Recognition and Anticipation of Wormhole Attack in ALARM Protocol (MANETs)

[1]Preetam Suman, [2]Amrit Suman, [3]Mohd. Amir Siddiqui, [4]Rupshi Jha

[1, 3] Computer Science Department, Integral University, Lucknow,

[2] Indian School of Mining, Dhanbad

[4]University of Cincinnai, Cincinnati, USA

Abstract- **Mobile Ad-Hoc Networks are picking up prominence to its crest today, as the users want remote availability regardless of their geographic area. There is an increasing danger of assaults on the Mobile Ad-hoc Networks (MANET) such as passive assaults and dynamic assaults. A detached assault does not irritate the functions of the system; snooping of traded information is finished by the assailant with no change of it. A dynamic assault endeavors to alter the information that have been exchanged in the system. In this manner this irritates the operations of system. Active attacks can be classified as: outside and inner assaults. Interior attacks are most capable assault on the grounds that these are the hubs that are entirely of the system which has all keys and approval. Wormhole assault is one of the active inner assaults in which two or more assailant hubs burrow the activity from one area to another area in the system.**

Anonymous Location-Aided Routing in suspicious MANET (ALARM) is a location based convention, gives assurance against detached assault, dynamic insider and active pariah assaults. The principle objective of ALARM convention is giving security and protection highlights in the MANET. Caution does not defeat the issue of wormhole assault and sink gap assault. This paper demonstrates the discovery and anticipation of the wormhole assault in the ALARM convention. Firstly call attention to which connection has wormhole burrow, then confirm really which connection is experiencing the wormhole attack. The effect of wormhole assault on the execution of ALARM is looked at. The results considered on the premise of throughput, bundle conveyance proportion and steering load in system.

Keywords- **ALARM protocol, Routing protocol, Wormhole attack and Location Aided Routing (LAR).**

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET)[6][8[9]] is an independent and dispersed wireless system. As the hubs in MANET are versatile, they are allowed to move in and out in the system. Hubs in a MANET may be mobile phone, portable PC, PDA, personal computer. MANET's hub can go about as host or switch or both in the meantime.

MANET is having capacity of self-arrangement and in view of that; they can be deployed quickly without the prerequisite of base station. System topology [14] of MANET is completely powerful in view of versatile hubs. In MANET, hubs are capable to communicate with one another with no current base. In right on time days Ad-Hoc examination was fundamentally concentrates on military systems, yet now Mobile Ad-Hoc networks can be utilized as a part of situations like gathering room, fiasco help, front line correspondence and it is additionally valuable, where organization of framework network is either immoderate or di religion. MANET is additionally helpful in situations such as search and salvage operations, vehicle systems, strategic systems, entertainment, sensor networks[16], military and law enforcement[17].Security in MANETs is the most critical sympathy toward the best possible usefulness of network. Due to its elements like open channel, progressively change topology, lack of focal security component, co-agent calculations and no powerful security instrument, MANETs oftentimes experience the ill effects of security assaults. These factors are huge issues in the MANETs against the security dangers. Because of nonappearance of brought together organization in MANET, hubs convey with each other on the premise of common trust. This normal for impromptu networks makes it more vulnerable towards security dangers and can be abused by an attacker in the system. Remote channel additionally makes the MANET more vulnerable to assaults; aggressor can go into the system and become acquainted with the information which is to be transferred. In MANETs, data must be transmitted in secure way. This is a challenging and di faction issue in light of the fact that, it uses open remote channel to transmit information. In order to avoid security assaults, the scientist must think about assaults can happen and their consequences for the MANET. In the MANET, assaults, for example, Wormhole assault, Black gap assault [20], Sybil attack[21], flooding assault, directing table assault, DoS, egotistical hub, mimic assault can occur. Correspondence is based on mutual trust and this makes MANET more delicate to these assaults.

II. MOTIVATION

Rapid Fast development of MANETs, because of value in different applications where security and protection saving systems administration operation MANET gets to be essential. This is principle motivation behind why MANETs assuming a fantastic part in numerous foundation less environments and applications, for example, Search and save operations, vehicle networks, strategic systems, excitement, sensor system, military and law enforcement. Now area data is effectively accessible through little and cheaper global situating framework (GPS) collectors. A transformative characteristic step is to receive such area based operation in MANETs. These outcomes in what then call area based MANETs. Security in MANET [10] is unavoidable sympathy toward the best possible working of system. MANET oftentimes experience the ill effects of security assaults on account of its components like open channel, framework less system, progressively change topology, absence of focal security instrument, co-agent calculations and no successful security mechanism. These variables are enormous issues in the MANETs against the security dangers.

