International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 559 - 563

Utilizing the protected learning calculation method to forestall the Black Hole Attacks in Mobile ad-hoc networks

Gayathri G N
Student, M.Tech (CSE)
S.I.E.T
Tumakuru, India
gaytri.infosea@gmail.com

C V Shanmuka Swamy
Associate Professor
S.I.E.T
Tumakuru, India
shanmuka.c.v@gmail.com

Abstract **-** Mobile Ad-hoc Networks (MANETs) are a gathering of portable hosts which speak with each other with no focal system power or altered foundation. Because of its attributes like portability furthermore, heterogeneity ad-hoc networks are more defenseless to assaults. Black hole is an assault where every one of the bundles sent to assailant hub, by neighboring hubs, are dropped purposefully. In this thesis, we propose a secure learning calculation method which intends to identify and securing the black hole by considering the bundle drop reasons in needless mode. Presented AODV direction convention is adjusted to distinguish and securing the black hole assault. The investigation results demonstrate that our proposed calculation secure the AODV against black hole assault in MANETs.

Key Terms: *Mobile Ad-hoc networks, Security Attacks, Black Hole Attack, Packet drop, Learning Calculation method.*

*****

I. INTRODUCTION

The outline objective of Mobile ad hoc networks innovation is to bolster web get to anyplace and whenever, with no pre-characterized base, which underpins the versatility of the clients, where system intelligence is set inside each mobile node. Because of its self-design and self-maintenance capacities MANETs can have a few sorts of uses like salvage operations, military what's more, security operation, conferencing, law requirement and home system.

MANETs are framework less [1] in which hubs are allowed to move and to convey themselves in a discretionary manner. Two nodes can have numerous connections between them for correspondence and sent in a stand-alone form, reasonable for expense and time compelling environment, and for a circumstance where framework is hard to setup.

MANETs communication is through single hop in connection layer Protocols and multi hop in network layer Protocols, taking into account the presumption that every one of the node in a system are agreeable in coordination process, however tragically this suspicion is not valid in unfriendly environment. Misbehaving assaults can without much of a stretch disturb system operation by disregarding convention details .The network layer operation in MANETs depend on routing and information bundle sending both are defenseless against pernicious assaults.

MANETs do not have a unified framework, without being subject to the focal power, each node in the system needs to assess the trust of different nodes by its own particular experience furthermore by the suggestion of other neighborhood nodes. The trust can be measured on the off chance that it is computed inside an extent in light of the fact that inside specific range limit trust esteem for continuous undertaking can be sensibly characterized. The edge trust values denote a breaking point of trust which a node needs to accomplish to stay trusted. A limit estimation of 0.3 is characterized and the node having trust values not as much as that is considered untrusted or traded off.

Security is trying in MANETs because of its attributes, for example, shared design, working without focal facilitator, dynamic topology, unstable operational environment, and incessant connection breakage because of versatile nodes, battery lifetime, computational limit and heterogeneity

Routing in MANETs is named as Reactive (On-interest) routing and Proactive (Table driven) routing. A reactive convention starts routes at whatever point they are required though proactive Protocols keep up reliable and cutting-edge tables which contain routing data from every node to each other node in a system.

Our manuscript concentrates on alleviation of Black Hole assault on AODV to notice and stop such attack and also by considering the packet drop reasons.

II. RELATED WORK

In this thesis, we are considering reactive protocol, for example, AODV. Since no security instrument is given by AODV, assault can be performed by any misbehaving node by defying the protocol details.

The major AODV vulnerabilities are Tricky increasing of Sequence Numbers and decrementing of hop Check [1]. Black Hole assault is an assault in which every

one of the bundles in a system are diverted to a particular node that dishonestly claims to have crisp route, and ingests or drops those packets without sending them to other or destination nodes. Our paper concentrates on alleviation of Black Hole assault on AODV by considering the packet drop reasons.

AODV [3] is a well-known and most widely used protocol in MANETs. It is reactive(on demand) protocol, in which routing information is exchanged only when communication needs to take place between nodes and only as long as the communication occurs this information is updated.

AODV protocol uses three control messages that are
Route Request (RREQ), Route Reply (RREP), and Route Error (RERR).

