IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Survey of Black-hole Attack Mitigation and Prevention in MANET

Sonali Khandelwal[1], Amit Shrivashtav[2]

Research Scholar, Dept of Computer Science Engineering, Swami Vivekannd College of Engineering, Indore, India[1]

Assistant Professor, Dept of Computer Science Engineering, Swami Vivekannd College of Engineering, Indore, India[2]

Abstract: Mobile Ad-hoc Networks features such as open medium, mobility of nodes, lack of back bone system and lack of infrastructure contribute various security attacks. Black hole attack is one type of attack that is more common in MANET reactive routing protocols. Black hole attack takes advantage of route discovery process in reactive routing protocols. In Black-hole attack, a malicious node misguide other nodes in the network by pretending to have the shortest and fresh route to a target node whose packets it wants to attack. This paper analyses the cooperative Black-hole attack detection and prevention. In this scenario, Ad-hoc on demand multipath distance vector routing protocol is configuring to provide multiple path for data communication. For this, we have listed various research carried out to discover and mitigate the single and cooperative Black-hole attack in MANETs.

Keywords: MANET, AODV, AOMDV, Security, Black-hole, Routing Protocol.

I. INTRODUCTION

MANET is a group of mobile devices that can spontaneously interconnect and share resources via wireless communication channels, with no fixed network infrastructure or central management. MANETs can be assembled quickly with little cost because they do not require central monitoring or fixed network infrastructure. Mobile nodes in MANETs need not to be of same type. They can be PDAs, laptops, mobile phones, routers and printers, as shown in Fig.1. The nodes are equipped with antennas which operate as wireless transmitters and receivers. The antennas may be unidirectional, highly directional, or a combination. The mobile nodes are resource constraint in terms of bandwidth and battery power [2, 3].

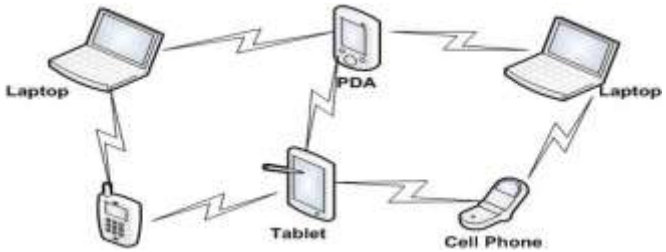

Figure 1 Mobile Ad hoc Network

MANETs are suitable to provide communications in many applications, particularly in cases where it is not possible to setup a network infrastructure. For instance, in a military operation, where there may be geographical barriers between participants, MANETs can be setup to facilitate communication. Also because it is easy to set up, it may be of assistance to replace the damaged network infrastructure in disaster recovery operations where temporary network infrastructure is Immediately needed [4,5].

MANETs Challenges

1) Confinement of transfer speed: Wireless connection have essentially bring down limit than foundation systems. Furthermore, the throughput of remote correspondence in the wake of representing the impact of various get to, blurring, commotion, and obstruction conditions, and so on, is regularly considerably less than a radio's greatest transmission rate.

2) Dynamic topology: A profoundly powerful topology is a recognizing highlight and test for MANETs. The hubs are allowed to move inside the system so that the connections between hubs made and broken consistently. This hub versatility not just influence the source hub or potentially goal, as in a customary remote system, additionally moderate hubs, because of the systems multihop nature. Accordingly the directing of parcel between the hubs is the significant issue in Mobile specially appointed systems.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

3) Routing Overhead: In Mobile ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
4) Hidden and uncovered terminal issue: Hidden terminal issue happens in systems utilizing conflict based conventions, for example, ALOHA, CSMA/CD, and so forth. At the point when two hubs which are out of scope of each other send information edges to a hub which is inside their separate radio ranges, a crash of information casings happens. An uncovered terminal issue is happens when hubs are in the scope of the transmitter, however out of the scope of the recipient.
5) Loss of parcels because of transmission mistakes: There are higher bundle misfortune encounters in Ad hoc remote systems because of expanded impacts, because of the nearness of covered up and uncovered terminals, nearness of obstruction, omnidirectional connections, visit way creation and breaks because of versatility of hubs.
6) Battery control imperatives: Devices utilized as a part of MANETs have impediment on the power source keeping in mind the end goal to look after versatility, gadget compactness, size and weight of the gadget.
8) Security: Security is a fundamental prerequisite in versatile specially appointed systems. MANETs are more helpless against security assaults because of the absence of a confided in concentrated expert and constrained assets.

