International Journal of Future Generation Communication and Networking
Vol. 15, No. 1, (2022), pp. 100–118

Detection Of Cooperative Black Hole Attack In Mobile Ad Hoc Network (Manet) For Next Generation Network (Ipv6) Routing Protocol

Mr. Ganesh D. Dangat,
ganesh.dangat@kbpcoes.edu.in Research Scholar,
Sathyabama University

Dr.S. Murugan,
snmurugan@gmail.com
Sathya bama University, Chennai India

Abstract

In some settings, mobile ad-hoc networks (MANET) can be set up quickly and without much effort. Routing with sufficient powerful performance is one of the main issues in installing MANET, which is characterised by a dynamic change in topology. In cooperative black hole attacks, each node falsely claims to control a dependable path between the starting point and the final resting place. The proposed unique solution takes into consideration the IPV6, IEEE 802.11e protocol, and aims for findings connected to the exchange of MANETs-Reactive routing protocols. The enriched routing protocol has a positive impact on performance and efficiency, resulting in significant enhancements to the protocol's features. Proactive routing protocols such as Asymmetric Outer-Distance Vector (AODV), Distance-Sequential Vector (DSDV), and Destination-Sequenced Distance Vector (DSDV) were tested in both IPv4 and IPv6 networks and compared using the cooperative black hole attack with respect to a variety of performance indicators (RO). The outcome demonstrates the effectiveness of the novel strategy as a whole, with throughput increasing and end-to-end latency decreasing.

Keywords*:* Mobile Ad Hoc Networks (MANET), Routing Protocols, Blackhole Attacks, Internet Protocol Version 6, and Routing Protocols; New Methodology.

I. INTRODUCTION

Ad hoc wireless networks have amazing potential. The proliferation of mobile and wireless devices in the modern era has made this type of network and communication system the most dynamic of its kind. When multiple mobile devices,

such as smartphones, laptops, sensors, etc., are brought together, they form a network known as an ad hoc mobile network. Self-configuring and lacking a fixed infrastructure or predetermined topology, ad hoc wireless networks are made up of a large number of mobile devices or nodes that communicate with one another in real time. Physical security, bandwidth, energy, and other resources all have their limits; MANETs traverse wireless networks via multiple hops; and Internet connection links are dynamic. Modern ad hoc networks are reliable and fast because routing processing has been built into mobile devices, cutting down on routing overheads.

The military, emergency services, security systems, marketing from remote areas, fixed infrastructure replacement, and disaster mitigation are just some of the many fields that have found use

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

for MANETs. Finding the most direct route from source to sink for data packets is an important function of MANETS [1].

Figure 01: Architecture of Mobile Adhoc Network

Congestion can arise due to the limited bandwidth of MANETs; to solve this issue, mobile nodes must employ efficient routing techniques; consideration is given to the need for multiple Internet addressing protocols (IP) to meet the needs of the mobile nodes; and the ability to communicate without the support of any physical infrastructure.

Providing uninterrupted data pass-through devices and keeping the correct route constructed is the primary difficulty in building an IPv6 MANET. As a result, the nodes rely on their neighbours to swiftly and reliably route the packets to the target over the designated network, ensuring that no data is lost along the way [2]. Ad hoc networks, which are characterised by the mobility of their nodes and by practises of power control, are an amazing example of how connectivity can shift.

To transfer data, the reactive & proactive routing protocol builds a path from source to destination [3]. The reactive routing protocol employs a flooding-based approach to determining the best paths between two points. Once a route has been determined, it is saved and marked in the router's cache. This routing protocol's primary advantage is its lower bandwidth requirements in wireless Ad hoc networks. The algorithm under consideration, AODV, is a reactive routing protocol, where the path is generated only when it is needed [4].

1.1 IPV6:

One of the most recent IP versions, IPV6 is used by packet switches to facilitate the transport of datagrams between different network protocols. This communication protocol [5] lays the road by identifying and locating devices in the network. The Internet Engineering Task Force (IETF) created IPv6 to fix the problems with IPv4. To the greatest extent possible, IPv6 has supplanted IPv4. About 3.41038 addresses are used by IPv6, which is equivalent to a 128-bit address (2128). But in reality, there are fewer because several ranges are set aside for special purposes [6].

As a practical matter, IPv6 employs 32-bit addresses. 7.91028 greater than IPv4, or 4.3 billion unique addresses. Security in networks is an essential part of the IPv6 architecture. Unicast, anycast, and multicast are the three forms of communication supported by the IPV6 addressing scheme as specified in RFC 4291 [7]. Each field of an IPV6 address is 16 bits in length, for a total of 128 bits. This data is represented by four hexadecimal digits.

1.2 IEEE802.11E

By incorporating improvements at the MAC (Media Access Control) layer, the primary goal of IEEE802.11e is to account for the unique priority characteristics of wireless LANs as QoS (Quality of Service). The importance of delay-sensitive applications has been elevated as a result of this standard [9].

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

For the purpose of defining Traffic Categories [11], the IEEE 802.11e MAC protocol uses HCF-Hybrid Coordination Function [10], which is made up of the two approaches EDCA-Enhanced Distributed Channel Access and HCCA-Hybrid Controlled Channel Access.

In EDCA, traffic is divided into high- and low-priority streams, with the former having higher odds of being handled before the latter [12]. Contention-free access for the TXOP (Transmit Opportunity) time is encouraged by establishing a contention window in accordance with the anticipated traffic in each AC, and this is represented by the ACs (Access Categories) [13].