III. ANONYMOUS LOCATION-AIDED ROUTING IN MANETS (ALARM)

Anonymous Location-Aided Routing in MANETs (ALARM) [4] has considered privacy-safeguarding secure correspondence in area based MANETs. It is proactive based steering convention. Caution gives solid protection and gives security properties in Mobile Ad-Hoc situation. Alert utilize hub's areas to securely propagate and assemble topology previews and send information. With the assistance of advanced cryptographic strategies like gathering marks, ALARM give both security and privacy furthermore gives hub verification, information uprightness, obscurity, and un-traceability. It additionally gives assurance against uninvolved assault and dynamic attack. This is first convention that offers security, protection, and execution tradeoffs in the upgraded connection state MANET steering. For security ALARM indicate how some advanced cryptographic methods can be utilized to accommodate them. The primary goal of ALARM convention is to avoid assaults, for example, inactive untouchable and passive insiders assault. Aloof insiders are most effective assaults on the grounds that they possess necessary cryptographic keys that used to decode directing control data.

A. *Bunch Signature*

Bunch signature [1] is a conventional open key mark which incorporates additional privacy highlights. In a gathering mark procedure, every gathering part has its own private key and a gathering open key. Every gathering part can sign a message, thereby creating a gathering mark. Check of gathering mark is done by anyone who has a gathering open key. A legitimate gathering mark infers that the signer is a substantial gathering part. In any case, it is computationally harder to figure out when two marks are given whether mark is produced by the same or different group individuals. At the point when arguments about a gathering mark occur, an uncommon group member called a Group Manager (GM) compellingly opens a gathering mark and recognizes who is the real underwriter. In light of this elements ALARM uses bunch signature for protection safeguarding. A gathering mark plan comprises of the following algorithms:

1) Setup: This calculation keeps running by the GM, and it yields a cryptographic condition for the gathering, including the gathering administrator's open and private keys.
2) Join: Join is convention between the GM and another client that need to join the group. The yield of this convention is gathering director's critical (its open membership key) and private yield for the client - its mystery participation key.
3) Sign: Sign is a calculation that executed by any gathering part for generating signature whose data comprises of: a message, a bunch's open key and a member's private key.
4) Verify: This calculation is executed by any gathering part for approval of the signature.
5) Open: This calculation, executed by the GM, when any question in signature occurs.
6) Revoke: This calculation is executed by the Group Manager to remove (revoke) a part from the gathering and to produce new gathering open key and other a set of bolster data.

B. *ALARM Basic Operation*

The essential strides in the operation of ALARM are as per the following

1) Initialization

The gathering supervisor (GM) begins the gathering mark plan and includes all valid MANET hubs as gathering individuals. At that point all part/hub makes a private key that is not presented to anybody. The private key is utilized to deliver a gathering signature. Each hubs additionally makes a comparing open key that is uncovered just to the GM. Bunch open key is known not individuals.

2) Operation

a). Time is isolated into openings of length T. Toward the start of every space, a node generates a provisional open private key pair: PK-TMPs and SK-TM, separately. Makeshift open is utilized by different individuals to scramble a session key.

b). All part show a Location Announcement Message (LAM) which contains its area (GPS co-ordinates), time-stamp,

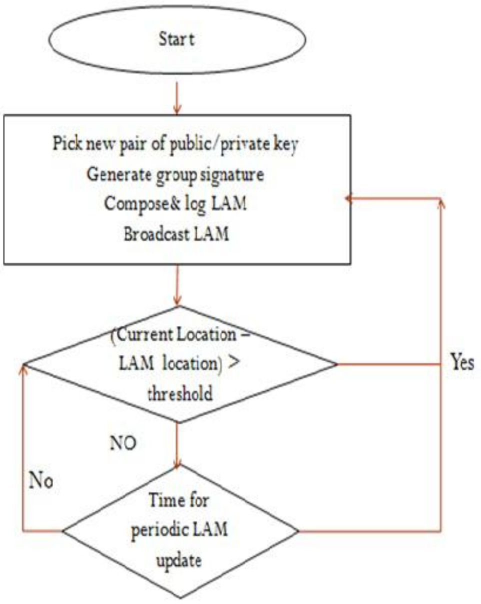
Start
Pick new pair of public/private key
Generate group signature
Compose& log LAM
Broadcast LAM
(Current Location – LAM location) > threshold
Yes
NO
No
Time for periodic LAM update

Figure 1: ALARM sender process flowchart

transitory open key (PKTMP's) and a gathering mark processed over these fields. LAMs are flooded throughout the MANET. This operation is appeared in the fig 1.

c). At the point when another LAM is gotten at the hub then hub first checks whether this LAM is gotten or not, if not, then confirms the group mark and the time-stamp. In the event that both are substantial, then LAM re-telecasts to its neighbors by the receiving hub. Furthermore gather every single current Lam of every hub then develop a geographical guide of the MANET and hub network diagram. Stream graph of this operation is given in fig 2.