Whatever remains of the paper is sorted out as takes after: Segment II depicts steering in MANETs and examines the distinctive classes of directing conventions, concentrating more on receptive directing conventions. Segment III clarifies dark opening assault. Segment IV depicts a portion of the arrangements that have been proposed to decrease the impact of the dark opening assault. Segment V portrays the proposed arrangement. Segment VI finishes up the study of Black-opening assault in MANETs.

II. ROUTING IN MANETS

In MANET topology is changing quickly because of free development of hubs joining and leaving the system at whatever time. Steering is vital with a specific end goal to find the current topology so that a refreshed course to a specific hub can be set up and a message handed-off to the right goal [3,6]. The conventional steering conventions, for example, separate vector and connection state conventions that have been organized for hard wired systems can't be straightforwardly connected to MANETs. This is a result of versatility and dynamic topology, which are the principal qualities of MANETs [7]. So as to overcome directing difficulties in MANETs and achieve successful steering, various directing conventions are characterized particularly for MANETs. These conventions can be sorted into proactive, responsive and half breed conventions in view of the ways are set up and kept up by the hubs [8]. The progression of the directing conventions in MANETs appears in Fig. 2.

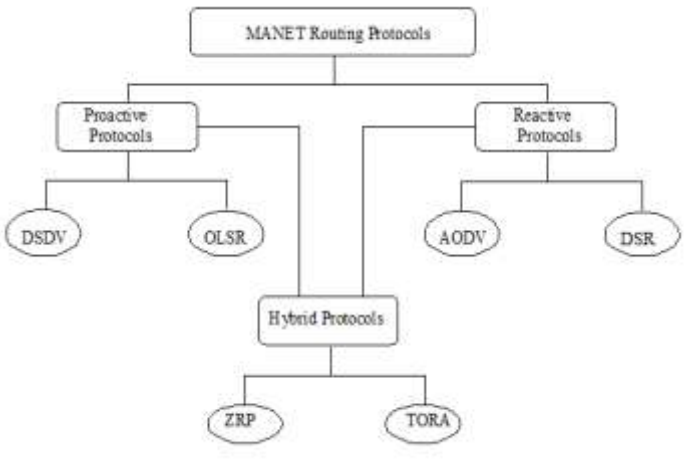

Figure 3 MANET Routing Protocols

A. Proactive Protocols

Proactive or table-driven steering conventions attempt to keep a record of new system courses. Every one of the hubs in the system have a table to store the directing data [8].The hubs trade topology data with the goal that they can all have a similar perspective of the system. The traded data mirrors any adjustments in the topology. At whatever point a hub needs to send messages, it just scans the directing table for the way to the goal. The sending of the message is not deferred by the remote course revelation [11]. Keeping up a progressive topology in the directing tables causes a high control overhead. The outstanding proactive conventions are goal sequenced separate vector (DSDV) directing convention and streamlined connection state steering (OLSR) convention.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

B. Reactive Protocols

Reactive protocols are on demand routing protocols. As the name suggests, the routes to destination nodes are established only when the nodes must send data to destination whose route is unknown. This implies that the source node initiates the searching of routing paths only when needed. It starts a route discovery process when a node wants to send data to a destination node within a network. Comparative to proactive protocols, the control overhead in reactive protocols is reduced; however the route searching process that occurs before data packets can be forwarded may cause source node to suffer long delays [15]. The most common types reactive protocols are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol.

C. Hybrid Protocols

Hybrid protocols are a mixture of proactive and reactive protocols. Their design merges the benefits of both proactive and reactive protocols to yield better results [9]. The hierarchical network model is used to structure majority of hybrid routing protocols. Firstly, all the routing information that is unknown is acquired by using proactive routing protocols after these reactive routing protocols are used to maintain the routing information when the topology changes [10]. The well known hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA).

On-Demand routing protocols work on the principle of creating routes when required between a source and destination node pair in a network topology. Our discussion is limited to two AODV and AOMDV routing protocols, as follows.