When implementing EDCA at the MAC Layer, four distinct types of network access are taken into account. The priority-id of the data packets transferred down from the higher layers is used to determine which auxiliary circuit should be used. Different application classes are assigned to individual A/Cs in the identified table. To further improve QoS, the EDCA-enhanced WLAN also allows for priority-based services to be used [14]. The implementation of prioritised QoS followed the creation of distinct types of network access.

A conwin min, A conwin max values[10], which are present in every physical layer that supports standard 802.11e [15], are used to derive one of the two fields from access categories, conwin min and conwin max values.

Defined QoS performs an accurate evaluation of both high- and low-priority traffic. Furthermore, there may be cases where data must be protected from all other sources of data in the same category. This is dealt with in EDCA through Admission Control [16].

The access point broadcasts beacons that indicate the bandwidth that is currently available. Customers should verify their bandwidth availability before adding to the current volume of traffic. The certified APs must be activated for EDCA and TXOP to work as intended. These stated enhancements are thought of as major, whereas other enhancements of IEEE802.11e are thought of as optional [16].

The new power save deliver and notification (APSD) technique [10] improves upon the Power Save Polling technique that has been present in earlier IEEE 802.11 standards. Reduced power consumption is achieved by this approach because it reduces the amount of signaling traffic and the frequency of collisions between power-saving polls [17].

1.3 Type of Security Attacks

Congestion, the spread of false routing information, and the disruption of nodes' ability to provide services are all outcomes of external attacks. Internal attacks, in which the attacker seeks to gain persistent access to the network and participate in its activities, can be carried out in one of two ways: either by the attacker posing as a legitimate node on the network in order to gain access to the web or by the attacker compromising an existing node and using it as a springboard from which to launch malicious activities [18]. Passive attacks and active attacks are the two main types of VANET security threats. Active attacks are further classified by their layer [19].

Passive Attacks

A passive attack does not disrupt the regular operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is challenging since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use a powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get helpful information from the data overhead [19].

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

Eavesdropping

In a passive attack, the attacker merely monitors the information flowing over the network without interfering with its normal functioning. In this case, confidentiality is broken. Passive attacks are difficult to detect because they do not interfere with normal network functioning. The implementation of a strong encryption technique to encrypt the sent data is one solution to the problem [19]. This would prevent the attacker from gleaning any useful information from the data overhead.

Traffic Analysis & Monitoring

An adversary conducting a traffic analysis attack would listen in on a network's packet traffic in order to deduce useful information, such as the packet's origin, final destination, and the two entities involved in the transmission.

Active Attacks

An active attack is one that actively works to corrupt or delete the information flowing through the network. Active attacks might come from the inside or the outside. When a network is attacked, it can be from the outside, by nodes that aren't even part of the web, or from within, by compromised nodes. Internal attacks are more damaging and difficult to detect than external attacks because the attacker is already inside the network. Active attacks include impersonation, modification, fabrication, and replication, and can be carried out by a third-party advisory or a compromised node within the network.

MAC LAYER ATTACKS

Jamming attack

Attacks using jamming techniques fall under the category of denial of service. Jamming devices are intended to disrupt lawful wireless communication. Either by blocking the transmission of packets from a legitimate source of traffic or by preventing the reception of such packets, a jammer can achieve this goal.

NETWORK LAYER ATTACKS

Wormhole attack

An adversary captures data packets from one part of the network and sends them over a secret tunnel to another. A wormhole is a tunnel between two conspiring attackers that can interrupt routing by transmitting routing control messages. It's important to remember that wormhole attacks pose a significant risk to routing protocols in VANETs. If an on-demand routing protocol like DSR or AODV were attacked with a wormhole attack, for instance, the attack could prevent the discovery of any routes other than the one leading through the wormhole.

Blackhole attack

There are two characteristics of the Blackhole assault. As a first step, the node uses a mobile ad hoc routing protocol like AODV to falsely claim to have a path to the destination node in order to steal data. Second, instead of transmitting the packets, the attacker swallows them. It is possible, though, that nearby nodes will keep tabs on the attacks and reveal their existence to the attacker. The more sophisticated variety of these attacks involves the selective forwarding of packets. If an attacker alters or drops packets coming from specific nodes but leaves data coming from other nodes unchanged, it is harder to determine which nodes are being targeted.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

A strike from Byzantium

Degradation or disruption of routing services can occur when a single compromised intermediate node acts alone or when multiple compromised intermediate nodes cooperate together to launch attacks such introducing routing loops, sending packets down suboptimal paths, or discarding messages arbitrarily.

Assaults on Routers

Many different kinds of attacks can be launched against the routing protocol, each with the express purpose of making the network unstable. Below is a quick overview of some attacks that can be made against the routing protocol:

The first kind of attack is called a "routing table overflow," and it consists of the attacker setting up connections to hosts that do not exist. In order to stop new routes from being created or to overwhelm the protocol implementation, it is necessary to generate a sufficient number of possible ways to do so. In contrast to reactive algorithms, which only generate a route when one is actually needed, proactive ones actively seek out this information in advance. An adversary can flood a network's routers with route ads if they're not careful. As opposed to proactive protocols, reactive ones don't bother with routing information in the first place.

The second type of attack is known as "routing table poisoning," and it involves compromised nodes in a network either sending fake routing updates or tampering with actual route update packets sent to other, uncompromised nodes. Sub-optimal routing, network congestion, and inaccessible web components are all possible outcomes of poisoning the routing table.