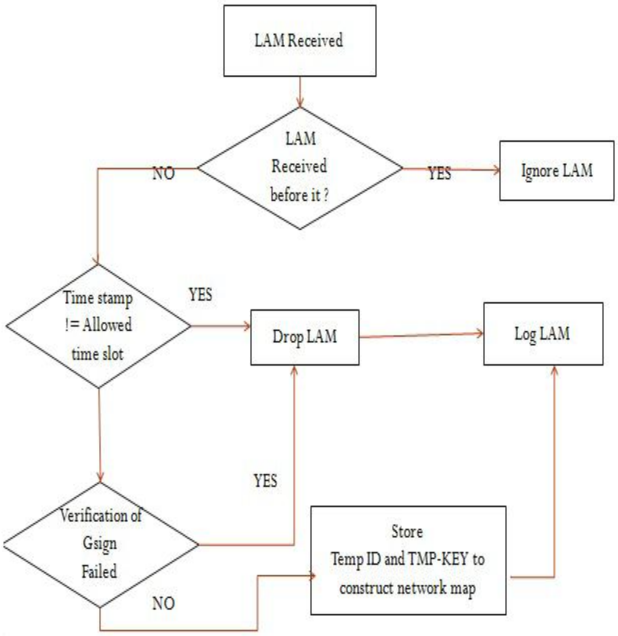
LAM Received
LAM Received before it ?
NO
YES
Ignore LAM
Time stamp != Allowed time slot
YES
Drop LAM
Log LAM
YES
Verification of Gsign Failed
Store Temp ID and TMP-KEY to construct network map
NO

Figure 2: ALARM LAM receiver process flowchart

d). On the off chance that any hub needs to convey to a sure area hub then it first checks if there is a hub at that area. Assuming this is the case, it transmit a message to the destination's present area and uses its interim ID (TmpID).The information is encoded with a session key and session key is likewise scrambled under the open key (PK-TMP), Destination's most recent LAM is incorporated with it. At the less than desirable end beneficiary hubs first decode the session key and afterward unscramble the message. This operation is appeared in the Fig 3.

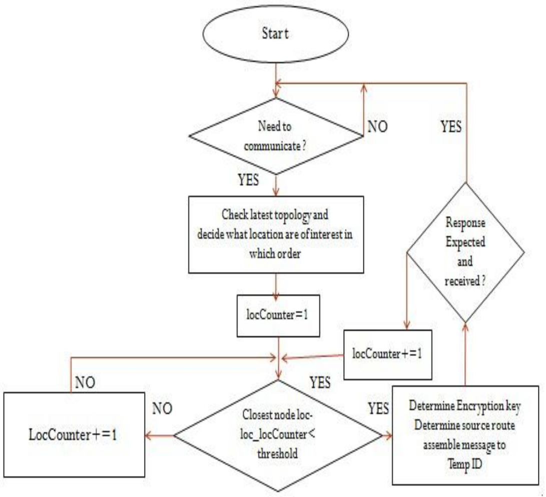
Start
Need to communicate ?
NO
YES
YES
Check latest topology and decide what location are of interest in which order
Response Expected and received ?
locCounter=1
locCounter+=1
NO
YES
NO
YES
LocCounter+=1
Closest node loc-loc_locCounter < threshold
Determine Encryption key Determine source route assemble message to Temp ID

Figure 3: ALARM communication decision Flowchart.

e). Sending: In the ALARM current topology, data disperses periodically on the premise of OLSR directing. Once every hub gets the whole topology view then it chooses whether (or not) to speak with a sure area node. Message sending is not reliant on the topology scattering.

IV. SECURITY ISSUES IN MANETS

Creating idiot proof security convention for MANETs [24] is intense assignment. This is mainly on account of certain uniqueness of Ad-hoc versatile system, specifically, common broadcast radio channel, shaky workplace, absence of focal administration and constrained accessibility of assets.

A. *Common Broadcast ratio channel*

Differently in wired systems where may be a solitary commit transmitting wire used between a two or more hubs yet in the MANET remote medium is utilized for communication which has TV nature and it is shared by all client nodes. So an assailant can undoubtedly discover information being moving in the system.

B. *Insecure working environment*

The working Environment where MANET systems are utilized may not always be secure like in the military system, hunt and save operation and fight fields. In such applications, hubs may join in and forget in the threatening and in secure area, where they would be very powerless to security dangers.

C. *Lack of central administrations*

In wired systems and base systems uses observing and movement control mechanism by uncommon essential issue, for example, base station, switch and get to points but in MANET there is no such main issue for executing this instrument.

D. *Lack of association*

MANETs is progressive in nature and hubs are portable. They at whatever time can leave and join the system. Hub confirmation systems are not there for joining new hub with a system so a malevolent hub can undoubtedly join the system and carryout its assaults.

