jun. 2013, pp. 1–5.
21. Q. Ding, X. Li, M. Jiang, and X. Zhou, ‘‘Reputation-based trust model in vehicular Ad Hoc networks,’’ in Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP), Oct. 2010, pp. 1–6.
22. KRISHNA CHOWDARY*, K.V.V. SATYANARAYANA,“MALICIOUS NODE DETECTION AND RECONSTRUCTION OF NETWORK IN SENSOR ACTOR NETWORK”, Journal of Theoretical and Applied Information Technology 15th February 2017. Vol.95. No.3.
23. H. Hartenstein and L. P. Laberteaux, ‘‘A tutorial survey on vehicular ad hoc networks,’’ IEEE Commun. Mag., vol. 46, no. 6, pp. 164–171, Jun. 2008.
24. C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, ‘‘Secure and efficient trust opinion aggregation for vehicular ad-hoc networks,’’ in Proc. IEEE 72nd Veh. Technol. Conf.—Fall, Sep. 2010, pp. 1–5.
25. Y.-C. Wei and Y.-M. Chen, ‘‘An efficient trust management system for balancing the safety and location privacy in VANETs,’’ in Proc. IEEE 11th Int. Conf. Trust Secur. Privacy Comput. Commun., Jun. 2012, pp. 393–400.
26. Nagendram, S., Rao, K. R. H., & Bojja, P. (2017). A review on recent advances of routing protocols for development of manet. Journal of Advanced Research in Dynamical and Control Systems, 9(2 Special Issue), 114-122.
27. Suma, P., Nagaraju, O., & Hussain, M. A. (2017). Node disjoint random and optimal path selection (NDROPS) algorithm for security in MANETS. International Journal of Electrical and Computer Engineering, 7(3), 1197-1203. doi:10.11591/ijece.v7i3.pp1197-1203
28. T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, ‘‘A distributed advanced analytical trust model for VANETs,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2012, pp. 201–206.
29. R. R. Sahoo, R. Panda, D. K. Behera, and M. K. Naskar, ‘‘A trust based clustering with ant colony routing in VANET,’’ in Proc. 3rd Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), Jul. 2012, pp. 1–8.
30. Y. Chen and Y. Wei, ‘‘A beacon-based trust management system for enhancing user centric location privacy in VANETs,’’ J. Commun. Netw., vol. 15, no. 2, pp. 153–163, Apr. 2013.
31. B. Pooja, M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, ‘‘Mitigation of insider and outsider DoS attack against signature based authentication in VANETs,’’ in Proc. Asia–Pacific Conf. Comput. Aided Syst. Eng. (APCASE), 2014, pp. 152–157.
32. R. S. Raw, M. Kumar, and N. Singh, ‘‘Security challenges, issues and their solutions for VANET,’’ Int. J. Netw. Secur. Appl., vol. 5, no. 5, pp. 95–102, 2013.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

33. LSS Amudhavel, J., Satyanarayana, K.V.V., Kathavate, P., Reddy, "Energy aware routing protocol with QoS constraint in wireless multimedia sensor networks", January 2017 ,Journal of Advanced Research in Dynamical and Control Systems 9(12):1449-1457.
34. Gurung, S.; Chauhan, S. A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wirel. Netw, 1–11,2019
35. Rupali Sharma , "Gray-hole Attack in Mobile Ad-hoc Networks : A Survey ," International Journal of Computer Science and Information Technologies, Vol. 7 (3), 1457-1460 , 2016.
36. Rajesh Babu, M., and G. Usha , "A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET," Wireless Personal Communications: An International Journal 90.2, pp. 831-845, 2016.
37. Patil, S. U , "Gray hole attack detection in MANETs," 2nd International Conference for Convergence in Technology, I2CT 2017,https://doi.org/10.1109/I2CT.2017.8226087
38. Sachin Lalar , Arun Kumar Yadav , "Comparative Study of Routing Protocols in MANET ," ORIENTAL JOURNAL OF COMPUTER SCIENCE TECHNOLOGY, 2017
39. Khan, D. , Jamil, M, "Study of detecting and overcoming black hole attacks in MANET: A review ," International Symposium on Wireless Systems and Networks , 2017.
40. Natarajan, K. , Mahadevan, G, "Mobility based performance analysis of MANET routing protocols ," International Journal of Computer Applications , 2017.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731