www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 4. March 2015

Prevention of Black Hole Attack in an Anonymous Communication

[1]T.Sindhu, [2]R.Kalaivani Sri,
[1]M.E., Computer Science Engineering
[2]Assistant Professor, Arunai College of Engineering
[1]Sindhunit100792@gmail.com, [2]Saikalai25@gmail.com

Abstract— Mobile ad hoc protocol concede nodes with wireless adapter to communicate with one another without existing infrastructure. At escalation of mobile ad hoc network, a device establishes to evoke lamentable heed specially a potential target for malevolent activities. Nodes in MANETs are not aim to tamper and examine data and traffic analysis by commune intrudes or assails routing protocols. By intrude the adversary nodes can analyze any routing protocol and procure information about the communication packets in their vicinity and locale of other nodes in the network. So, MANET uses anonymous location based efficient routing protocol (ALERT) that dubious originality and/or route from outside onlooker. ALERT vitally exclude the network field into zones and arbitrary choose node in zones as intermediate relay nodes, which form a non traceable unidentifiable route. It resilient to intersection attacks and timing attacks. However, this protocol does not support security to black hole attack. In black hole attack, an adverse node uses its routing protocol in order to promulgate itself for having the minuscule track to the target node. By incorporating apriori algorithm in ALERT protocol, we avert from black hole attack by enacting intercession with neighbours who assert to preserve a route to destination.

Keywords— MANET, Traffic analysis, eavesdropping, black hole attack, apriori algorithm

I. INDRODUCTION

Mobile ad hoc networks (MANET) are sovereign and decentralized wireless system. The nodes in MANET's progress independently in any direction and an interrelation between the devices transmute repeatedly. Nodes in a MANET may be mobile phone, laptop, and PDA. These nodes can act as host/router or both at the same time. They can construct erratic topologies depend on their connectivity with each other in the network. These nodes have the capability to arrange themselves and because of their self configuring ability they can establish urgently without entail of any infrastructure. MANET's are discovering escalate approach in both defense and non-combatant system owing their self configuring and self prolongation potentiality.

Fig.1 Mobile Adhoc Network (MANET)

Collateral in MANET is the most significant concern for the rudimentary functionality of network. MANET's often suffer from security attack because of its trait like unsecured medium, adapting its topology dynamically, absence of control monitoring and proprietors, collaborative algorithm and no lucid guarding mechanism. Traffic analysis is one of the most subtle and unsolved safety assail against MANET's.

Anonymous location based efficient routing protocol(ALERT) are pre-eminent in MANET's to provide reliable conveyance by hiding node uniformity, locality and thwarting traffic analysis attacks from external spectator. Anonymity in MANETs incorporates identity and location anonymity of data origin and targets as well as route anonymity. ALERT dynamically severance into a network field into precinct and randomly selects nodes in zones as intermediary relay nodes,

which form a non traceable incognito route. In each routing step, a data sender or forwarder segregate the network field in order to disparate itself and the destination into zones. It then randomly chooses a node in the other zone as the next relay node and uses AODV algorithm to send the data to the relay node. Then the data is transmitted to provisional destination nodes in the destination zone, providing anonymity to the targets. ALERT is also supple to intersection attacks and timing attacks. Howbeit, it does not protect a node from black hole attack. In this paper, we incorporating apriori algorithm in ALERT to prevent black hole attack. Black hole alludes to locale in the network where succeeding traffic is descended without informing the source that the data did not extend its intended receiver. Black hole attack is a sort of Denial of Service. In this attack, a malignant node uses the routing protocol to proclaim itself as having the shortest route to the node whose packets it wants to obstruct and in this way it trade-off the service.

II. RELATED RESEARCH

MANET is very much admired by people due to the fact that these networks are vital, configuration less and scalable. In spite of the fact that support of MANET, these networks is very much revealed to attacks. Different kinds of attacks have been inspected in MANET and their influence on the network. In this section we present an overview of exploration in MANET which looks on geographical routing and black hole attack. A lot of different approaches have been implemented to prevent black hole attack.

A. Anonymous Routing

Karim Defrawy et al., [5] have proffered a procedure for Anonymous Location-Aided Routing in MANETS (ALARM) that exhibits the viability of concomitantly procures powerful solitude, and security properties, with sensible organization. Even though it might seem that their security and privacy properties dispute each other, they show that some advanced cryptographic techniques can be used to reunite them. This protocol offers protection against both passive and active insider, outsider attacks.