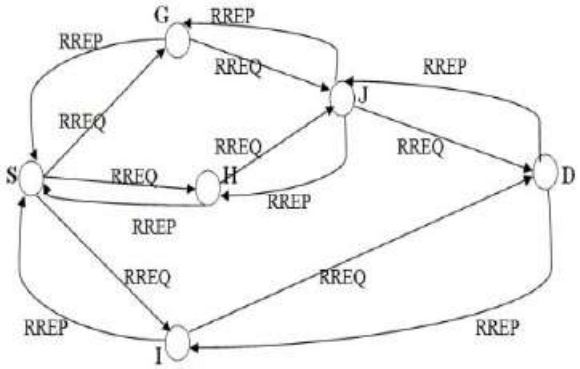

Fig 1: AODV Routing Protocol

RREQ packet is broadcasted to the nodes in the network, by the source to find a path, all the nodes which receive RREQ packet keep transmitting it until it finds a fresh enough route to the destination. On receiving RREQ, if the node is destination or if the node has fresh route to destination, it sends RREP packet. Hop count of every node increases by one on receipt of RREQ message and route entry is updated with new data by intermediate nodes on receipt of RREP message. A node increases its sequence number each time a new RREQ, RREP, RERR messages are sent. Whenever a node wants to communicate with other node, a route discovery process is initiated.

Blackhole Assault [2] is a sort of Denial of Service Assault. Blackhole Assault is a misbehaving node utilizes its directing convention to promote itself having the briefest way towards destination node. At the point when path is set up, then misbehaving node drops the bundles or advances it to the assailant fancied location.

There are two types of Blackhole attacks namely (i) Single Blackhole Attack (ii) Co-operative Blackhole Attack

In single Blackhole assault, one and only malicious node present in the system. It sends fake RREP to source node attempting to trick source node that it has most brief way to destination.

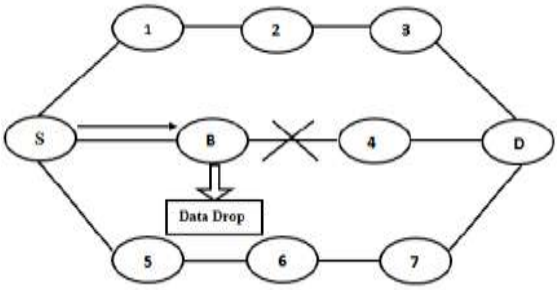

Fig 2: Single Blackhole Attack

In Fig 2, S source node will not consider any routes and sends information to Blackhole hub. In the wake of getting information from source node, Blackhole node drops every one of the information data packet which it needs to forward to node 4.

In co-operative Blackhole assault, two or more nodes act misbehavily in collaboration with each other in the system.

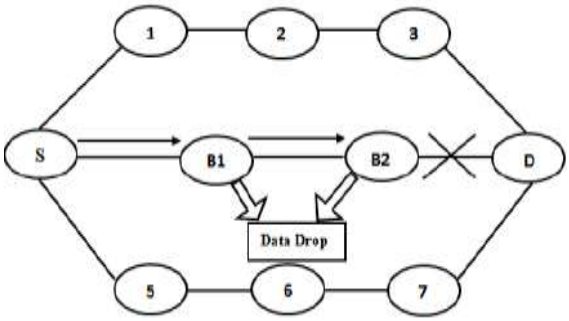

Fig 3: Co-operative Blackhole Attack

In Fig. 3 demonstrates the helpful Blackhole assault in which node B1 also, B2 drops every one of the information bundle without sending it to destination D.

III. Existing Methods

Routing protocols [6-8] which aims to find secure route based on Public Key Infrastructure (PKI), where network has to depend on third party and also, PKI adds extra overhead regarding key maintenance.

The protocols [4-5] aim to mitigate black hole attack taking in account packet drop but not considering the reasons for packet drop.

SubhashisBanerjee MousumiSardar et.al[9] have proposed trust based mechanism for detection and mitigation of black hole nodes from the network. They have introduced mechanism which detects malicious node from the network without introducing additional control packets and without modifying routing table. Detection is originator initiated hence there is no need to rely on intermediate nodes.

Fidel Thachil et al. in [3] proposed a method to mitigate black hole attack in which each node monitors its neighbor by maintaining a cache which records the packets forwarded to the neighboring nodes. The node checks the packet it forwarded to its neighbor is being further

forwarded or not and based on it a trust value is calculated on the neighboring node. If the trust value of a node goes below a predefined threshold, it is declared malicious. The paper . The paper calculates trust value based on packet drop but does not consider packet drop reasons.

L TamilSelvan et al. in [10] proposed a solution whichmodifies AODV such that it stores more than one RREP. In 'TimerExpiredTable' a timer is set after receiving first RREP. All the replies that arrived before the timer expires are stored in 'Collect Route Reply Table' (CRRT). All received RREP are checked by source for repeated next hop node to destination, after timer is expired. An RREP is chosen if it is repeated next hop, else a random RREP is chosen. In case there is no repeated node, it's difficult to predict maliciousness.

