Performance Enhancement and Mitigation of Black Hole Attack in MANET using CRN and Enhanced AODV

Natasha
Research Scholar at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

Preety Chaudhary
Assistant Professor at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

Rakesh Kumar
Assistant Professor at department of Computer Science &Engg.
Sachdeva Engg. College for Girls, Gharuan

ABSTRACT
MANET is field of networking that is used to transmit information. MANET utilizes different routing strategies for data transmission from source to destination. Mobility is main concern in MANET due to path management for data transmission. In this paper MANET security has been discussed to overcome various attacks performed by attacker.in this paper black hole attack detection has been done on the basis of dynamic detection strategies malicious node that degrades performance of network has been detected. Purposed approach provides much better results than previous approaches available for data communication and attack detection in MANET.

Keywords
Black hole nodes, CRN, Mobile Ad-hoc Network

1. INTRODUCTION
The mobile ad hoc network is a collection of independent mobile nodes and nodes are communicated to each other through the radio waves. The mobile nodes are interacting with radio range that can directly communicate to each other. Others need the help of in-between nodes to route their packets. Every node has a wireless boundary to communicate with each other. These types of networks are completely circulated and we can work at any place without the help of any fixed infrastructure as access points or base stations.

Figure 1 following a simple ad-hoc network with 3 nodes. Node 1 or node 3 are not within range of each other, however the node 2 can be used to onward packets among node 1and nodes 2. The node 2 will take action as a router and these three nodes together form an ad-hoc network.

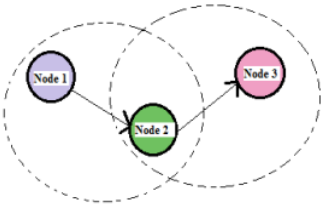


Fig. 1 Example of mobile ad-hoc network

A. MANET's characteristics

1) **Distributed operation**:
There is no backdrop network for the essential control of the network operations. The control of the network is distributed among the nodes. The nodes concerned in a MANET should help with each other and correspond among themselves and each node acts as communicate as desirable, to execute specific functions such as routing and security.

2) **Multi hop routing:** when a nodes transfer some information to other nodes but which is out of its communication gap through the range, the all packet should be forwarded by one or more intermediate nodes.

3) **Autonomous terminal:** the MANET each mobile nodes is a self-governing node, which could purpose as both a host and a router.

4) **Dynamic topology:** all nodes are free to move randomly with different speed. Therefore, the network topology may modify randomly and at impulsive time. These nodes in the MANET Energetically set up routing among themselves as they travel around, establishing their own network.

5) **Light-weight terminals:** In these nodes at MANET are mobile with fewer CPU ability, low control storage and small memory size.

6) **Shared Physical Medium:** The wireless communication intermediate is accessible to any entity with the appropriate equipment and sufficient resources. So, access to the channel cannot be restricted

Cognitive radio is enabling an adaptive approach in utilizing existing wireless spectrum.

This approach introduces a dissimilar perception of physical layer operations and ultimately affects the whole greater layers.

The cognitive radios have become accepted in the past few years.

The major reasons are because they present the capability for secondary users (SUs) to use and share the approved variety bands opportunistically and support prioritization for the transmissions of approved/primary users (PUs), concurrently. Hence, cognitive radios are possible to increase the spectrum utilization.

In order to use the approved spectrum band, SUs must have at smallest amount one cognitive radio transceiver. With the cognitive radio transceivers, SUs search for empty spectrum, called spectrum chance, by conducting spectrum sensing. Since the Pus have the authority to use the certified spectrum

Band, SUs necessity not interrupts the transmissions of PUs by performing reconfiguration of transmission parameters or moving to other vacant spectrum bands [1]. This is creates dynamic use of spectrum bands, somewhere the SUs are able to switch among dissimilar spectrums.

The dynamic uses spectrum bands that creates adverse effects on network performance, if the same communication protocols in their developed considering a fixed frequency

band, are useful. Consequently, new protocols should be designed suitably to suit the cognitive radio network environment. Some Years ago, the cognitive radio networks existed mainly in the physical and medium access control layers, as well as spectrum sensing, spectrum sharing, and spectrum management.