Thirdly, a malicious node may attempt to spread outdated information by copying and redistributing packets. This wastes the nodes' resources, including bandwidth and battery life, and muddles the routing process [21].

Poisoning of the route cache is a problem for on-demand routing protocols (like the AODV protocol [11]) since every node keeps a copy of the routes it has learned about recently. Identical to routing table poisoning, an attacker can similarly poison the route cache to achieve similar aims.

Five, the Rushing Attack is a threat to on-demand routing algorithms that rely on duplicate suppression in their path discovery procedures. Before other nodes in the network can respond to a Route Request packet, an adversarial node that has received one from the source node will rapidly broadcast it across the network. When a node receives a genuine Route Request packet, it may mistake it for a duplicate of a packet it has already received via an adversarial node and so delete it. The adversary node would always be included in any path found by the source node. As a result, the origin node would be unable to locate optimal paths (paths that do not pass through the hostile node). However, in ad hoc wireless networks, it is difficult to identify such attacks.

Resource consumption attack

The sleep-deprivation attack describes this phenomenon. An attacker or compromised node may try to drain a victim's power supply by initiating excessive route discovery requests or sending unnecessary packets to the victim node [22].

IP Spoofing attack

In conflict-detection allocation, the new node selects an arbitrary address, say y, and sends out a message to the entire VANET. If a node objects, it will be unable to use that address. If the malicious node always

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

responds with vetoes as if it were a member that has used the same IP address, then it is likely to be that node.

State Pollution attack

The state pollution attack occurs when a malicious node responds with incorrect parameters. If the new node is given an already-in-use address during best-effort allocation, the VANET will repeatedly broadcast Duplication Address Detection messages, leading to the rejection of the new node.

Sybil attack

Sybil attacks happen when one rogue node pretends to be multiple other nodes that don't exist. All auto-configuration methods and secure allocation techniques based on the trust model are vulnerable to this attack, which targets network services when cooperation is required. Sybil attacks, however, cannot be stopped in any realistic way. [23].

Fabrication

Malicious nodes can wreak havoc by either tampering with or disrupting normal network packet routing, or by creating their own fake packets to send via the network. Message fabrication attacks, like sleep deprivation attacks, could be launched by inserting large packets into networks. It's important to note that route salvaging attacks, for example, can be the result of malfunctioning nodes within the network rather than external actors.

Modification

By tampering with routing messages, an attacker can compromise network packets in a message modification attack. Due to the dynamic nature of ad hoc networks, where nodes are free to roam and self-organize, it is possible for malicious nodes to become embedded in the networks' social fabric. It's possible that these hostile nodes could use the weakened connections in the network to take part in the packet forwarding process and then execute the message modification assaults. Packet rerouting and impersonation are two kind of assault that can be categorised as message alteration attacks.

STRIKES AGAINST TRANSPORTATION LAYERS

Concurrent session hijacking attacks

Most communications are secured (by giving credentials) during session setup but are not thereafter, which is exploited in session hijacking. The attacker in a TCP session hijacking attack pretends to be the victim's IP address so that they can learn the correct sequence number the target is expecting and launch a denial-of-service assault against them. This allows the attacker to continue the session with the target as if they were the victim node [24].

An assault with YN flooding

SYN flooding is a denial-of-service attack. The attacker initiates many TCP connections with the victim node but never finishes the handshake, leaving the connection open and vulnerable.

ATTACKS ON THE APPLICATION LAYER

Contradiction assault

Firewalls can be set up in the network layer to allow or deny access to data packets. End-to-end encryption of actual connections is possible at the transport layer. Unfortunately, neither the

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

authentication nor the non-repudiation issues are addressed by these alternatives. The term "repudiation" describes a refusal to acknowledge any responsibility for the messages. The classic form of repudiation attack on a commercial system would be for an individual to refuse to authorise a financial transaction, such as a credit card purchase or an online bank transfer.

II. RELATED WORK

The following section explains the overall structure and function of the current project.

Aarushi and company. An incredibly fast solution for preventing attacks from being made via black hole nodes was proposed in [1]. When a malicious node transmits a Hello message, no one will hear it. The authors propose a variety of methods for detecting and stopping dark hole attacks in MANET, but each one has its own set of caveats and widely accepted safeguards. The primary security issue that can affect the presentation of the AODV routing convention is a pernicious node. Except for average packet delivery rate and average start-to-finish time, every metric has significantly improved, despite the fact that these two metrics have increased in size due to the overhead of a critical component. The hope is that through this development, we can better estimate these factors.

In order to locate and escape the Black hole attack in Mobile Ad Hoc Networks, Abdelhakim et al. [3] suggested a useful approach. An implementation of the AODV (Ad hoc on Demand Distance Vector) Routing protocol is used for the calculation. Both a lone Black hole assault and a combined one are recognised by the calculation. The brilliance of the current calculation described is that it can differentiate the Black hole nodes even if the node is idle, in addition to identifying the black hole attacked nodes.

Using encryption, Akyildiz et al.[5] proposed the Encryption Verification Method (EVM) technology, which may successfully identify a large number of dark hole nodes. The confirmation method is initiated in a limited manner and verifies the succession number to ensure it was not spoofed by a malicious node. The simulation proves the EVM reduces control overhead and accurately identifies the malicious node. In the future, this formula can be expanded to provide an explanation for a targeted sending assault, such as a black hole assault.