Karim El Defrawy et al., [6] have proposed on-demand location-based anonymous MANET routing protocol (PRISM) that attain privacy and security against both outsider and insider rivals. The PRISM protocol which aids an anonymous reactive routing in cynical location-based MANETs depend on group signatures to validate nodes, ensure probity of routing messages while preventing node tracking. This protocol employs not only with any group signature strategy but also with any location-based forwarding procedure.

A Mix zone [12] is an anonymous location service that discloses the locality of mobile users in a long time period in order to prevent users' motion from being trailed. Each position appraised of application that can observe nodes' locations relates with some zones but remain unregistered; these users' location changes are untraceable in the zones.

B. Malicious Node Detection

The CORE protocol [15] proposed by Michiardi *et al*., uses three reputations (subjective, indirect and functional). This mechanism uses reputation table to conserve the reputation value for each node and the watchdog mechanism to observe that a vital purpose is fulfilled by the solicit node or not. The reputation is defined on direct scrutiny and on the foundation of details furnished by distinct nodes. The reputation value will promote a node to determine the self-regard of an invocation node and eventually guide whether to perform or to diminish ARM [2], Anonymous on demand routing scheme for MANET is a systematic result that provides anonymity in a stronger opponent model. The adversaries are an outer universal submissive adversary who can monitor all possible communications between all nodes in the network at all time and a collaborate node inside the network, possible adversary. It prevents global tractable adversary from learning the destination of the messages and which nodes are parts of the path from the source to the destination. It prevents a cooperating node from not being able to determine whether another node in the network is the sender or the destination of a particular message and from not being able to determine whether another node is part of a path between two nodes.

C. .Cooperation of Nodes

The CONFIDANT protocol suggested by Buchegger *et al*. [15], in which the first module called Monitor that is liable for perceiving and inscribing the delinquency of neighbouring nodes. The second module the reputation system is organized for computing the reputation of nodes on the robustness of direct observation and indirect observation. The third module trust manager is gathers caution messages from friends, and finally the fourth module the track manager defines the path for routing by rejecting a selfish node. In this protocol, each node monitors its neighbourhood behaviour and observed misbehaviour is reported to the reputation system. If the misbehaviour is not manageable then it is reported to the path administrator, and then the path manager excludes the nodes from the routing path and computes new paths. This method has delicacy due to unstable estimation difficulty, for the reason that every node has dissimilar evaluations for the same node and has arduous to recognize correct selfish

node. Another limitation is in terms of more battery power utilization of a node which is tracked at the centre of network in analogy to situated at the fringe of the network.

III. An Anonymous Location-Base Efficient Routing Protocol

A. Networks and Assail Representation

ALERT can be implemented in disparate network replica with diverse node gesture patterns such as random way point model and group mobility model. Consider a MANET locates in a massive field where geographic routing is used for node transmission in order to minimize the communication latency. The locality of a communication sender may be disclosed by solely revealing the transference route. Consequently, an anonymous communication protocol that can dispense intractability is required to strictly establish the anonymity of the sender when the sender transfers with the other side of the field. Furthermore, a malevolent spectator may attempt to restrict the data packets by understanding a number of nodes, obstruct the packets on a number of nodes, or even find the sender by recognizing the data transmission path. Hence, the route should also be imperceptible. A malignant spectator may also try to perceive destination nodes through traffic analysis by injecting an intersection attack. It also provides anonymity of the destination zone by hiding exact location of the destination node

B. Random Incognito

In ALERT, all nodes employ a random pseudonym as its node identifier instead of using its actual MAC address, which can be used to discover nodes' extant in the network. To circumvent pseudonym smash, we use a collision repellent hash function, such as SHA-1, to hash a node's MAC identifier and contemporary time stamp. To prohibit an attacker from computing the pseudonym, the time stamp should be sufficient. To further make it more strenuous for an attacker to compute the time stamp; we can increase the computation complexity by using randomization for the time stamps. A node's pseudonyms become invalid after a specific time period in order to thwart opponent from identifying the pseudonyms with nodes. If pseudonyms are changed too constantly, the routing may get disturbed; and if pseudonyms are changed too infrequently, the opponent may relate pseudonyms with nodes over pseudonym changes. Therefore, the pseudonym prearranged. Each node at fixed intervals piggybacks its revised position and pseudonym to "hello" messages, and sends the messages to its nearby nodes. Also, each node sustains a routing table that keeps its neighbours' pseudonyms related with their location.