But today, there are an amount of works that recommend routing protocols for cognitive radio networks. This is might be triggered by the exceptional properties of cognitive radio networks that guide researchers to explore diversity of methods to best suit cognitive radio networks: since adding some adaptations of obtainable routing protocols to creating entirely new protocols.

In this paper, on-demand routing protocols appropriate for cognitive radio ad hoc networks (CRAHNs) are classified and reviewed, and then challenges and open issues are discussed. These protocols are based on the ad-hoc on demand distance vector (AODV) dynamic source routing (DSR), and hybrid on-demand routing protocols. Since of the demanding nature of CRAHNs, there are several single issues encountered while designing a routing protocol. The association study shows that there are an amount of challenges remaining in order to design an absolute and feasible routing protocol for CRAHNs.

2. REVIEW OF LITERATURE

Di crescenzo, G. "Securing reliable server pooling in MANET against byzantine adversaries" In this paper, author execute comprehensive of the security of serpool in MANET beside both server failure and particularly, complex attacks. In this paper formulate security necessities for serpool in MANET. This is design capable and dispersed survivable security solution for both main phases of serpool; these are service detection or service prevision. In this paper author use secure the service discovery phase by secure multiple dominating set creation protocol. Secondly provide the service provision phase with using a novel type of the threshold signature scheme. These all protocols using for address novel security goals. In this paper find some independent interest we can find application to the other areas these are most notably the creation of dispersed and survivable public-key transportation in MANET.

Bellavista, P. "Convergence of MANET and WSN in IoT Urban Scenarios" In this paper author describes Ubiquitous smart environments, prepared with economical low and easy-deployable wireless sensor networks (WSNs) and widespread mobile ad hoc networks (MANETs).In this paper opening brand new opportunities in wide-scale urban monitoring. Certainly, MANET and wireless sensor network divergence paves the method for the expansion of latest internet of Things (IoT) it provides communication platforms with a high impending for a wide collection of applications in different domains.

Overlays are used to dynamically distinguish and fasten the relief of insistent sensed data over low-latency MANET paths by integrating with latest growing standards/disclaimer for WSN data sets. The reported tentative outcome illustrates the feasibility and efficiency (e.g., limited coordination overhead) of the proposed key.

Ziming Zhao. "Risk-Aware Mitigation for MANET Routing Attacks" In this paper, author proposes a risk-aware response mechanism to analytically cope with the recognized routing attacks.

In this paper author explained risk-aware approach is based on a complete Dempster-Shafer mathematical hypothesis of verify introducing a notion of significance factors. This paper explaining accumulation, these experiments display the helpfulness of this approach with the concern of several performance metrics.

Gaeta, R. "Exploiting Rate less Codes and Belief Propagation to Infer Identity of Polluters in MANET" In this paper author proposed SIEVE, a completely distributed technique to conclude the identity of malicious nodes. These nodes creates what we termed a ensure when a large piece is decoded a check is a pair composed of the set of other nodes that provided coded blocks used to decode the chunk (the chunk up loaders) .flag representative whether the chunk is corrupted or not. The author explained separate exploits rate less codes to detect chunk integrity and belief propagation to suppose the individuality of malicious nodes. In particular, every node separately constructs its own bipartite graph (a.k.a. factor graph in the literature) whose vertexes are checks and nodes, correspondingly. Then sometimes runs the belief broadcast algorithm on its factor graph to conclude the probability of other nodes being malicious. In the paper by running complete simulations using ns-3 that SIEVE is extremely perfect and robust under several attack scenarios and deceiving actions. Author discuss how the topological properties of the factor graph impacts SIEVE act and demonstrate that nodes speed in the MANET plays a role on the recognition accuracy. Additionally, an appealing trade-off amid coding efficiency and SIEVE accuracy, completeness, and reactivity is exposed. Author also shows in this paper that SIEVE is capable requiring low computational, memory, and communication resources.

3. METHDOLOGY

MANET is field of networking that deals with transmitting information from source to destination without interference of any external device. In MANET communication between nodes gets with utilization of intermediate nodes available in the network. Sender nodes transmit a route request message to neighbor nodes for route discovery from source to destination. In the process of route discovery mechanism Route request message has been transmitted from the sender node that contain source and destination id, IP address, hop-count and destination sequence number. Neighboring nodes receives the request and transmit information forward to their intermediate nodes and match destination id at the RREQ message receiving node. If destination gets matches at receiver end a route reply message has been forwarded from the destination node by intermediate nodes and a route between sender and destination has been established that has been used for data transmission.