Ayday et al. [6] offered a calculation that made use of the trust value that is used to identify the malignant node; once the malicious node has been identified, it will be removed from the nearby table and we will choose an alternative path. With the help of the suggested algorithm, it is possible to provide a secure transmission link between any pair of nodes in a network. Authors advocate for a new AODV convention and justify the setup with examples of its use in practise and in games built with NS-2.33. This upgrade analysis demonstrates the significant boost in end-to-end delay, throughput, and packet delivery rate of AODV in the neighbourhood of Black hole attack.

Black hole attacks in the AODV routing convention were addressed by Karma et al. [8] who offered a method to avoid them by employing the Triangular Encryption Method in the NS2 Simulator. Given its small impact on performance, Triangular Encryption was chosen. When compared to other methods of black hole identification, the proposed method is shown to be more effective. The suggested solution was limited in that it could not identify or remove Black Hole nodes, only avoid their behaviour. As the number of nodes grows, the implementation becomes noticeably sluggish. Network burden increases because the amount of data packets sent is significantly more than in the initial AODV convention.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

A method based on node verification and advanced mark was proposed by Khosravi et al.[9] to ensure the safety of the system's data transmissions. Although methods used in the past to identify potentially harmful nodes are discussed, there is currently no way to ensure a new node is safe before it is integrated into the system. With the help of AES and other cutting-edge cryptographic techniques, this new configuration of the convention ensures honesty, privacy, non-renunciation, and verification. Validation of nodes is achieved via their unique IP addresses. Modern cryptographic procedures were developed using RSA and the hash function MD-5. The SMDNA (Securing MANET Data employing Node Authentication) security mechanism enhances the presentation of the AODV routing protocol.

For the purpose of locating and foreseeing dark hole attacks on MANETs, Mishra et al.[16] provide a grouping strategy in the Ad-hoc Onrequest Distance Vector (AODV) routing standard. Now, someone in the group will ping the cluster's master node once to highlight the striking discrepancy between that node's incoming and outgoing data loads. If something strange is detected, all of the nodes will go black to remove the malicious ones. The results of the simulation confirm that the grouoing strategy is responsible for the complete transmission of data packets, even while passing close to a large number of black hole nodes. Both identification speed and throughput have seen significant increases, respectively.

Dark hole attacks are handled by Mislove et al.[17], who also developed a start-to-finish affirmation based mechanism to ensure that intermediary nodes are providing data correctly. The suggested method not only recognises the modification and reiteration of message attacks, but also the black hole that is being either directly or indirectly addressed. It demonstrates the effectiveness of the proposed approach in both proactive and responsive direction based systems with respect to delay from beginning to end and system load through a reproduction using the OPNET test system. The method is compared to two other popular ones, 2-bounce ACK and the watch dog approach, and evaluated based on their discovery rate, their transmission rate, and the amount of extra work they require. In order to identify and isolate hostile nodes via the routing layer data, the Trust Based Cross-Layer Security Protocol organises a trust based data packet sending strategy. To facilitate the transfer of data packets, it employs trust values and keeps a trust counter for each node. If the trust value drops below a predetermined threshold, the associated intermediate node is marked as malicious [24]. The cross-layer security convention achieves low delay and overhead [25] while maintaining a high packet delivery rate percentage. Best-exertion deficiency tolerant routing was used to finish MANET routing, and the authors looked into how well their predicted framework worked in practise with regards to both packet delivery speed and routing overhead.

Identifying malicious nodes in MANET was proposed by Mohaisen et al. [18] using a heterogeneous approach. For this calculation, it was necessary to establish links between nodes that could be trusted and those that could not. In this case, we were able to identify the cyclical nature of data packet loss and conclude the presentation on the basis of the percentage of lost data. For the purpose of identifying and eliminating the rogue nodes in MANET, it employed a route foundation approach and data packet sending calculation.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

Table 01: Issue-wise Major Solution Approaches

Approach/ Technique Used	Problem solved
Security Issues	
Compressed AH & ESP for 6LoWPAN	Successful secure integration of IPv6 WSN with the internet.
Policy Based Security	Policy Based Security Management (PBSM) new theoritical approach to allow the secure deployment of the host based security (HBS) system
Simple Secure Addressing Scheme (SSAS)	Sucessfully provided privacy & security by randomizing the IID, adding SSAS signature, using RPKI and binding between the publickey and IP address
Secure address Validation Improvements (SAVI)	System protected from address resolution attacks by checking NS &NA messages coming from validating ports.
i-SeRP risk assessment system	Developed tool useful for assessment of the IPv6 network security risks
Online Forensic tool (6Foren)	6Foren system sucessfully recorded attack event replays in Attack Event Database
• **Addressing Issue**	
Micro Sensor Routing Protocol	carried out performance comparisons on Packet Delivery Ratio, Average End to end Delay and Routing Overhead and MSRP has better performance compared to AODV.
Escort Tunneling Protocol	Escort protocol analyzed on the basis of packet processing latency and it was around 6us ~ 10us along with more security, sportedmobility and multi-homing with capability of traversing symmetric NATs.
Auto-configuration Implementation in LoWPAN	Theoretically reduced the header size and decreased thecommunication and save nodes energy to extend the average life time of the entire network.
Error Detection Issue	
CRC based Packet Recovery Mechanism for Wireless Network	System reduced computation and resource consumption for CRC based Packet Recovery
• **Network Optimization issues**	
Memory Management system in 6LoWPAN	Buffer Overflow memory problem was successfully resolved in Wireless Sensor Networks
IPv6 based Database Retrieval Systemfor Wireless Sensor Networks	It provided the concept for the research to implement databaseretrieval system in the Wireless Sensor Networks.