C. The ALERT Routing Algorithm

ALERT is a dynamic and random routing trail, which contains a number of dynamic intermediate relay nodes. As shown in Fig.2, we horizontally separate a nodes it into two zones A1 and A2. Again it has vertically segregated a zone A1 to B1 and B2. After that, horizontally parting zone B2 into two zones. Such zone splitting consecutively diverge the trivial zone in an alternating horizontal and vertical manner. This process is called as hierarchical zone partition.

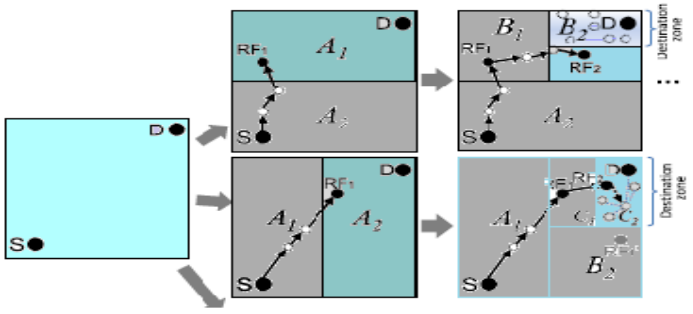

Fig.2 Zone partition

ALERT uses the hierarchical zone segregation and randomly selects a node in the segregated zone in every action as an intermediate relay node, thus dynamically provoke an uncertain routing path for a message. A Fig. 3 exhibits an example of routing in ALERT. The zones possess k nodes where D inhabits the target zone, represented as ZD. K is used to authority the standard of anonymity security for the destination. The darken zone in Fig. 2 is the destination area. Particularly in the ALERT routing, each data source or forwarders accomplish the hierarchical zone partition. It first inspects whether itself and destination are in the same zone. If so, it splits the zone alternatively in the horizontal and vertical routes. The nodes reiterate this procedure until itself and ZD are not in the same zone. It then randomly selects a location in the other zone called temporary destination

(TD), and uses the AODV routing algorithm to forward the data to the node adjacent to TD. This node is described as a random forwarder (RF).

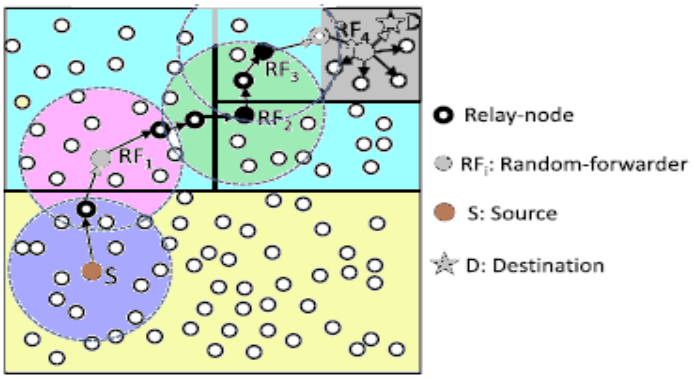

Fig.3 Routing among zones in ALERT

D. The Destination Zone Position

Zone positions allude to the top left and bottom-right coordinates of a zone. One difficult is how to discover the position of ZD, which is required by each packet forwarder to examine whether it is separated from the destination after segregation and whether it occupies in ZD.

IV. ANONMITY PROTECTION

A. A. Anonymity Safety

ALERT provides originality and location anonymity of the source and destination, route anonymity effectively. Disparate, geographic routing which invariably takes the shortest route. ALERT establish the route between a S-D pair strenuous to locate by arbitrarily and effectively choosing the relay nodes. The determined dissimilar routes for a communication between a specified S-D pair construct rigid for an intruder to discover a statistical pattern of communication. Owing to fact that RF set alters due to the random assortment of RF for the time of transmission of all packets. Even if an intruder discovers all the nodes through a route once, this observation does not assist it in finding the routes for following transmissions between the same S-D pair. Furthermore, since a RF is only conscious of its originate node and arrived node in path, the source and destination nodes cannot be distinguished from other nodes en route. Also, the anonymous route between S and D fortify that nodes on the route do not realize where the endpoints exist. ALERT nourishes the seclusion security for S and D by the unrelated of the transmission endpoints and the transmitted data. It means that, S and D cannot be related with the packets in their communication by opponent.