Route Request Message Format (RREQ)

Table 4.1 RREQ message Format

Header	Flag	Type	Packet Size	Hop Count
Broadcast ID				
RREQ ID				
Destination IP Address				
Destination Sequence Number				
Source IP Address				
Source Sequence Number				
Path Node IP Address				
Path Node Sequence Number				

This table defines route request message format that has been used for broadcasting the message to the available nodes in the transmission range. In this message contain hop count, packet size, header, destination and source id for data transmission from source to destination.

In the data transmission from source to destination this node checks the route table for data transmission if any route exists in the table then follow particular route for data transmission, if no route is available then route request process starts for data transmission. Source node generate request packet that contain source, destination id, hop count and sequence number. This packet also contain broadcast ID that get incremented at each time node use RREQ message.

In the process of data transition from S node to D, source starts broadcasting message from S to all the nodes that receive the packet and transmit to other nodes that are neighbor to P node. Each node matches ID with destination ID from the message if ID gets matched with node ID then message will not be forwarded again.

Table 2 Request Reply Message Format (RREP)

Type	Flag	Reserved	Packet Size	Hop Count
Destination IP Address				
Destination Sequence Number				
Source IP Address				
Lifetime				

Table 4.2 Route Reply Message Format

This table represents route request reply message format that has been transmitted by the intermediate node and destination node. The best path has been selected from all the request reply messages from destination to source. In the selection of best route different routes with sequence number and hop count has been selected from routing table. If there is multiple routes reply path for data transmission then by default first route is selected or route with greater sequence number and less hop count has been selected for data transmission. Data has been transfer from source to destination by using the various intermediate nodes available in the network.

In the process of route selection due to mobility in the nodes deployed in the network route has to be update after each re-run. On transmission of the data after every successfully data transmission roué has been established using RREQ process.

Due to advancement in the network various attackers are pruned to degrade performance of network. In the purposed work black hole detection has been done using detection approach. In this process attacker perform single or multiple black hole attacking process in the network. Any node that has been subjected to an attacker cause itself has a shortest path from source to destination by transmitting RREP message having highest sequence number. A Black hole node available in the network receives data from source node and doesn't forward data to destination. This causes low performance of network.

In the purposed work detection of black hole node has been done by using detection mechanism that works on the principle of cooperative bait based detection approach. In this process if any node transmit RREP to source node then single hope neighbor node result has been transmit. This bait request has been forwarded when any node packet delivery ratio gets less than a particular threshold value then CBDS message has been forwarded to single hope neighboring nodes for checking of malicious nodes from the networking nodes. In the purposed work one-hop neighboring nodes has been detected for malicious node detection.

One hop neighboring node message has been transmitted by the node to check the reverse tracing mechanism. In the purposed work detection mechanism has been detected using three different strategies for malicious node detection that use dynamic delivery threshold, destination sequence difference and cooperative bait detection scheme in a combination for detection of malicious node.

4. RESULTS

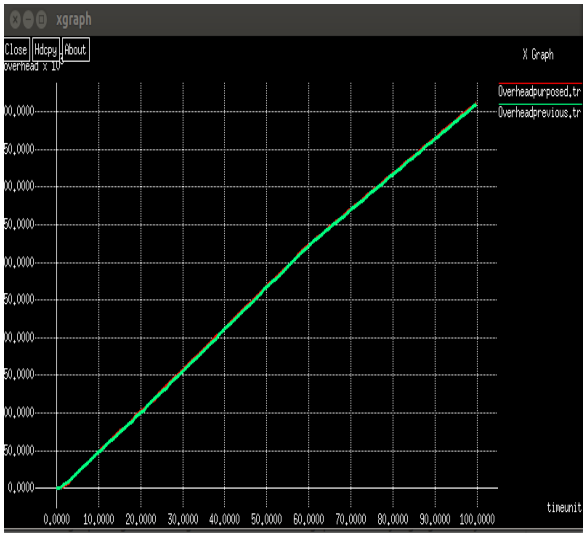
In the purposed work MANET malicious node detection has been simulated using NS-2.35 simulator. This simulator provides platform for deployment of AMNET in a particular are and nodes mobility and routing strategies has been defined for simulation. In the purposed work 50 nodes has been deployed in the network that has been used for simulation of MANET. The nodes start transmission information from source to destination using ad-hoc on demand vector routing protocol. This simulation use dynamic route selection strategy for data transmission.