E. *Limited Resource availability*

Asset, for example, transmission capacity, battery force, and computational force are limited in MANETs. So it is di religion to actualize complex calculation for security.

V. MANETS SECURITY ATTACKS

MANET's assault can be separation in real classes, as latent assault and active attacks. A uninvolved assault does not exasperate the elements of the system; snooping of traded information is finished by the aggressor with no alteration of it. This attack damages the secrecy furthermore examined the information that assembled by snooping. Detached assault is harder to identify in light of the fact that it doesn't an influence the network operation. This sort of assault can took care of by utilization of a powerful encryption calculation. A dynamic assault endeavours to adjust the information that has been traded in the system. Consequently this exasperates the operation of network. Active assaults are separated into two classes: outside and interior assaults, these assaults are appeared in the Fig 4. Inner assaults are most effective attack because these are the hubs that are quite of the system which has all keys and approval so it is hard to discover.

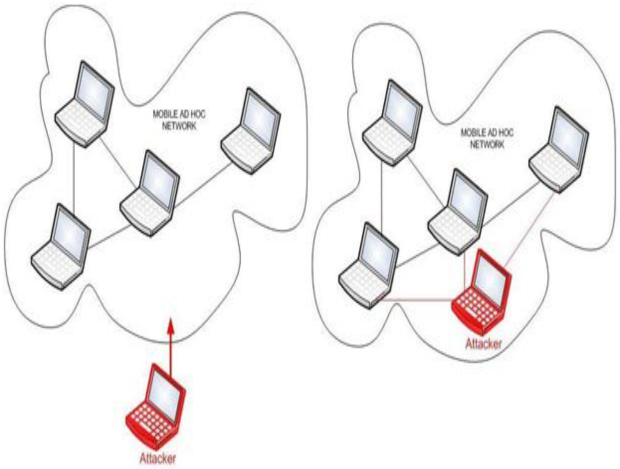

Figure 4: External and Internal Attacks in MANETs

VI. WORMHOLE ATTACK

In the wormhole assault, an assailant gets bundle at one area in the network and then passage to another area in the system [13]. This passage between two assailants hub is known as wormhole passage. It can be set up by a single long range remote connection or even by a wired connection included between the two attackers. Attacker makes the utilization of their area i.e. they have most brief way between the nodes as appeared in the Fig 5. They publicize their way letting alternate hubs in the system to know they have the briefest way for the transmitting their information.

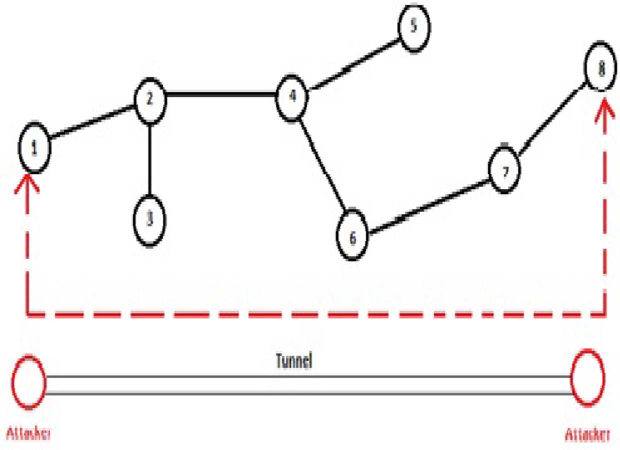

Figure 5: Wormhole attack

VII. RELATED WORKS

MANETs gets prevalence as a result of trademark, for example, system's dynamic topology, no framework and adaptability. Indeed, even with the truth of fame of MANET, these systems are all that much open to the assaults [22][12]. Radio channel also makes the MANET more helpless against assaults and make for the attackers to enter in the system and become acquainted with the proceeding with correspondence [2]. Several kinds of assaults have been concentrated on in MANET which influences on the network. Some assaults are similar to dark gap, where the assailant hub carries on perniciously for the time till the bundles are dropped and after that act typically [3]. MANETs routing protocols are additionally being dampened by the aggressors as flooding attack or DoS assaults, which is finished by the assailant by sending superfluous request packet [15].Every client needs its information to be sent secure and quick, numerous assailants, announce them-selves to have the most brief way and have high data transfer capacity for the transmission such as in wormhole assault and dark opening assault, gets bundle and toss it [18][7]. One of the constraints of MANET is the restricted battery, aggressors take a point of interest of this blemish and tries to keep the hubs occupied until it lost all energy and the hub go down [23]. Area based directing in ALARM protocol is more secure yet it has assault like wormhole and sink gap or dark gap attack [16][5]. This paper concentrates on the effect of Wormhole assault in Anonymous Location based steering in suspicious MANET (ALARM).

