IJRSET OCTOBER 2017 Volume 4, Issue 10 Pages: 9-14

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

BLACK HOLE ATTACK PREVENTION USING ENHANCED PROACTIVE SECRET SHARING SCHEME

[1]M.mohan, [2]Mr. H. Lookman Sithic, MS (IT)., Mphil., (Ph.D).,
[1] Research scholar, [2]Asst Prof
[1] Dept of Computer Science, [2]Dept of Computer Applications
[1,2] Muthayammal College of Arts and Science
[1,2] Rasipuram, Namakkal.

ABSTRACT: Cell phones are ending up exceptionally prevalent because of the extensive variety of systems administration fitness for the cell phone clients. The security issues in MANET end up noticeably dreary since the control towards the administration of the various number of hubs in the MANET is conveyed. The hub versatility, dynamic topology, transfer speed confinement, uncertain remote correspondence interface and the nonappearance of settled foundation makes the security of information transmission in MANET as a basic issue. There are many steering attacks caused because of absence of security. Any sort of attack in MANET will irritate the whole correspondence and the aggregate system can be crumpled. The vast majority of the steering conventions don't address the issues of the directing attacks. The most well-known attack experienced by the MANET is the black hole attack.

Keywords: [MANET, Attacks, Black hole attack]

1. INTRODUCTION

Cell phones are winding up exceptionally prevalent because of the extensive variety of systems administration capability for the cell phone clients. By and by there are assortments of uses accessible to be gotten to on the cell phones to satisfy the standard errands. The gathering of cell phones shape a system called the versatile specially appointed system (MANET). These are the framework less system where the hubs can join or move out of the system's range whenever. A hub can go about as a switch to forward the information to the neighbor hubs. They have decentralized organization and it is proficient to deal with any mischief of the hubs or any impacts that happens because of topology changes. The connections between the hubs are broken at whatever point the hub moves out of the radio correspondence scope of the system.

The influenced hubs on the course in the system send a demand for new course Foundation and the new connections are built up. Versatile Ad hoc Networks (MANET) are self-governing and decentralized remote frameworks. MANETs comprise of portable hubs which might be the frameworks or the gadgets like cell phone, tablet and individual advanced help. The versatile hubs can shape arbitrary topologies in view of the availability with every one of the hubs in the system. These hubs are capable to constitute themselves and because of their self design office, they can be sent quickly without the need of any framework. The Figure 1.1 shows the dynamic topology of the MANET.

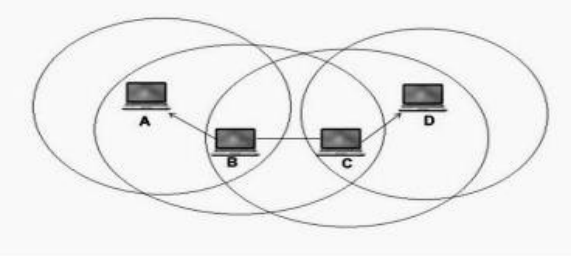

Figure - 1 Dynamic topology of MANET

2. LITERATURE SURVEY

H.Deng et al proposed an answer for keep the black hole attack in AODV. This strategy keeps the middle of the road hub to forward the RREP parcel. Just the goal is permitted to forward the RREP to the source hub. This strategy evades black hole attack, however if there should arise an occurrence of the substantial system, the course foundation delay is expanded. A vindictive hub can without much of a stretch fake a RREP message by caricaturing the IP address. To keep away from this entanglement the creators proposed an answer with the expansion of next bounce's data to the RREP parcel before sending it to the source. The source can confirm whether the following jump hub is a neighbor hub of the middle of the road hub and checks for the accessibility of the course to the goal. This proposed strategy can keep the black hole attack caused by the single pernicious hub. It isn't vigorous in taking care of the circumstance when both the following bounce hub and the transitional hub perform breakdowns. The fundamental disadvantage is that it builds the overhead if the check procedure ends up noticeably repeating for each middle of the road hub answering to the RREQ.

Sun.B et al proposed a strategy to secure AODV convention. In this strategy after the course revelation process, the source sends a control bundle to every one of the hubs on the way that has sent the RREP parcel from the goal asking for to send the present neighbor data. The source hub looks at the got present neighbor data from all the moderate hubs. On the off chance that the contrast between them is bigger than a predefined limit esteem then the black hole attack is distinguished. The arrangement is planned utilizing the cryptographic plan, where the source can build up the right way to the goal there by identifying the black hole hub. However, this strategy endures in keeping the black hole attack.