Table 5.1 simulation parameter

Parameter	Description
Area	1500 * 1500
Number of nodes	50
Antenna	Omni
Queue Type	Drop Tail
Queue Length	250
Routing Protocol	AODV
MAC Type	8.02/11
Queue Length	200
Mobility Speed	0-20 m/s
Application Traffic	CBR
Packet Size	128

This table represents various simulation parameters that have been defined for MANET communication. In the purposed work various parameters have been analyzed for performance evaluation of purposed work.

In the purposed work various parameters have been analyzed for performance evaluation of purposed work. On the basis of these parameters performance of purposed work has been validated.



Graph 5.1: Overhead

This figure is use to represent the overhead in the network. The overhead reduction observed in the figure gives us a margin, which is enough to add some overhead generated by the modifications and new mechanisms needed to introduce hierarchical routing to MANET, and to keep an important reduction.

Graph 5.2: Throughput

It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation.

In this graphical representation comparison has been made between Purposed Throughput & previous Throughput. Red line represents the purposed Throughput & Green line represent the previous Throughput.

Graph 5.3: Packet Delivery Ratio

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

PDR = (P r / P s) * 100

In this graphical representation comparison has been made between Purposed PDR & previous PDR. Red line represents the purposed PDR & Green line represent the previous PDR.

Graph 5.4: Delay

This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

D = (T r - T s)

Where, T r is receive time and T s is sent time of the packet. In this graphical representation comparison has been made between Purposed Delay & previous Delay. Red line represents the purposed Delay & Green line represent the previous Delay.

5. CONCLUSION& FUTURE SCOPE

MANET is used for communication between different nodes using intermediate nodes without any external source. In this paper malicious node detection has been done using dynamic delivery threshold, DSN and CBDS approach that use reverse tracking mechanism for detection of malicious node. Black hole node transmit RREP message to source about shortest path for data transmission and does not forwarded data. In the purposed work detection approach provides better data transmission and detection of malicious nodes available in the network. By analyzing various parameters for performance evaluation that are packet delivery ratio, throughput, end to end delay and network overhead we can conclude that purposed approach provide better data transmission and security in the network.

6. REFERENCES

[1] Shakshuki, E.M. "EAACK-A Secure Intrusion-Detection System for MANETs" IEEE Journals on Industrial Electronics, Volume 60, 2012, pp. 1089–1098.

[2] Lee, Uichin. "Efficient peer-to-peer files sharing using network coding in MANET"IEEE Journal on Communications and Networks, Volume10, 2008, pp. 422–429.

[3] Hiranandani, "MANET protocol simulations considered harmful: the case for benchmarking" IEEE Journal on Wireless Communications, Volume: 20, 2013, pp. 82 – 90.

[4] Burbank, J.L. "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology" journal IEEE on Communications Magazine, Volume 44, 2006, pp-39 – 45.

[5] Dongkyun Kim. "Improving TCP-Vegas Performance over MANET Routing Protocols" journal IEEE on Vehicular Technology, Volume 56, 2007, pp. 372 – 377.

[6] El Defrawy, K. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs IEEE Journal on Mobile Computing, Volume10, 2010, pp. 1345 – 1358.

[7] Di Crescenzo, G. "Securing reliable server pooling in MANET against byzantine adversaries" IEEE Journal on Selected Areas in Communications, Volume 24 , 2006,pp- 357 – 369.

[8] Bellavista, P. "Convergence of MANET and WSN in IoT Urban Scenarios" IEEE Journal on Volume 13, 2013, pp.3558 – 3567.

[9] Ziming Zhao "Risk-Aware Mitigation for MANET Routing Attacks", IEEE Journal on Dependable and Secure Computing, Volume 9, 2011, pp. 250–260.

[10] Gaeta, R. "Exploiting Rate less Codes and Belief Propagation to Infer Identity of Polluters in MANET", IEEE Journal on Mobile Computing, Volume 13, pp. 1482 – 1494.