VIII. PROBLEM STATEMENT:

Beforehand the work done on security issues i.e. assault (Wormhole assault) involved in MANET depended on directing convention like Ad-Hoc On Demand Distance Vector (AODV) and proactive steering like OLSR. Wormhole assault is studied under the Location based directing convention like LAR and ALARM and its effects are investigated by expressing how this assault exasperates the execution of MANET. Very little consideration has been given to the effect of Wormhole assault in MANET. To think about the weakness impacts of wormhole assault on the ALARM protocols against the assault, there is a need to address the area based conventions as well as the effects of the assaults on the MANETs.

A. *Objective*

Objectives of this paper work are summarized as follow

1) To addressing so as to improve security in ALARM convention wormhole assault.
2) The study concentrates on examination of Wormhole assault in MANET and its outcomes.
3) Breaking down the impacts of Wormhole assault on premise of, Network burden, throughput and Packet conveyance Ratio in ALARM.
4) Recreating the Wormhole assault utilizing Proactive directing conventions

B. *Methodology*

In our writing review we came to realize that few methodologies have been developed to guard against wormhole assault in versatile specially appointed systems on that basis we have a procedure for discovery and counteractive action. Taking after calculation is utilized to detection and avoidance of wormhole assault.

1) Identification of Suspicious Links

In the Suspicious connection identification handle first we identify exceptionally plausible connection which is included in the assault. Idleness of wormhole is moderately more than the normal wireless spread inactivity. This condition is sufficient to recognize wormhole attack because inactivity relies on different variables like blockage and intra-nodal processing. So for suspicious connections location include two parcels: HELLOreq and HELLOrep and doing taking after steps.

a. Sent HELLOreq to neighbours and set the Timer.
b. At the getting a HELLOreq message, the collector must react with a HELLOrep message.
c. Check whether HELLOrep Packet is touched base before the clock out or not, if it got landed before time out, status of connection is set demonstrated generally set is suspicious.
d. Stop correspondence with that hub till the wormhole verification Flowchart of the suspicious connection discovery is appeared in the figure 6.

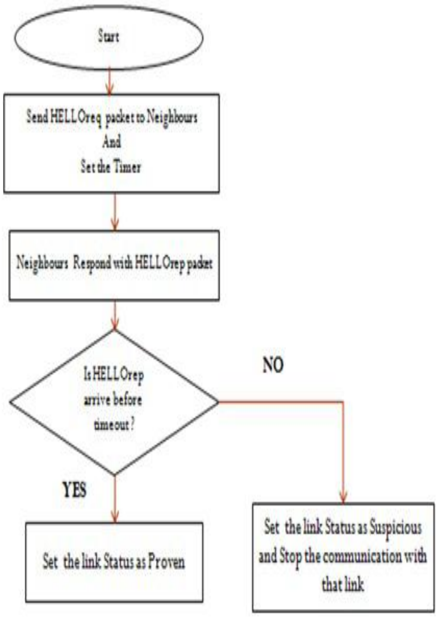
Start
Send HELLOreq packet to Neighbours And Set the Timer
Neighbours Respond with HELLOrep packet
Is HELLOrep arrive before timeout?
NO
YES
Set the link Status as Proven
Set the link Status as Suspicious and Stop the communication with that link

Figure 6: Flowchart of Detection suspicious Link

2) Wormhole Verification

In the confirmation strategy every connection checks whether there is wormhole attack or not between source hub and destination hub. For this two more bundle are added to convention specifically as PROBreq and ACKprob and do the accompanying steps:

a. Sends a PROBreq to the majority of its suspect hubs.
b. Collector answers with an ACKprob and it is likewise includes its own supposition about the status of hub of sender.
c. Sender again checks whether the ACKprob touched base before the timeout and also chooses status about conceivable suspicious connections.
d. Sender thinks about its consequence of the status of the other endpoint of the suspicious link with the other hub's aftereffects of its own status:

- If(Proved, Proved):If the assessment of sender is demonstrated and substance of ACKprob is additionally demonstrated Then there is no Wormhole burrow.
- If(Suspicious, Proved) or (Proved, Suspicious): Repeat the above procedure after an arbitrary sum time. In the event that again one of them is Suspicious then regards this connection as a wormhole burrow.
- If(Suspicious, Suspicious): If status of remote hub is suspicious, originator's status likewise Suspicious this presumes the connection contains a wormhole tunnel.

C. Implementation & Scenario:

Target of this situation is to perform and avert wormhole assault on ALARM convention then gather ALARM related insights and break down the system element changes. Alert is as proactive steering convention and uses multi-point hand-off (MPR) streamlining for controlled flooding and operations. In the ALARM convention when wormhole assault is propelled amid the spread of connection state bundles, the wrong connection data flows all through the system, prompting steering disturbance. For the recreation study done on base of execution parameter like PDR (bundle conveyance proportion), Network Throughput, Packet lost and Network Load.