Outcome of survey in IPv6 Addressing:

- - The authors of 6LoWPAN added support for Dual Stack Networks and IPv6 Address Auto-configuration.
- -

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

- Microsensor routing, an escort tunnelling system, fragment and header size optimization for local area networks, mobile routing, and a proxy were just some of the methods created by the research community. [27].
-
- Tools for testing network performance, preventing IPSec gateway failure, and using Mobile IPv6 for network mobility.
- While some strategies did use real-world test environments for evaluation of solution performance, the vast majority relied on network simulators [28].
- Auto-configuration, security during dual stack, security holes, and techniques like routing, NAT, CGA, SEND, MAC, and multicasting are only a few of the IPv6 addressing topics covered in the aforementioned works of research.

The outcome of survey in Error Detection:

- CRC-based packet recovery mechanism for wireless networks, CRC checking at the Network Layer to reduce link layer processing overheads, and a comparative analysis of various error detection and correction approaches were all proposed to cut down on processing time in high-speed data transfer [28].
- Many of the proposed algorithms were tested on simulators, while others were tested on a Gigabit Ethernet network.
- Having CRC testing done at the network layer instead of the link layer improved link layer speed by lowering processing overheads.
- It's important to test CRC checking algorithms in a real-world network setting, as they can be tailored to fit different architectures [29].

III. PROBLEM STATEMENT

In particular, MANETs necessitate strong adaptability to various scenarios and minimal latency for various uses. It must then be reconstructed in order to subvert the established network architecture and facilitate easier hardware operation. When it comes to the safety of MANETs, individual nodes in the network can be easily captured, hacked, and communicated with by malicious actors; additionally, messages sent and received by individual nodes may have been eavesdropped upon, and malicious actors may have introduced or replayed false messages into the network. To achieve their goal of disrupting the normal functioning of the network, malicious nodes actively interfere with its normal daily activities. The implementation of MANETs would be significantly hampered by these problems. For this reason, MANET's defence has a more difficult duty [30].

The poor performance of wireless networks between nodes and the lack of a source-destination connection are two examples of such problems. As a result, MANET must be extremely adaptable so that it can deal with any circumstance.

There are, however, still a number of obstacles that need fixing. Here are just a few examples,

- **Performance & Flexibility**
- **Scalability**
- **Interoperability**

Security in a MANET needs to be ensured while minimizing overhead as much as feasible because the network is composed of diverse devices, some of which may have limited resources.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

IV. PROPOSED APPROACH

A climate sensor node picks up data and passes it along, either directly or indirectly via other nodes. The sensor nodes are bundled in several sensor implementations to provide for adaptability, uniformity, and reduced stream [31].

A large number of sensor nodes are being dispatched. Direct communication between nodes and the hub is impossible. The sensor node itself is tacked onto the group's top, isolating the node from the rest of the network. The leader of a bunch collects data and sends it to the sink's central hub. Integrating into the organisation requires a deep understanding of topics like network life and power. In this article, we use a hybrid cluster-based approach to achieve the highest throughput possible. Some of the specifics of our unconventional method are as follows.

The following are some of the most crucial components of the cluster approach:

a) Belonging to a cluster.

In a nutshell,

b) the brains of a cluster.

c) The hub node

d) Connection within the cluster.

e) Connectivity between clusters.

4.1 Architecture

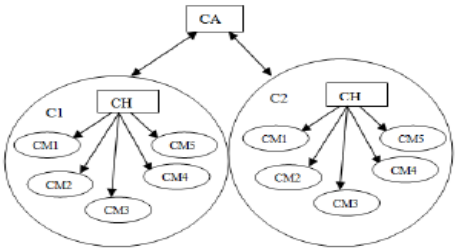


Figure 02: Clustered Architecture

For a visual representation of the network's structure, see figure. C1 and C2 are examples of clusters, and they, along with the CA, the CH, and the CM1 and CM2 members, make up the certification authority.