B.Schneider et al depicts a strategy to maintain a strategic distance from the vindictive hub from the directing way of authentic hubs. The attacks can be maintained a strategic distance from by counteractive action based systems which is difficult to accomplish in MANET.

S.Marti et al proposed a guard dog - way rater component to manage the black hole hub issue. The proposition depends on the inactive criticism system which is intended to secure the DSR convention. Here the guard dog hub will transmit the parcel to the following bounce. A trusted hub is utilized to catch the medium to verify that the moderate hub has sent the parcel to the following hub. On the off chance that the black hole hub is distinguished then the way rater is started to locate another course by staying away from the recognized black hole hubs. In the event that the parcel isn't sent because of the substantial reasons like bundle impact, low power or course movement then this strategy sits tight for the timeframe to infer that the hub is the vindictive hub. So it requires long investment to choose up on the black hole hub. The scheme between the gatherings of hubs can trap the guard dog system. Subsequently the malignant hub can be wrongly surveyed as a real hub.

3. NEPSSS PROTOCOL SCHEME USING ENHANCED PROACTIVE SECRET SHARING SCHEME

Keeping a malevolent hub from knowing any data about the mystery or remaking the mystery is the essential goal of this plan. Here it is conceivable to permit the trusted investors (t) to reproduce the mystery at any timeframe. This upgrade conspire is

actualized in two phases like Black Hole Attack Detection and Secret Sharing Procedure to guarantee the legitimacy of data being conveyed amongst source and goal hub.

3.1 Black Hole Attack Detection

At the point when source S needs to speak with goal D through the moderate hubs (A, B and C), source communicate the course ask for message RREQ. RREQ is adjusted to incorporate the parameters like goal character [Did], successive number[seq_num],the Source's id scrambled by goal's open key [PbD [Sid]] and Time subordinate trust dynamic value[TA]. Following is the altered organization of RREQ parcel.

RREQ [seq_num, PbD [Sid], Did, TA]

At first hub A has the trust an incentive on hub B at time t1. After certain period, hub B may go to another zone which is out of radio scope of hub A, because of the hubs portability in MANET. At time t2, hub B happens to be back in hub A's radio range once more. The trust esteem would rot amid this time hole. Let A T B (t1) be the trust estimation of hub A to hub B at time t1 and A T B (t2) be the rotted estimation of the same at time t2. At that point trust dynamic esteem is characterized as takes after,

$$A^T B(t_2) = A^T B(t_1) * e^{-(A^T B(n)\Delta t)^{2k}}$$

When node A receives RREQ, it looks up its trust list for the trust values of the neighbors and encrypts its own id with proper policy and append in the message. The message which is sent by A will be in the following form

RREQ [seq_num, PbD[PvA[Aid], PbD[Sid], Did , A RB]

where PvA is the private key of A. Evaluation of the node proposal is given by A RB which is node A‘s evaluation to node B by collecting the node recommendations. Node proposal A RB is also used to identify the malicious behavior. The following denotes node A‘s evaluation to node B.

$$R_B^A = \frac{\sum_{v \in \gamma} V|A \to C| * V|C \to B|}{V|A \to B|}.$$

where C | s a gathering of recommenders, V | An is trust vector of hub A to C and the trust vector of hub B to C will be C | . V | B Presently Node B gets the RREQ from Node An and rehashes a similar method took after by Node A. At the point when D gets RREQ from B, it utilizes its private key and people in general key of the middle of the road hubs to verify them. D checks whether there are any vindictive hubs by assessing the hub proposition esteems and the trust dynamic esteem. On the off chance that every one of the hubs are trusted, D creates a stream character (Fid), and communicates the accompanying RREP message.

RREP[PbB[Fid],PbA[Fid],PbS[PvD],[Fid]]

A moderate hub that gets the RREP utilizes its private key to unscramble the message and gets the Fid. At that point it refreshes its course table with Fid assigned to goal D. The middle of the road hubs will forward the RREP to the source hub S.

At the point when S gets RREP, it confirms whether the stream personality of the RREP is its neighbor hub's character. In the event that it is along these lines, at that point it confirms all the security parameters in the RREP bundle. After this check, the source confirms the advanced security endorsement parameters of the middle of the road hubs. The parameters incorporate hub suggestion and hub proposition esteems. Group head keeps up the trust limit esteem in view of the trust dynamic and the hub proposition esteems to distinguish the assaults. In the event that the check succeeds then it utilizes its private key to decode the message and D's open key to distinguish the goal. Assist it will send the message with Fid.