1) Simulation Scenario

Figure 7 and table 1shows the recreation setup of a situation there is 30 hubs. Number of hubs is settled and reproduction time has taken 100 seconds. Recreation zone taken is 800 x 600 meters. Transmission Rage 100 meters.

In the figure 8, topology information is transmitted to within nodes and routing table updated. ALARM protocol is a proactive routing protocol, so MPR node periodically updated the topology information to its neighbour.

TABLE I
SIMULATION PARAMETERS

Simulation Parameters	
Protocols	ALARM protocol and OLSR
Simulation time	100 seconds
Simulation area (m x m)	800x600
Number of Nodes	30 (Number as 0-29)
Traffic Type	TCP, CBR and UDP
Performance Parameter	Throughput, PDR , Packet Lost and Routing Load of the network

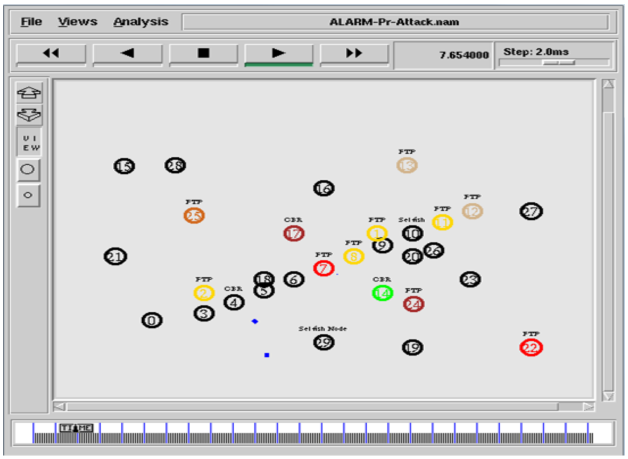

Figure 7: Simulation topology

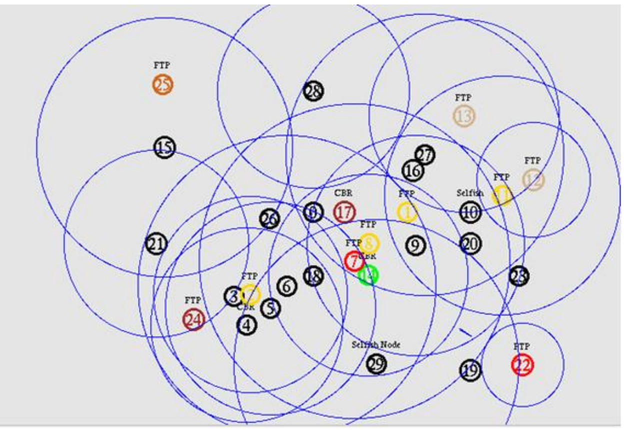

Figure 8: Dissemination of Network traffic information topology

IX. RESULTS

Here the comparison of the behavior ALARM convention on the off chance that without Wormhole assault, with Wormhole assault and after the counteractive action of wormhole assault, then considered the execution measurements of Packet Delivery Ratio (PDR), Network throughput, Packet lost and Network load.

A. Packet Delivery Ratio (PDR)

Parcel Delivery Ratio is characterized as it is proportion between no. of parcel got to no. of bundle transmitted in the system. Fig. 9 demonstrates a chart in which comparison of PDR is given among the ALARM, ALARM with Wormhole assault and after Prevention of Wormhole assault. In the diagram at Y hub PDR in rate and X axis demonstrates the time in second. PDR is less contrasted with without wormhole attack. In instance of wormhole assault most extreme parcels are either dropped or transmitted anywhere in the system so add up to no. of parcel got bundle is less think about to without wormhole.

B. Network Throughput

System Throughput is second parameter of our study. Throughput is the average rate of effective bundle conveyance over a correspondence divert or successful packet conveyance in per unit time or every second. System throughput is decreased in instance of assault on the grounds that wormhole gets parcel from one area and passage it to in the system, so effective bundle conveyance perishes. Throughput of system enhances when apply wormhole recognition and anticipation procedure (appeared in the figure 10).

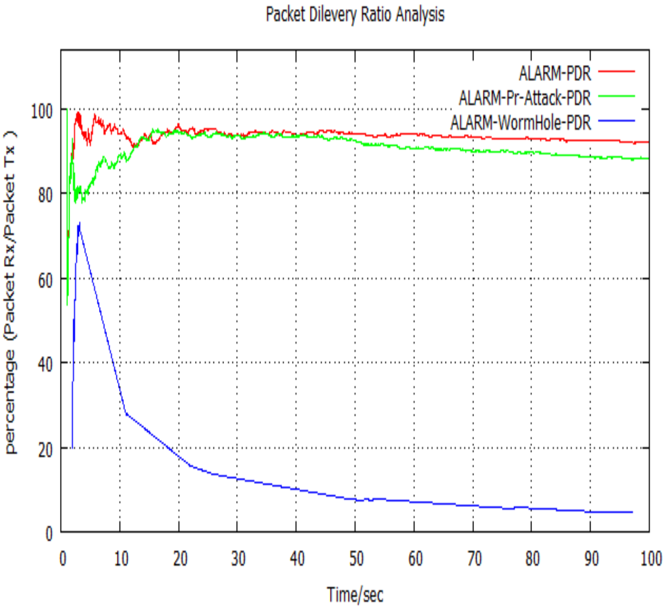

Figure 9: Packet Delivery Ratio (in percentage)