Ankita V. Rachh et al. in [5] proposed an approach called EBAODV (Enhance Black hole AODV), which creates leader nodes for detecting malicious nodes. A timer is set as the source node generates RREQ. Before expired time if RREQ is received a fake packet is sent to destination and on receiving acknowledgement (ACK) original packet is sent by source. Packets are dropped if ACK is not received. Method for selection of leader nodes is not given. Sending fake packets causes additional overhead and packet drop reasons are not considered.

In this thesis, we present a narrative advance to alleviate black hole attack while taking into consideration of packet drop reasons.

IV. PROPOSED SCHEME

The proposed an approach for detection and prevention of Black hole attack using protected learning calculation method in which it used immoral mode to ensure data delivery to receiver node, also finds packet drop reasons before declaring node as a black hole node. In this method, AODV protocol is modified, so that every node in a network listens to its neighboring nodes promiscuously and nodes compares the neighbor node information stores in its fm and rm table entries: fm table hold the detail about recent packet forwarded. rm table hold the detail about neighboring node detail like destination address, TTL value, and Node Energy. If any entries in the table which has fm ≠ rm and threshold value is reached then modification attack otherwise trusted node. If rm and threshold value is reached then Black hole attack.

Knowledge table contains the information about the packet which is most recently transmitted. When any node detects a black hole node in a network, it broadcasts the node's id to other nodes so as that the malicious node can be avoided in routing process. Our algorithm is based on AODV, where the best path is based on minimum hop and maximum sequence number.

At the point when source needs to send the data to destination, it telecast the control parcel RREQ to its whole neighboring node. RREP is generated by destination through trusted nodes only, if any node is found malicious during route discovery process, its information is transmitted to all other nodes. If already a route is established and later it learns that one of the nodes of its route is a black hole node than the source node removes that node and re-initiates the routing process.

The proposed method is as follows:

STEP 1: Each hub in indiscriminate mode keeps up a table containing two fields "fm" and "rm".

STEP 2: Looking at "fm" and "rm"

- ✓ In the event that fm ≠ rm and threshold is achieved then modify Assault and otherwise node is trusted hub.
- ✓ Assuming no 'rm', Check Packet Properties.
  (i) Destination address
  (ii)Time To Live(TTL)
  Assuming alright, Check Hub Properties (Vitality)
- ✓ Assuming no "rm" and threshold reaches then Blackhole Assault.

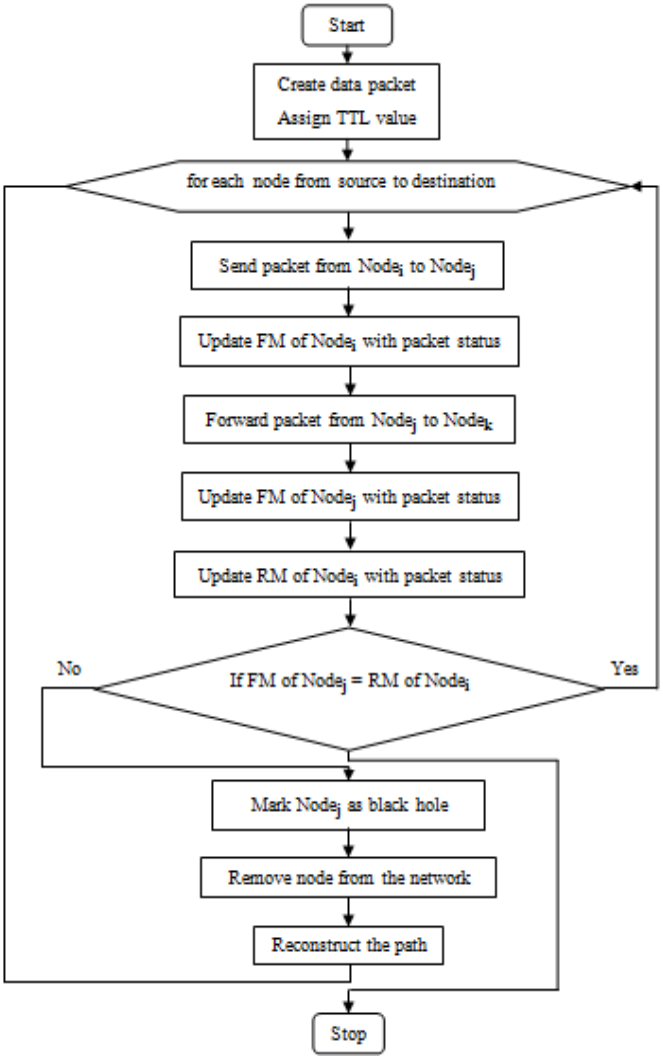

Fig 3: Flow chart of proposed Method

V. EXPERIMENTAL RESULTS

The experiment results for our proposed method is carried out with of Network Simulator Version-2 (NS2).We have successfully implemented protected knowledge method to secure AODV routing protocol against black hole attack.