3.2 Secret Sharing Procedure

In this technique, shares are created utilizing Shamir mystery sharing plan. Another arrangement of offers is built from the old offer by choosing an irregular polynomial Q with the end goal that Q(0) = 0. Let (S1, S2,...,Sn) be the offers of the mystery key S with the hub k having Sk, where Sk is characterized from a limited field D=Zr and g, a primitive component in people in general key F. Hub K ({1,2,3,… n} K) haphazardly produces Sk's sub shares like (Si1, Si2,... Sin) for (t,n) shares. All sub shares Skp({1,2,3,… n} P) is disseminated to hub p through the safe connection. At the point when hub j gets the sub shares {S1k, S2k, … ..Snk}, it figures another offer from these sub offers and its old offer with the accompanying condition

$$S_P^{'} = S_p + \sum_{k=1}^{n} S_{k_p}$$

Source S sends its mystery sharing banner M_start to all the investor hubs. All Share holder hubs send the M_start_ack banner to the next investor hub to start the sharing technique. The moderate hub sends the revive banner to all investor hubs. All hubs revive its offers S1, S2, S3 with the new sub shares S'p and send sub offers to other investor hubs with the computerized security endorsement and encoded open key of goal hubs.

3.3 Verify and authenticate the digital security certificate

The advanced mark is one of the security parameter incorporated into the computerized security endorsement of the hub. The advanced mark is checked to guarantee whether the offers are gotten from the confirmed hubs. Here, the general population key F, message m, signature (p,q) is utilized as the contribution of mark confirmation to approve the advanced security declaration. The mark (p,q) is the whole numbers in the middle of the interim [1,N-1]. Here N is the request of the framework. The encryption esteem is computed by,

$$e = H(m)$$

H denotes a hash function whose output has bit length not more than that of N. The integer value is calculated as

$$v = q^{-1} \bmod N$$

The whole number v is utilized to ascertain the estimation of request of N. It is utilized to confirm the mark of the q concerning request N of the framework. The u1 arrange of U is changed over to a whole number 1u and the esteem y = 1u mod N is resolved. On the off chance that q =s-1 (e+cp) (mod N) at that point the mark (p,q) is available on the message m which is created by the endorser (goal hub signature). The offers are then refreshed by reshuffling as takes after

z2c(modN) z1 vcp ve 1cp p 1e p cp) 1(e p s

In the event that y=p then the mark is acknowledged. In the event that this confirmation bombs, at that point the mark is rejected. The source sends end banner to all investor hubs. In the wake of accepting this end hail, it sends revive end banner to all investor hubs. At the goal, the mystery key is remade. On the off chance that Sk holds shares (m1, n1) and Sp hold shares (m2, n2), at that point the investor hub reproduces the mystery. In the event that m1 = m2, at that point the mystery is n1, generally the mystery is n2. This checked mystery shares can't be barged in by any of the black hole hub.

CONCLUSION

MANETs are for the most part made by a group of versatile hubs, interrelated through remote connections, which consent to team up and transmit each other's bundles. One of the principal thoughts for the outline of directing conventions in MANETs is that

each hub is trusted. On the off chance that a hub reports a connection disappointment, the connection will never again be utilized. This presumption can in a general sense help the plan and execution of steering conventions to acquaint a helplessness with a few sorts of Denial of Service (DoS) attacks. To dispatch this trouble making, a noxious hub can mindfully drop the steering parcels transmitted through it. This kind of bad conduct is for the most part alluded as black hole attack, which is considered as a standout amongst the most basic attacks that prompts the system fall. Because of the inadequacy of physical insurance and solid medium access component, black hole attack speaks to a genuine risk to the steering capacity in MANETs.

REFERENCES

[1] Cai, Jiwen,Yi, Ping,Chen, Jialin,Wang, Zhiyang, Liu, Ning , —An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network‖, IEEE International Conference on Advanced Information Networking and Applications, pp.275-280,April 2010.

[2] StanisławJarecki and NiteshSaxena, —On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol‖, IEEE Transactions on Information Forensics and Security, Vol. 5, No.4, pp.739-749,December 2010.

[3] Umang.S, Reddy.B.V.R, Hoda.M.N, —Enhanced Intrusion Detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption Communications‖, IET, Vol.4, pp.2084-2094, November 2010.

[4] Hongwei.L and P.Atam, —MOSAR: A secure on demand routing protocol for mobile multilevel ad hoc networks‖, International Journal of Network Security, pp.121-131, 2010.