The following schematic outlines how the innovative method operates,

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

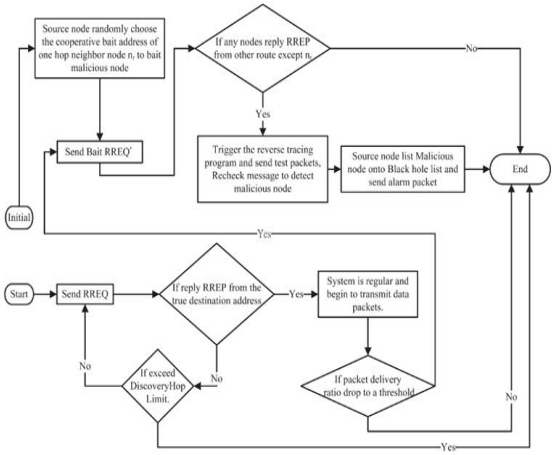


Figure 03: Flow of novel approach

As can be seen in the illustration, the route discovery process begins with the source node S sending out RREQ messages to its neighbouring nodes. The incoming RREP was validated to ensure it originated from the correct node D. Once a path is identified, data transmission can commence. When a new time period begins, the PDR is recalculated and compared to the dynamic threshold value. A new RREQ type, Bait RREQ', is transmitted from the source node if the PDR drops below a certain level; if the RREP is received from a node other than the current route, the system does a reverse tracing operation to identify the partially malevolent node. In the second stage, after a malicious node has been partially identified, additional parameters, such as mobility and congestion, are extracted to undertake a more in-depth study of the node [30]. The fine-grained analysis estimates the root cause of packet losses based on the retrieved parameters. In the event that the results of the partial detection and fine grained analysis are consistent, the node in question is added to the list of attackers and an alarm packet is sent to the other nodes. If any further causes of packet losses are found, the current route is discarded and a new one is discovered with the exception of the node that was just tagged as unstable. The results of the fine-grained analyses are used to regularly update the list of unstable nodes. Because of the high mobility and congestion in the network, these methods not only increase the detection rate, but also minimise packet drops and excessive overhead.

4.2 Methodology

We use a weighted clustering technique that combines CM and CH to group nodes into meaningful groups. In order to establish trust across network nodes, CH must first verify each node's certificate using the public key it obtained from CA. If the certificate of a node cannot be verified by the CH, that node is flagged as a bad actor and the CA is notified to revoke its certificate [31].

4.3 Algorithm:

Assumptions:
CA=Certifying authority
CH= Cluster Head
WL= Warned List
BL= Blocked List
NN = Number of Nodes

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

SNi = Specific Node,
SCk = Specific Cluster,
MAX = Number of maximum nodes per cluster,
PD = Packet Data,
NBi = Buffer of Specific Node,
SNTCi = Specific node's trust counter (Initially set to 0 for each node),
SNTSi = Specific node's trust status (Initially set to 'F' for each node)
TV = Threshold Value (Set default is 0.8)
k = Used for Cluster Number
count = Used to count number of nodes in cluster

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

```
Initialize
k = 0
count = 0
Step 1: Cluster formation

for i = 1 to NN
{
Find out degree of each node ();
Find out power status of each node ();
}
while (making cluster by putting every node in to
any one cluster)
  {
  if (SNi = = max (degree of node and power
status of node))
        {
          Add SNi into SCi
          Set count = count +1
        }
  if (count > MAX)
        {
          k++
          Set count =0
        }
   }

Step 2: Detection of suspected nodes

while (SNTCi < TV)
{
   if ( SNi sends accusation message against
node M = True)
      {
        CA updates WL and BL
      }
   else
      {
       CH sends recovery packet to CA
       CA broadcast this information
       SNTCi = SNTCi + 0.2
      }
Step 3: Process for suspected nodes
Send Testing packet data RREQ to the node with
TTL=1
if (receives response)
  {
    if (SNTCi  < TV )
         Set SNTSi as 'F'
  }
else
    {
    Set SNTSi as 'D'
    Go to step 4
  }
Step 4: Detection of false accusation ();
Step 5: Send accusation message for time t
```

The cluster-based network can be protected in the ways described below.

Creating Certificates

2. Clustering

Identifying Network Nodes

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

4. Identifying the offending node
5. Recognizing a false accusation when it occurs.
Sixth, maximising efficiency under constrained conditions.
When nodes from different clusters try to have a conversation with one another, misunderstandings and even false accusations can occur. If a valid node in one cluster sends a communication request to the CM in another cluster, the node that receives the request notifies its CH. Afterward, CH verifies in its buffer whether or not the node's certificate is present, and if it isn't, it sends a blocking message to CA [31]. This data is used by CA to add the node to the BL and then broadcast that change throughout the network. If the CH of the accused node receives a blocking message from CA, the CA will be notified and the node will be unblocked [32].

4.4 Advantages of Clustering

One, it helps businesses adapt and save money by reducing their energy use and the amount of data they collect.
Second, it can consolidate the group's routing structure within itself, reducing the need for as large of a routing table to be stored at the node.
3. It conserves communication transmission capacity by reducing the distance between clusters linked through the cluster leader.
4. it prevents the unnecessary relaying of information between sensor nodes. [33].

V. PERFORMANCE METRICS

Our parameters for measuring the success of the suggested approach are as follows:

Normalized Transportation Via the Sky

The total number of routing control messages in k bit/s, including RREQ, RREP, RRER, HELLO, etc.

Flying Packet

This is the proportion of data packets received in the simulation compared to control packets sent [34].

Transmission Success Rate

It is the proportion of packets sent from the "application layer" CBR sources to those received by the "application layer" CBR sink at the destination.

The Typical Delay From Start To Finish Is:

How long, on average, it takes for a CBR source to deliver a data packet and for that packet to be received by a CBR sink. All the time it takes to find a new route, have it buffered and processed by intermediate nodes, have it retransmitted by the MAC layer, etc., all count toward this total. In this case, milliseconds [35] are used as the unit of measurement.