B. B. Source Anonymity

ALERT bestow to the procurement of anonymity by hindering a node's visibility solely to its vicinal and concocting the same rudimentary and forwarded messages. It forges arduous for an intruder to apprise if a node is a source or a forwarding node. To sturdiness the anonymity hinders of the source nodes, we furthermore proffer a diaphanous implementation called "notify and go." Its pivotal design is to let a number of nodes dispatch the packets at the same time as S in order to shroud the sender packet amidst multiple distinct packets.

C. C. Resilience to Timing attacks

In timing attacks, through packet egress time and advent time, an intruder can discern the packets dispatch between S and D, from which it can eventually discern S and D. For exemplar, two nodes A and B liaise accompanied by other at an interval of 5 seconds. After a prolonged scrutiny time, the intruder realize that A's packet consign time and B's packet accrue time have a stable five second difference. Then, the observer would reckon that A and B are commune with each other. Circumventing the spectacle of interaction between commune nodes is a way to counter timing attacks. In ALERT, the "notify and go" implementation and promulgate in ZD both put the communication between S-D into two sets of nodes to obscure intruders.

D. D. Resilience to Intersection Attacks

In an intersection attack, an assailant with knowledge regarding mobile users at a stated time can govern the sources and destinations that transmit with each other along recapitulate inspection. Intersection attacks are familiar obstacle and have not been well reconcile. Although, ALERT proffer k-anonymity to D, an intersection attacker can still recognize D from replicated scrutiny of node manoeuvre and communication if D invariably remains in ZD for the time of transmission session as long as D is orchestrating communication, an intruder can observes the revamp of an adherent in the destination zone incorporating D. As time progress and nodes proceed, all variant members may move out of the destination zone exclude D. As an outcome, D is recognizing as the destination because it repeatedly visible in the destination zone. An assailant may grasp and scrutinize packets; the hindmost forwarding node amends a number of bits in every packet to intercept the attacker from discern uniform packets in one broadcasting.

V. APIRORI ALGORITHM

Apriori algorithm is the most frequently used association rule finding algorithm although it employs the recurrent sets. Apriori algorithm utilizes the downward closure property and benefit of the method is that provide a prior perusal the database at all extent. Also it amenable prunes divergent sets, which ensure implausible to be perennial sets. Apriori algorithm has become a referral procedure and has been revamped in divergent ways in appellation of time complexity, scans of the nodes, size of negotiation, threshold When a node suspicion on rectitude of a vicinal node, it instigate an acumen procedure and it has strengthened this process by Apriori algorithm.

APRIORI ALGORITHM

1. Initialize: k:=1,C_1=all the 1-itemsets;
2. read the traffic bit-matrix to count the Support of C_1 to determine L_1
3. **while** $L_{k-1}\neq\emptyset$ **do**
4. C_k= gen-candidate-itemsets with the given L_{k-1}
5. *Prune*(C_K)
6. **end while**
7. L_1:={frequent 1-itemsets};
8. K:=2; *// k represents the pass number*
9. **for** all rows $\in$ bit-matrix **do**
10. increment the count of all candidates in C_k that are contained in r;
11. L_k:= All candidates in C_k with minimum Support;
12. K:= k+1
13. **end for**
14. Answer L:=$U_K L_K$;

Table.1 Apriori Algorithm

A malignant node dispatch respond packet to each accepted route request and it receives data packets and merely detach them. To discover malign nodes, member nodes should observe their neighbours with transcribing number of RREQ, RREP, obtained and forwarded data packets. When a member node reckon on another node, it sends an appeal to gather registered data of other members. Requester generates a database from congregated information and Apriori algorithm is used to deduce malevolent nodes. Any node could enact Apriori algorithm to reckoning about integrity of initiator of reply packets. But movement of a node in a network show its moral. To produce a suitable acumen about integrity of a node, every node has to record the declared statistics. Every member node observes neighbour node's movement. It registers the required data to fill fields of judge table. Although each node upon acquire a RREP packet from a nearby node; computes level of integrity for nearby node.