Ad-hoc On-Demand Distance Vector Routing

Portable PCs utilize AODV strategy for directing messages to each other. It permits these portable PCs or hubs, to go messages through their neighbors to hubs with which they can't straightforwardly impart. AODV finds the courses along which messages can be passed. AODV ensures these courses don't contain circles and tries to locate the briefest course conceivable. AODV can deal with changes in courses and can make new courses if there is a blunder. A hub keeps data of its neighbors by communicating HELLO Message. At the point when source hub needs to speak with goal hub that is not its neighbor it communicates a Route Request Message (RREQ). The RREQ message contains taking after data: the source, the goal, the life expectancy of the message and a Sequence Number. At the point when neighbors of the source hub get the RREQ message they have two options; in the event that they know a course to the goal or on the off chance that they are the goal they can send a Route Reply (RREP) message back to the source hub, else they will rebroadcast the RREQ to their arrangement of neighbors persistently until the life expectancy of message is up. On the off chance that source hub does not get an answer in a set measure of time, it will rebroadcast RREQ message with longer life expectancy and another ID number. Fig. 3 (a) delineates the arrangement of directing table sections for AODV.

Ad-hoc On-demand Multipath Distance Vector Routing

AOMDV [9] protocol has improved the performance of AODV protocol. It computes disjoint multipath with having loop freedom [1]. In AOMDV, advertised_hopcount replaces hopcount in AODV.A route_list replaces the nexthop, and essentially defines multiple next hops with respective hopcounts. A node i updates its advertised_hopcount for a destination d whenever it sends a route advertisement for d .

$$advertised\_hopcount_i^d := max_k \{hopcount_k \mid (nexthop_k, hopcount_k \in route\_list_i^d)\}$$

As similar to AODV the following condition holds good for two successive nodes i and j on any valid route to destination d.

$$(seqnum_i^d, advertised\_hopcount_i^d, i) > (seqnum_j^d, advertised\_hopcount_j^d, j)$$

Fig. 3 (b) illustrates the formation of routing table entries for AOMDV.

Destination
Sequence number
Hopcount
Nexthop
Expiration time

(a) AODV

Destination
Sequence number
Advertised Hopcount
Route_list {($nexthop_1$,$hopcount_1$), ($nexthop_2$,$hopcount_2$)..}
Expiration time

(b) AOMDV

Figure 3 Formation of routing table entries in AODV and AOMDV

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

III. BLACK HOLE ATTACKS

The best possible working of MANETs relies on upon the common assention and comprehension between the hubs in the system; however a few hubs may wind up noticeably pernicious and get into mischief. Dark gap assault is one of the unsafe assaults brought about by a noxious hub that acts up in a system [21]. In this assault, a malevolent hub demonstrates that it has a legitimate and new course to the goal hub at whatever point it gets RREQ parcels. It sends the REPP with most elevated goal succession number and least jump tally an incentive to originator hub .whose RREQ parcels it needs to capture. For instance, in figure 4, when hub "S" needs to send bundles to goal hub "D", it starts the course revelation prepare by sending RREQ Message. The pernicious hub "M" when gets RREQ Message, it quickly sends RREP Message to hub "S". In the event that answer from hub "M" achieves first to the hub "S" than the source hub "S" disregards all other RREP messages and start to send parcel by means of course hub "M". Subsequently, all information parcels are dropped at pernicious hub. A malignant hub can work freely to dispatch the assault, and this is alluded to as single dark opening assault appeared in figure 4 (an), or malevolent hubs can function as a gathering and the assault is alluded to as helpful dark gap assault appeared in figure 4 (b)[10].

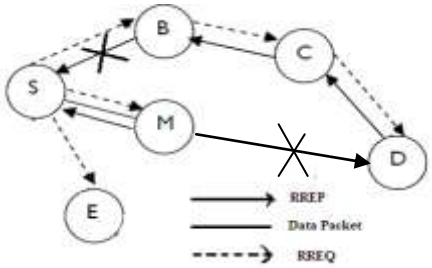

Figure 4(a) Single Black-hole Attack

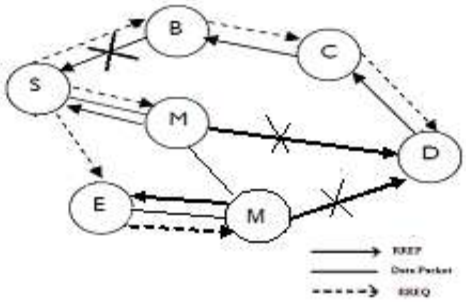

Figure 4(b) Cooperative Black-hole Attack

IV. BLACK HOLE ATTACK MITIGATION

There has been various research carried out to discover and mitigate the black hole attack in MANETs. Some of the mitigation techniques are discussed below:

1) Detection, Prevention and Reactive AODV(DPRAODV)