[5] YibeltalFantahumAlem, Zhao HhengXaun, —Preventing Black Hole Attack in MANETs using Anomaly Detection‖,2nd IEEE International Conference on Future Computer and Communication(ICFCC), Vol.3, pp.672-676, May 2010.

[6] W.Kozma, and L.Lazos,—REACT:Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits‖, in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103-110, 2009.

[7] D.Djenouri, Mohamed Bouamama and OthmaneMahmoudi ,—Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks‖, International Journal of Security and Networks, Vol. 4, No.4, pp.246-262, 2009.

[8] LathaTamilselvan and Dr.V.Sankaranarayanan,—Prevention of Black hole Attack in MANET‖, Journal of Networks, Vol.3, No.5, pp.13-20,May 2008.

[9] D.Djenouri and Badache.N, —Struggling against selfishness and black hole attacks in MANETs‖, Journal of Wireless Communications and Mobile Computing, Vol. 8, No.6, pp.689-704, August 2008.

[10] K Liu, J.Deng, P.K.Varshney and K.Balakrishnan, —An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs‖, IEEE Transactions on Mobile Computing, pp. 536-550, May 2007.

[11] S. Kurosawa, H.Nakayama, N.Kato, A. Jamalipour and Y. Nemoto, —Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method‖, International Journal of Network Security , pp. 338-346, November 2007.

[12] N. Nasser and Y. Chen ,—Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks‖, in Proceeding of IEEE International Conference on Communication (ICC 07), pp.1154-1159, June 2007.

[13] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang, —Securing Mobile Ad Hoc Networks with Certificate less Public Keys‖, IEEE Transactions on dependable and secure computing, Vol. 3, No. 4, pp.386-399, December 2006.

[14] S. S. Ramaswami and S. Upadhyaya, —Smart handling of Colluding Black hole attacks in MANETs and Wireless Sensor Networks using Multipath Routing‖, in Proceeding of Workshop on Information Assurance, pp.253-260, June 2006.
[15] E. Altman, A. Kherani, P. Michiardi and R. Molva, —Non cooperative forwarding in ad hoc networks‖, in Proceedings of the 4th IFIP International Conferences on Networking, pp.486-498, May 2005.
[16] M. G. Zapata, —Secure Ad Hoc on-demand Distance Vector (SAODV) Routing‖, IETF Internet Draft,draft-guerrero-manet-saodv-03, 2005, accessed on 20 Jan 2013.
[17] Y. Zhang, W. Lou, W. Liu and Y. Fang, —A secure incentive protocol for mobile ad hoc networks‖, Wireless Networks Journal, Vol.13, pp.569-582, October 2007.
[18] D. Djenouri and N. Badache, —New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks‖, in Proceeding of Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecurComm‘05), pp.288-294, September 2005.
[19] Al-Shurman , S. M. Yoo and S. Park, —Black Hole Attack in Mobile Ad Hoc Networks‖, in Proceedings of 42nd Annual Southeast Regional Conference (ACMSE‘04), pp.96-97, April 2004.
[20] Sun.B, Guan.Y, Chen.J, Pooch.UW, —Detecting Black-hole Attack in Mobile Ad Hoc Networks‖, in Proceeding of 5th European Personal Mobile Communications Conference, pp.490-495,April 2003.
[21] A.Patcha and A. Mishra, —Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks‖, in Proceedings of Radio and Wireless Conference (RAWCON ‘03), pp.75-78, August 2003.
[22] S.Buchegger and J.Y.LeBoudec, —Performance Analysis of the CONFIDANT Protocol‖, in Proceedings of 3rd ACM International Symposium on Mobile Ad Hoc Networking and computing (MOBIHOC‘02), pp.226-236, June 2002.
[23] H.Deng, W.Li and D.P.Agrawal, —Routing security in wireless ad hoc networks‖, IEEE Communication Magazine, pp.70-75, October 2002.
[24] B. Schneider, Secrets and Lies.—Digital Security in a Networked World‖, John Wiley & Sons, Inc, 1st edition, 2000.
[25] S. Marti, T.J.Giuli, K.Lai and M. Baker, —Mitigating routing misbehavior in mobile ad hoc networks‖, in Proceedings of 6 th IEEE/ACM annual international conference on Mobile computing and networking (MOBICOM ‘00), pp.255-265, August 2000.
[26] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, —Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks‖, International Conference on Wireless Networks (ICWN‟03) ,pp.570-575, 2003.