VI. Simulation Result

With the reactive and proactive systems' strengths in mind, a DSR-based routing scheme capable of detecting grey hole/collaborative black hole assaults in MANETs has been presented. According to, the proposed approach outperformed both proactive and reactive security methods, but only using the PDR parameter to label a node as malicious raised concerns about the accuracy of their detections. In this approach, a rogue node is tracked down via a reverse tracing algorithm [12] if the PDR falls below a predetermined level. However, in MANET, packet losses can occur for a number of reasons, therefore it's

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

important to double-check their accuracy before labelling a node as malicious. The following paragraph provides a comprehensive summary of the results of the simulation,

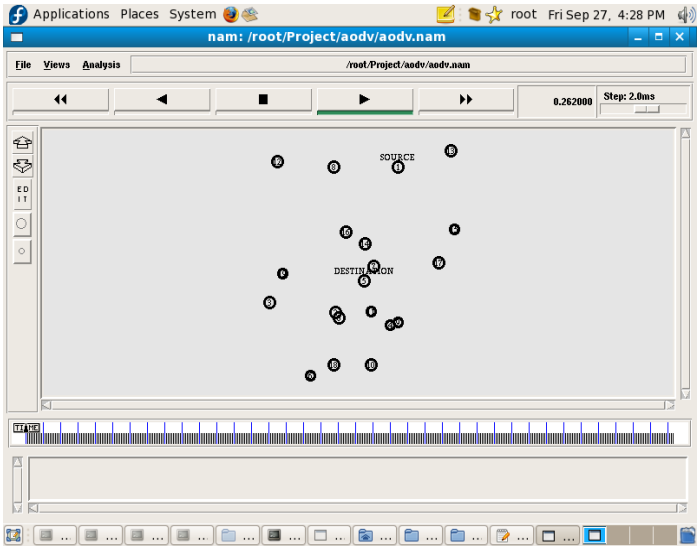


Figure 04: Propagation model of Simple 20 node.

By repurposing routing packets already in use, our suggested solution does not increase the total number of messages sent. This includes messages about queue and connection status (already required according to routing Protocol standards). Furthermore, as demonstrated in the below image, the data channel continues to relay genuine malicious nodes while incurring little energy costs.

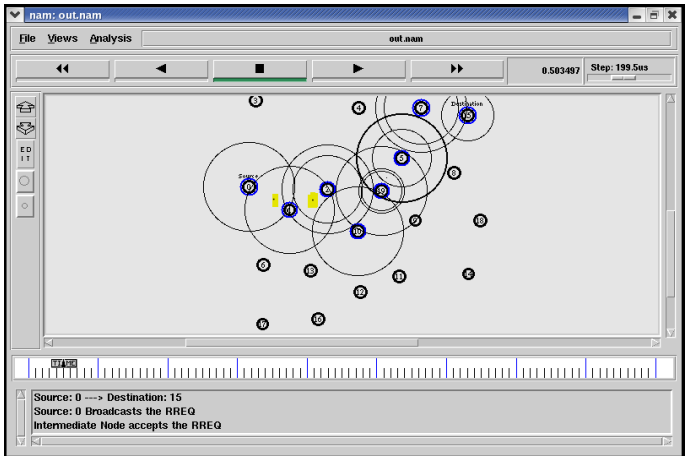
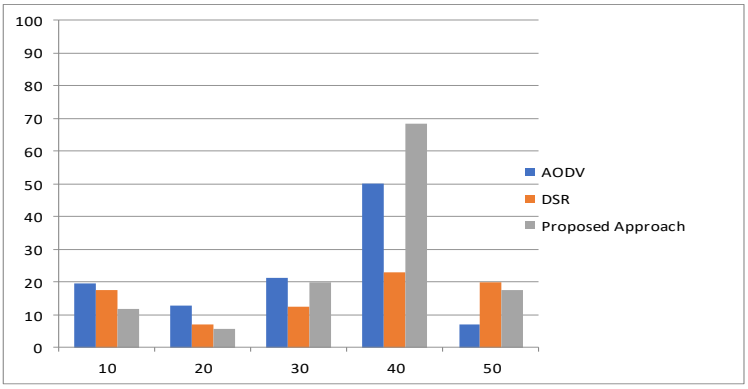


Figure 05: Source Broadcast the Route Request for sharing data.

Increasing numbers of malicious nodes in Graph 01 demonstrate that the proposed PDR system outperforms the state of the art. In all cases, the Proposed Routing Protocol results in less data loss as a percentage than DSR and AODV.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC



Graph 01: Comparison of PDR Delay of AODV, DSR & Proposed Approach.

The above study found that the Proposed cluster-based Approach outperforms competing protocols and accurately identifies attacks.

VII. CONCLUSION

There is a growing need for academics to find ways to protect mobile networks from cyber-attacks as the technology behind them evolves. In the studies conducted, it was shown that when the number of jamming nodes was increased while the time between messages was decreased, the network became jammed and the receiving node lost messages from benign hosts. DDoS, eavesdropping, Man in the Middle, and cooperative black hole assaults are the most popular forms of cyber-attack. Using the proposed cluster-based technique, we demonstrated an experiment with a combined black hole assault designed to jam the communication channel in a MANET network. The long-term strategy involves adopting IPV6, which will foil such attacks in the future and ensure top throughput.