In et al.(2009) [11],DPRAODV is proposed. In this plan, AODV convention is altered to have another control parcel called ALARM and a limit esteem. A limit esteem is the normal of the distinction of goal arrangement number in the steering table and succession number in the RREP bundle. In the typical operation of AODV, the hub that gets a RREP parcel checks the estimation of arrangement number in its directing table. The arrangement number of RREP bundle must be higher than the succession number an incentive in the steering table with the end goal for RREP to be acknowledged. In DPRAODV, there is an additional limit esteem that is coordinated to RREP succession number, and if RREP grouping number is more prominent than the edge esteem, then the sender is viewed as malignant and added to the boycott. The neighboring hubs are informed utilizing an ALARM parcel so that the RREP bundle from the noxious hub is not prepared and gets blocked. Consequently, the edge esteem gets refreshed utilizing the information gathered in the time interim. This refreshing of the limit esteem recognizes and stop dark gap assaults. The ALARM parcel contains the boycott that has a noxious hub. This rundown helps the neighboring hubs not acknowledge any RREP bundle sent by a vindictive hub. Any hub that gets a RREP bundle investigates the boycott and if the answer originates from a hub that has been boycotted, it is overlooked and additionally answers from that hub will be disposed of. Subsequently the ALARM parcel disconnects a malevolent hub from the system.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

2) EnhancedAODV (EAODV)
In et al.(2011) [12], the creators proposed EAODV. Like IDSAODV, EAODV permits various RREPs from different ways to help the impact of dark gap assault. This strategy makes a suspicion that inevitably the genuine goal hub will unicast a RREP parcel, so the source hub disregards all past RREP passages, including the ones from pernicious hub and takes the most recent RREP bundle. The source hub continues refreshing its directing table with RREPs being gotten until a RREP from the genuine goal is gotten. At that point all RREPs get dissected and suspicious hubs are found and separated from the system. The confinement to this strategy is that it includes two procedures that expansion deferral and fumes vitality of the hubs.

3) Intrusion Detection System AODV (lDSAODV)
IDSAODV is proposed in et al.(2012) [13] with a specific end goal to diminish the effect of dark gap. This is accomplished by changing the way typical AODV refreshes the steering procedure. The directing refresh process is changed by adding a strategy to neglect the course that is built up first. The strategy connected in this technique is that the system that is assaulted has numerous RREP bundles from various ways, so it is expected that the main RREP parcel is produced by a noxious hub. The supposition depends on the way that a dark opening hub just sends a fake RREP bundle, without seeking through the directing table. Along these lines, the principal RREP is overlooked to abstain from refreshing directing table with wrong course data. This technique enhances bundle conveyance however it has restrictions that; the main RREP can be gotten from a middle of the road hub that has a refreshed course to the goal hub, or if RREP message from a pernicious hub can arrive second at the source hub, the strategy is not ready to distinguish the assault.

4) Two Tier Secure AODV
TTSAODV is proposed in et al.(2012)[14] identifies single as well as collaborative black hole attack by verifying the trueness of the RREP message with verification messages sent by neighbours of the intermediate node which sent the RREP without considering the sequence number in the RREP. The basic assumption in this solution is that there is a strong symmetric key distribution system in the MANET. Thus, every pair of nodes in the network has unique common secret key.

5) Trust-based Approach
The creators in et al. (2016) [15] recommended a trust based way to deal with moderate the dark gap assault. In this approach, each hub keeps a trust an incentive on every one of its neighbors. The trust esteem is figured as the extent of disposed of parcels to sent bundles. Every hub guarantees that the neighboring hub advances the bundles sent to it, unless the parcel is bound to the neighboring hub. As an approach to guarantee that the bundles are sent, every hub executes a reserving instrument by putting away the parcel being sent to the neighboring hub in its store, and after that indiscriminately observing the neighboring hub to check whether it advances the parcel. On the off chance that the neighboring hub advances the parcel, it contrasts it and the bundle put away in its store, and the hub expect the bundle has been sent in the event that they coordinate. Else, after a set time the hub accept the bundle has been disposed of by its neighbor and the neigbouring hub is suspected to be malevolent. Every one of the hubs in the system will become acquainted with the conduct of the neighboring hubs, and can in this way occasionally allot trust values that speak to the reliability of the neighboring hubs. All RREP parcels from a hub that has been perceived as vindictive are disregarded, and the courses may be chosen through confided in hubs**.**