VI. SIMULATION RESULTS

It exhibit how Apriori algorithm is used on malignant nodes from recorded data of MANET nodes. The simulation is accomplished by NS2. Parameters used in the simulator are summarized in Fig5 and Fig6. Hundred nodes are assigned randomly in the simulation zone of 1000 × 1000 m^2 and with a 250 m communication scale for each node. The Propagation replica of the communication is "Two Ray Ground". The channel ability is 2 mbps. The random mobility method of the nodes is produced by the CMUs node motion service "setdest" with diverse Node Mobility Speeds (NMS) within the span of 5-30 m/s. The nodes do not proceed throughout the simulation time, i.e., they terminate according to a sustained pause time parameter, which lasts for one second. The packet magnitude is 512 bytes.

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 4. March 2015

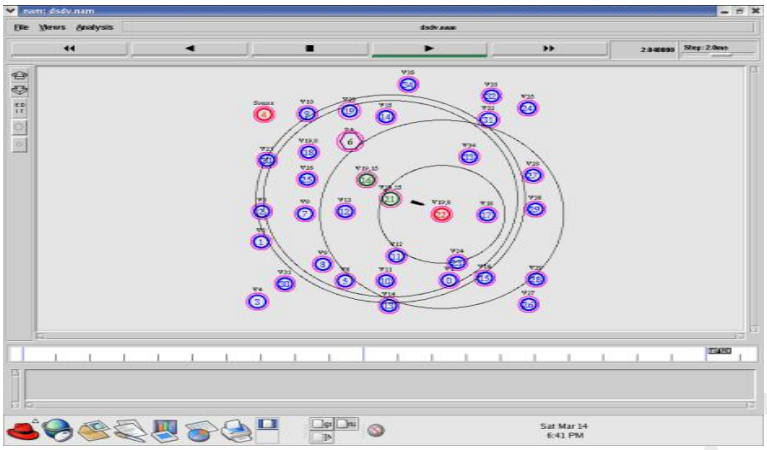

Fig.4 Prevention of Blackhole attack

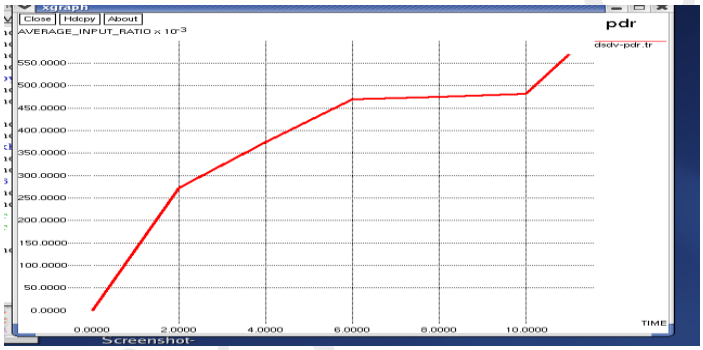

Fig.5 Packet delivery ratio

Fig.6 Throughput

VII. Conclusion and Future Work

In this paper, the routing safety issues of MANETs have been described and one type of assault, the black hole, which could be smoothly established against the MANET, has been reported. In this paper, an apriori algorithm has been propounded to locate and intercept black hole attacks in MANETs with low complexity. In addition, it proffers a security from flooding attacks. Future works could be strenuous on ways to minimize detain in the network and to acquire further enhancement.

References

[1] A.Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonomity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[6] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[8] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[10] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[11] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

[12] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[13] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[14] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[15] Sonja Buchegger and Jean-Yves Le Boudec. "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes — Fairness In Dynamic Adhoc Networks". Proc. Of IEEE/ACM MobiHOC, 2002.

[16] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce

[17] node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

.

Authors Short Profile:

T.Sindhu received her Bachelor's degree in Computer Science and Engineering from Sri Nandhanam College of Engineering and Technology, Anna University, Chennai in 2013, and currently she is on the verge of completing Master's Degree program (2013-2015) in Computer Science and Engineering from Arunai College of Engineering, Anna University in 2015. Her area of interest includes Ad hoc networks, Network Security and Mobile Computing.

Mrs.R.Kalaivani Sri, M.Tech, received her B.E. degree in Computer Science and Engineering from Annamalai University in 2007, and the M.Tech degree from Prist University in 2013. She is an Assistant Professor in Arunai College of Engineering. Her research interests include Network Security, Cloud Computing and Artificial Intelligence.