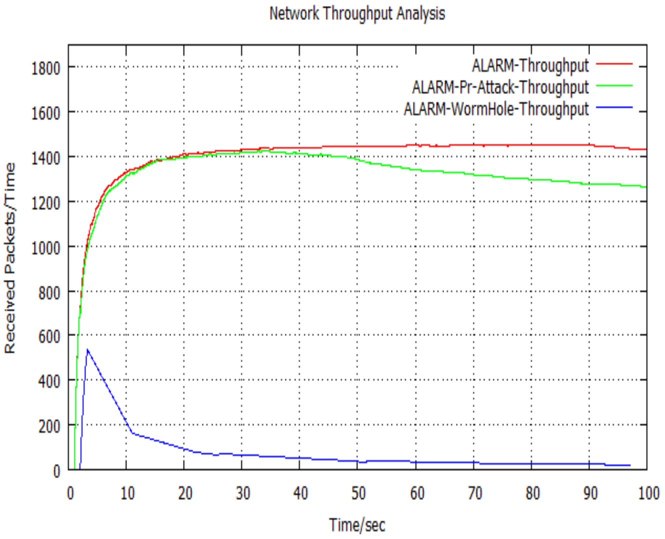

Figure 10: Network Throughput (packet/sec)

C. Network Load

Burden alludes to measure of information or movement being conveyed by the system, or total number of parcel got by whole system. System Load diagram of ALARM, ALARM with assault and without assault is appeared in figure 11.The system load of ALARM in the event of assault is much high as contrast with ALARM without attack. After the avoidance of assault system burden minimizes yet at the same time more noteworthy than ALARM without assault in light of the fact that in wormhole discovery and anticipation strategy present four new parcels.

D. Packet Loss

In the figure 12 an examination diagram of bundle misfortune in the event that ALARM with and without attack and after counteractive action of Attack appeared. Parcel misfortune rate if there should arise an occurrence of attack is high, it is minimized in the assault counteractive action handle yet it is still more as compare to typical ALARM.

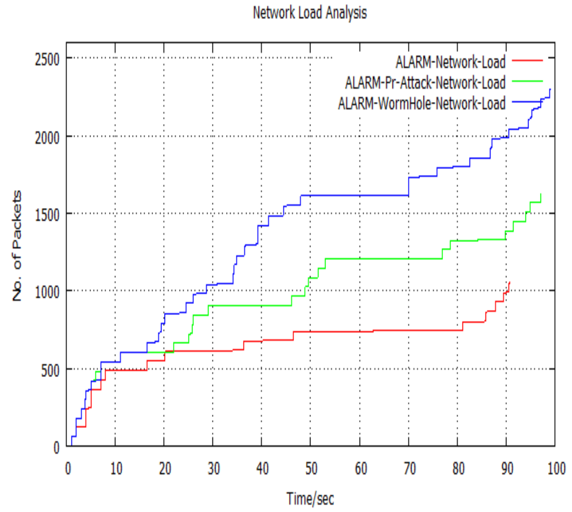

Figure 11: Network Load

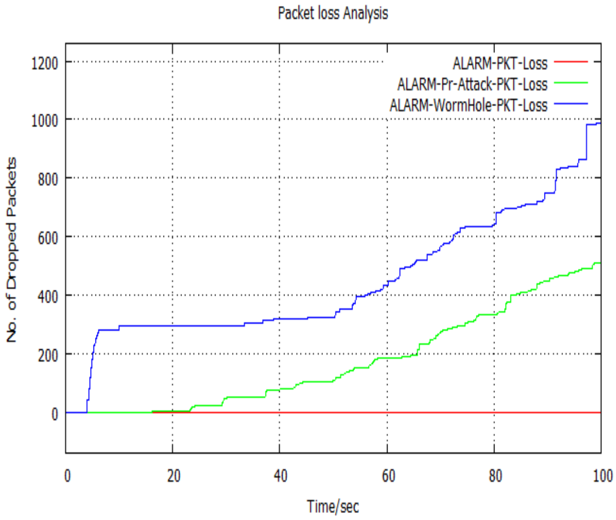

Figure 12: Packet loss in the network

X. CONCLUSION

Mobile Ad-Hoc Networks could be conveying in environment where wired network or framework based system can't in any way, shape or form be sent. With the importance of MANET and its colossal potential it has still numerous difficulties to overcome. MANET Security is a standout amongst the most vital prerequisite its arrangement and development. There are numerous dangers of security one of them is wormhole attack. Wormhole assaults are fierce assaults that can without much of a stretch be propelled in any system even systems has solid classification and validness component.