REFERENCES

1. Aarushi, A & Bedi, H 2014, 'Modified AODV for Detection and Recovery of Worm Hole Attack', International Journal Of Engineering And Computer Science, vol. 3, no. 10, pp. 8498-8501.
2. Aashima, G & Kumar, P 2012, 'Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review', International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 5.
3. Abdelhakim, M, Lightfoot, LE, Ren, J & Li, T 2014, 'Distributed detection in mobile access wireless sensor networks under byzantine attacks', IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 950– 959.
4. Adya, A, Bahl, P, Padhye, J, Wolman, A & Zhou, L 2004, 'A multiradio unification protocol for IEEE 802.11 wireless networks', In Broadband Networks, BroadNets Proceedings, First IEEE International Conference on, pp. 344-354.
5. Akyildiz, IF, Lee, WY & Chowdhury, KR 2009, 'CRAHNs: Cognitive radio ad hoc networks, AD hoc networks, vol. 7, no. 5, pp. 810-836.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

6. Ayday, E, Lee, H & Fekri, F 2010, 'Trust Management and Adversary Detection for Delay-Tolerant Networks', Proc. Military Comm. Conf. Milcom '10.
7. Barreto, J & Ferreira, P 2004, 'A replicated file system for resource constrained mobile devices', In Proceedings of IADIS International Conference on Applied Computing, pp. 1-9.
8. Karma, A & Choudhary, J 2014, 'MPLI: a novel modified parametric location identification for AODV in MANET', International Journal of Computer Applications, vol. 100, no.4, pp. 48–53.
9. Khosravi, H, Azmi, R & Sharghi, M 2016, 'Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks', International Journal of Future Computer and Communication, vol. 5, no. 2.
10. Ko, YB & Vaidya, NH 2000, 'Location-Aided Routing (LAR) in mobile ad hoc networks. Wireless networks', vol.6, no. 4, pp. 307-321.
11. Li, J, Halder, B, Stoica, P & Viberg, M 1995, 'Computationally efficient angle estimation for signals with known waveforms,' IEEE Transactions on Signal Processing, vol. 43, no. 9, pp. 2154–2163.
12. Li, J, Li, R & Kato, J 2008, 'Future Trust Management Framework for Mobile Ad Hoc Networks', IEEE Communications Magazine on Security in Mobile Ad Hoc Networks, vol. 46, no. 4, pp. 108-114.
13. Li, X, Jia, Z, Luguang, W & Wang, H 2010, 'Trust-based Ondemand Multipath Routing in Mobile Ad Hoc Networks', IET Information Security, vol. 4, no. 4.
14. Liu, W & Yu, M 2014, 'AASR: authenticated anonymous secure routing for MANETs in adversarial environments', IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585–4593.
15. Meka, K, Virendra, M & Upadhyaya, S 2006, 'Trust based routing decisions in mobile ad-hoc networks', In Proceedings of the Workshop on Secure Knowledge Management.
16. Mishra, A, Nadkarni, K & Patcha, A 2004, 'Intrusion detection in wireless ad hoc networks, Wireless Communications, IEEE, vol. 11, no. 1,pp. 48-60.
17. Mislove, A, Post, A, Gummadi, K & Druschel, P 2008, 'Ostra: Leveraging Trust to Thwart Unwanted Communication', Proc. of USENIX NSDI, pp. 15-30.
18. Mohaisen, A, Hopper, N & Kim, Y 2011, "Keep your Friends Close: Incorporating Trust into Social Network-based Sybil Defenses', Proc. of IEEE INFOCOM, pp. 1-9.
19. Sathish M, Arumugam K, S.NeelavathyPari, Harikrishnan V S,Detection of Single and Collaborative Black Hole Attack in MANET.Paper presented at IEEE WiSPNET 2016 conference.
20. Praveena, A., & Smys, S. (2017, January). Prevention of inference attacks for private information in social networking sites. In 2017 International Conference on Inventive Systems and Control (ICISC) (pp. 1-7). IEEE.
21. Verma, S. S., Patel, R., Lenka, S. K. ,Analysing varying rate food attack on real flow in. International Journal of Information and Communication Technology, 10, 276–286,2017
22. T. Jamal, SA Butt, "Malicious node analysis in MANETS", International Journal of Information Technology, 2018
23. Raj, J. S. Qos optimization of energy-efficient routing in IoT wireless sensor networks. Journal of ISMAC, 1(01), 12-23,2019.
24. Kumar, A. Dinesh, and S. Says.;An energy-efficient and secure data forwarding scheme for wireless body sensor network.;International Journal of Networking and Virtual Organisations 21, no. 2 : 163- 186,2019.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC

25. Yasin and M. Abu Zant, "Detecting and Isolating Blackhole Attacks in MANET Using Timer Based Baited Technique," Wireless Communications and Mobile Computing, vol. 2018, 2018
26. Zardari, ZA, He, J, Zhu, N, et al. A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. Fut Internet Vol 3(11) 2019
27. Gurung, S.; Chauhan, S. A dynamic threshold-based algorithm for improving security and performance of AODV under blackhole attack in MANET. Wirel. Netw, 1–11,2019
28. 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.
29. 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.
30. 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
31. Sachin Lalar , Arun Kumar Yadav , "Comparative Study of Routing Protocols in MANET ," ORIENTAL JOURNAL OF COMPUTER SCIENCE TECHNOLOGY, 2017
32. Khan, D. , Jamil, M, "Study of detecting and overcoming black hole attacks in MANET: A review ," International Symposium on Wireless Systems and Networks , 2017.
33. Natarajan, K. , Mahadevan, G, "Mobility based performance analysis of MANET routing protocols ," International Journal of Computer Applications , 2017.
34. Vikash Kumar , "Prevention of Black Hole Attacks in MANETs ," International Journal of Engineering Trends and Technology (IJETT) – Volume 61 Number 3, pp. 166-170, July2018.
35. J. Manoranjini, A. Chandrasekar S. Jothi , "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework," Automatika, 60:3, pp.274-284 , January 2019 , DOI: 10.1080/00051144.2019.1576965.

ISSN: 2233-7857IJFGCN
Copyright ⓒ2022SERSC