V. PROPOSED WORK

In the event of MANET the quantity of hubs are can move unreservedly in the territory in light of the fact that there is no focal controller in the MANET.It is self-designing framework. So when the information is send from source to goal parcel drop is high extensively and Link disappointment issue happen because of free or effectively developments of the hubs. To overcome and diminish the above issue of system different strategies of multipath directing technique had been proposed in the earlier circumstances. Among all the proposed strategies multipath directing is the most productive and dynamic method for development of system execution securing portable specially appointed systems. The proposed system needs to build up a technique by which the directing calculation self-distinguish and keep away from the dropping assault in system. The proposed security model is about of examination of hub conduct in different edge requirements for setting up secure way while AOMDV is altered. This guarantees to give a safe correspondence demonstrate. In this manner the proposed procedure needs to join the accompanying arrangement.

- To provide efficiency during the route discovery this process is taken place
- Obtain some essential network parameters that help to design the node behaviour property which employee security of node that exists on various paths and it improves the performance during the attack.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

This work, we will improve the Detection rate of the attack at the same time when packets are forwarded from single source to multiple destination followed by multipath routing scenario in MANETs. The enhancement will be based on the actual property of the node behaviour. In this work, development of the proposed technique will be done to increase its efficiency in terms of energy, end to end delay, throughput and

VI. CONCLUSION

Security which is a basic element is these sorts of systems because of absence of concentrated control. In this paper, we have investigated the security dangers confronted by a portable specially appointed system and exhibited the security issues that should be accomplished. On one hand, the security-delicate uses of portable specially appointed systems require high level of security; then again, versatile impromptu systems are naturally powerless against security assaults. This study paper starts enter safeguard dangers in MANETs and furthermore investigates Black-gap assault recognition and avoidance procedures, and how these arrangements are able to safe the system. So the at last, by assess the upsides and downsides of realistic systems the open research challenges in versatile impromptu system are examined.

REFERENCES

[1] H.D.Trung, W.Benjapolakul, P.M.Duc, “Performance evaluation and comparison of different ad hoc routing protocols”, Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007
[2] K. Osathanunkul and N. Zhang, "A countermeasure to black hole attacks in mobile ad hoc networks," in Networking, Sensing and Control (TCNSC), 2011 IEEE International Conference On, 2011, pp. 508-513.
[3] B. Wu, J. Chen, J. Wu and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security Springer, 2007, pp. 103-135.
[4] C. Rajabhushanam And A. Kathirvel, "Survey Of Wireless Manet Application In Battlefield Operations," (Ljacsa) International Journal Of Advanced Computer Science And Applications, Vol. 2, Pp. 50-58,2011.
[5] R. Mishra, S. Sharma And R. Agrawal, "Vulnerabilities And Security For Ad-Hoc Networks," In Networking And Information Technology (Lcntt), 2010 International Conference On, 2010, Pp. 192-196.
[6] W. Li and A. Joshi, "Security issues in mobile ad hoc networks-a survey," Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, pp. 1-23,2008.
[7] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE, vol. 14, pp. 85-91,2007.
[8] N. Sharma and A. Sharma, "The black-hole node attack in MANET," in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference On, 2012, pp. 546-550.
[9] V. C. Giruka and M. Singhal, "Secure Routing in Wireless Ad-Hoc Networks," in Signals and Communication Technology, pp. 137-158, 2007.
[10] P. K. Singh and G. Sharma, "An efficient prevention of black hole problem in AODV routing protocol in MANET," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On, 2012, pp. 902-906.
[11] P. N. Raj and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," IJCSI, vol.3, pp. 54-59, 2009.
[12] Z. Ahmad, K. A. Jalil and J. Manan, "Black hole effect mitigation method in AODV routing protocol," in Information Assurance and Security (lAS), 2011 7th International Conference On, 2011, pp. 151-155.
[13] R. Suryawanshi and S. Tamhankar, "Performance Analysis and Minimization of Blackhole Attack in MANET," lJERA, vol.2, pp. 1430-1437, July-August, 2012.
[14] M. Umaparvathi and Dharmishtan K. Varughese “Two Tier Secure AODV against Black Hole Attack in MANETs” European Journal of Scientific Research ISSN 1450-216X Vol.72 No.3 (2012), pp. 369-382
[15] J. Pan and R. Jain, "A survey of network simulation tools: Current status and future development," Internet: http: // wwwl. cse. wustl. edul-jainlcse567-08/ftp/simtools. pdf, Nov. 24,2008 [May 5, 2016].