In this paper first perform wormhole assault at area based protocol (ALARM) then identify and recoup the wormhole assault furthermore investigate the behavior of convention with assault and without assault. The Analysis is done on basis of system throughput, Packet conveyance proportion, parcel dropped rate and the network load.

REFERENCES

[1] G. Ateniese and G. Tsudik. Some open issues and new directions in group signatures. In Financial Cryptography, Pages 196-211. Springer, 1999.

[2] K. Biswas and M. Ali. Security threats in mobile ad hoc network. University essay from Blekinge Teknisha Ho Gskola/Sektionen for Teknik (TEK), 2007.

[3] O. Chandure and V. Gaikwad. A mechanism for recognition & eradication of grayhole attack using aodv routing protocol in Manet.

[4] K. Defrawy and G. Tsudik. Privacy-preserving location-based on-demand routing in Manets. Selected Areas in Communications, IEEE Journal on, 29(10):1926-1934, 2011.

[5] K. Defrawy and G. Tsudik. Privacy-preserving location-based on-demand routing in Manets. Selected Areas in Communications, IEEE Journal on, 29(10):1926-1934, 2011.

[6] P. Garg and A. Tuteja. Comparative performance analysis of two ad-hoc routing protocols. In Proceedings of 2011 1st International Conference on Network and Electronics Engineering (ICNEE 2011), 2011.

[7] S. Gupta, S. Gill, and A. Joshi. Analysis of black hole attack on aodv and olsr routing protocols in Manet.

[8] D. Johnson, D. Maltz, Y. Hu, and J. Jetcheva. The dynamic Source routing protocol for mobile ad hoc networks (dsr), July 2004. URL http://www.ietf.org/internet-drafts/draft-ietf- Manet-dsr-10. txt. Last visited, 10, 2005.

[9] J. Kim and G. Tsudik. Srdp: Securing route discovery in dsr. In Mobile and Ubiquitous Systems: Networking and Services. The Second Annual International Conference on, pages 247-258. IEEE, 2005.

[10] Y. KO and N. H. Vaidya. "Location-aidedroiuting (lar) in Mantes". Pages 66-75. Proc. ACM MobiHoc, Oct. 1998.

[11] S. Murkowski, T. Camp, N. Mushell, and M. Colagrosso. A Visualization and analysis tool for ns-2 wireless simulations: Inspect. In Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2005. 13th IEEE International Symposium on, pages 503-506. IEEE, 2005.

[12] S. Lu, L. Li, K. Lam, and L. Jia.Saodv: a Manet routing protocol that can withstand black hole attack. In Computational Intelligence and Security. International Conference on, volume 2, pages 421-425. IEEE, 2009.

[13] H. Nguyen and U. Nguyen.A study of different types of Attacks on multicasting mobile ad hoc networks. Ad Hoc Networks, 6(1):32-46, 2008.

[14] A. Perrig, R. Canetti, J. Tygar, and D. Song. The tesla broadcast authentication protocol. 2005.

[15] M. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy. A Reputation-based mechanism for isolating selsh nodes in ad hoc networks. In Mobile and Ubiquitous Systems: Networking and Services. The Second Annual International Conference on, pages 3-11. IEEE, 2005.

[16] J. Ren, Y. Li, and T. Li. Spm: source privacy for mobile ad hoc networks. EURASIP Journal on Wireless Communications and Networking, 2010.

[17] R. Shah and J. Rabaey. Energy aware routing for low energy ad hoc sensor networks. In Wireless Communications and Networking Conference, IEEE, volume 1, pages 350-355, 2002.

[18] N. Song, L. Qian, and X. Li. Wormhole attacks detection in wireless adhoc networks: A statistical analysis approach. In Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, IEEE, 2005.

[19] Y. Sun, S. Kumar, and A. Jantsch. Simulation and evaluation for a network on chip architecture using ns-2. In 20th IEEE Norchip Conference.Citeseer, 2002.

[20] I. Ullah and S. Rehman. Analysis of black hole attack on Manets using different Manet routing protocols. Program Electrical Engineering with emphasis on Telecommunication, Type of thesis-Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698, 2010.

[21] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.

[22] A. Vani and D. Rao. Article: Providing of secure routing against attacks in Manets. International Journal, 24:16-25.

[23] D. Westhoff. Method for authentication, Sept. 13 2006. US Patent App.11/519,929.

[24] H. Yih-Chun and A. Perrig. A survey of secure wireless ad hoc routing. Security & Privacy, IEEE, 2(3):2839, 2004.