The following are the parameters to do the simulation part.

Total Number of Nodes	ten, twenty, thirty
Size of network	600 * 600
Medium access control	802.11
Radio Propagation Range	Two hundred and fifty meter
Time of Simulation	Hundred sec
Traffic Source	Constant bit rate
Packet Size	Five hundred and twelve
Model of mobility	Random Way Point mobility
Speed of node	Two, four, six and twelve m/sec

Table 1: Simulation

This strategy gives better execution contrasted with existing AODV convention in throughput and Delay. The principle goal of reenactment is to demonstrate proposed technique is legitimately securing existing AODV with all security perspective regarding Blackhole Attacks.

.

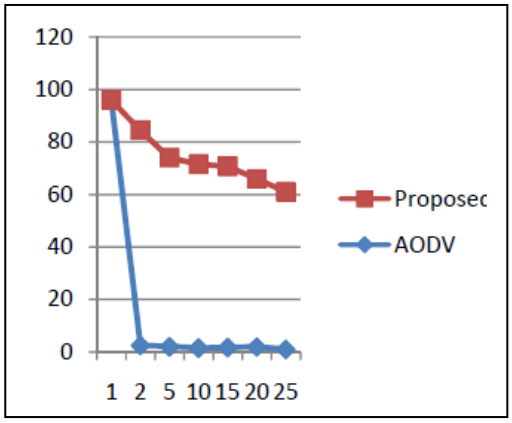

Fig 4: packet delivery ratio v/s number of misbehaving node with100 sec Simulation time

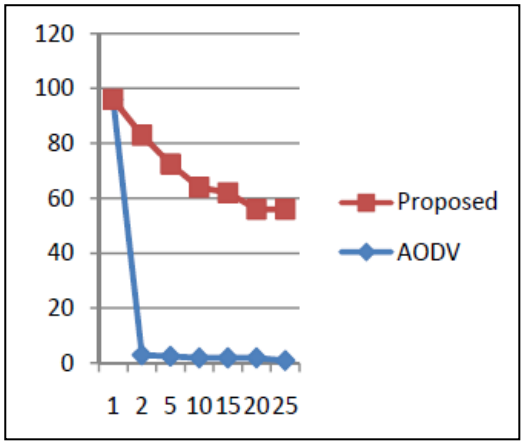

Fig 5: packet delivery ratio v/s number of malicious node with 500sec Simulation time

VI. CONCLUSION AND FUTURE SCOPE

Here, it is conclude that the proposed scheme will identify and also avoid the Blackhole attacks in a network. The method monitors the data packets that are being forwarded in immoral mode to ensure that the packets are delivered to destination node.

If any node drops a packet our method checks for the packet drop reasons first, before announcing it as a black hole node. So it ensures to prevent the trusted node in a network.

As future work, research work intend to develop simulations to analyze the performance of the proposed method depends on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of single and multiple attacks against AODV.

REFERENCES

[1] Ayesha Siddiqua Kotari Sridevi Arshad Ahmad Khan Mohammed, “Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm”, SPACES-2015, Dept of ECE, K L UNIVERSITY.

[2] Payal J. Desai1, Urmi Desai “Detection of Cooperative Blackhole Attack on Multicast In MANET” ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-2, ISSUE-7, 2015.

[3] Fidel Thachil, K.C. Shet, "A Trust Based Approach for AODV protocol to Mitigate Black hole attack in MANET ," 2012 International conference in Computing Science., IEEE 2012.

[4] Durgesh Kshirsagar, Ashwini Patil, “Black hole Attack Detection and Prevention by Real Time Monitoring”, 4th ICCCNT 2013, July 4-6, 2013, Tiruchengode, India.

[5] Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, “A Novel Approach for Detection of Blackhole Attacks” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74.

[6] A.Rajaram, Dr. S. Palaniswami,”Malicious Node Detection System for Mobile Ad hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010.

[7] Y.-C. Hu, D. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Ad Hoc Networks, Elsvier, vol. 1, no. 1, 2003.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proc. 8th Ann. Int’l Conf. Mobile Computing and Networking (MobiCom’02), ACM Press, 2002

[9] Banerjee, Subhashis, MousumiSardar, and KoushikMajumder. "AODV Based Black-Hole Attack Mitigation in MANET." In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013, pp. 345-352. Springer International Publishing, 2014.

[10] TamilSelvan, L.; Sankaranarayanan, V., "Prevention of Black hole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on , vol., no., pp.21,21, 27-30 Aug 2007.