IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Detection of Unavailability and Black hole Attack over ALERT protocol in MANET

Akshay Jaitpal[1], Pavan Kodihal[2], Pratik Gothiwadekar[3]

Computer Dept. DYPIET, Pune University, India[1, 2, 3]

Abstract: MANET (mobile ad hoc network) is a wireless, infrastructure-less mobile network. Every device in a MANET can move omnidirectional. Mobile Ad-Hoc Network (MANET) uses anonymous routing protocol for security purpose. ALERT protocol hides nodes original identity from an intruder, so that the observer cannot threaten the security of the network. There are few prevailing anonymous routing protocol available for MANET. The protocols such as ASR, AO2P, ALARM provides node anonymity, but these protocols do not provide route anonymity. ALERT protocol dynamically divides the partition into zones. Every zone has nodes which act as intermediate nodes. The nodes get randomly selected for routing so that the observer cannot identify the route. ALERT provides source, destination and route anonymity using pseudonym which changes frequently. ALERT also has a strategy against timing attacks, Blackhole attacks.

Keywords: Mobile Ad-Hoc Network, Anonymity, Timing attack, Black hole attack etc.

I. INTRODUCTION

Nowadays using MANET, the abundant Wireless applications can be developed and these are used in many numbers of areas like, education, commerce and entertainment. Some features of MANET are Self organizing, infrastructure less and with no centralized administration Characteristics of MANET are: - I] Easy to use II] Mobility of nodes. III] Scalability.

Every device in MANET is free to move independently. The mobile nodes that are in radio range of each other can directly interact, whereas others needs the assistance of intermediate nodes to route their packets. Each of the nodes has a wireless interface to interconnect with each other [6]. All the nodes in the network are mobile and uses wireless communications to connect with other nodes. Challenges in MANET: - I) Limited bandwidth: Wireless link continues to have considerably lower capacity than infrastructure networks. Moreover, the known output of wireless communication after calculating for the effect of multiple access, waning, noise, and interfering conditions, etc., are frequently much less than a radio's maximum delivery rate. II) Dynamic topology: Dynamic topology may disturb the trust affiliation between nodes. The confidence may also be disturbed if some nodes are noticed as cooperated. III) Routing overhead: In wireless ad hoc networks, nodes frequently change their location within the network. So, some flat routes are generated in the routing table which clues to unnecessary routing overhead. IV) Hidden terminal problem**:** Hidden terminal problem denotes to the collision of packets at a receiving node due to the synchronized transmission of those nodes that are not within the direct transmission range of the sender, but are within the communication range of the receiver. V) Packet losses due to transmission errors: Ad hoc wireless networks experience a much advanced packet loss due to issues such as increased collisions due to the existence of hidden terminals, occurrence of intrusion, uni-directional links, frequent path breaks due to mobility of nodes[5]. An attack occurs when an intruder tries to exploit the susceptibilities of a system. There are many types of attacks in MANET**.** Generally speaking**,** these attacks can be classified into two comprehensive categories: passive and active attacks. In passive attacks, the attackers typically involve snooping of data, thus reveal the information about the location and routing of mobile nodes. This kind of attack is very problematic to detect, because the attacker seldom exhibits irregular activities. Active attacks, on the other hand, involve activities performed by an intruder. Mainly data get lost or stolen by black hole attack or by attacking routing protocol. This security issue can be solved using anonymous routing in the network that cannot be identified by any other nodes or attacker. The anonymous routing is very essential in the Military, Banking application, where security of communication is the main purpose. Anonymous routing provides safe communication between two nodes by hiding the original identity of source and destination and prevent these nodes from timing attacks and intersection attack. In this paper the main task of unidentified routing is to detect the black hole attack identity and to provide anonymity to source, destination and route, so that an attacker cannot easily identify the identity and location of the source and destination in the network as well also prevent from black hole attack.

II. MOTIVATION

Security, Scalability and Anonymity are the main challenges of Mobile ad hoc networks. Anonymity is the state of being not identified a subject among many subjects. Anonymity protection is necessary in the MANET. Anonymous routing is crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

III. EXISTING ANONYMOUS ROUTING PROTOCOL

A] ALARM

Anonymous Location Aided Routing is one of the anonymous routing protocols in MANET. ALARM finds out difficulties in the MANET and also provide secure routing in the network [10]. ALARM uses the link state routing protocol. It takes nodes current position to broadcast and forward data. ALARM uses advanced cryptographic techniques as well as it provides node authentication, confidentiality features, data integrity. It also provides security against active and passive attacks. But the problem with ALARM is, it cannot protect the location anonymity of the source and destination node.

B] ASR

Another routing protocol is Anonymous Secure Routing (ASR) protocol. This protocol provides additional identity, anonymity and location privacy, as well as at the same time ensure the security of discovering routes against various passive and active attacks [7]. But ASR protocol does not provide solution to the route anonymity problem.

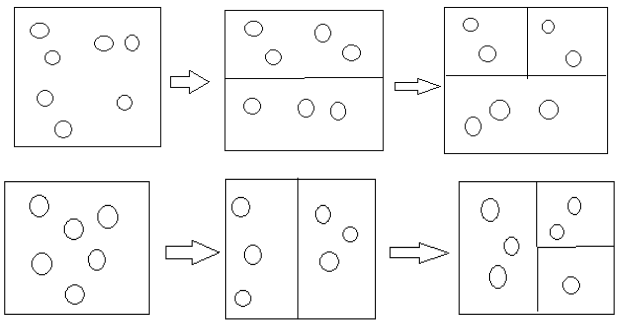
C] AO2P

AO2P is a significant anonymous routing protocol. It is an on-demand position-based private routing algorithm. AO2P protocol mainly provides communication anonymity [7]. In this instead of node identity, nodes location is used for route discovery.

IV. SYSTEM ARCHITECTURE

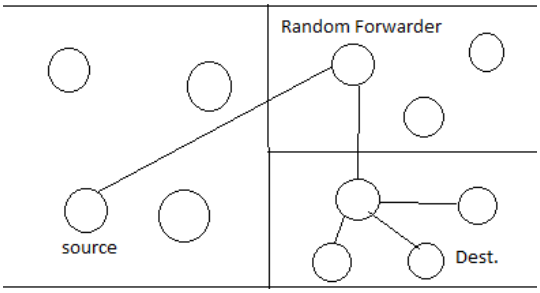
A] The ALERT Routing

Generally ALERT provides random and dynamic routing path, which has no. of dynamically selected midway nodes [10]. I] First ALERT partitions the given network into two zones as horizontally (or vertically). II] Then again splits every partition into two zones as vertically (or horizontally). III] After partitioning ALERT arbitrarily select a node in each partition at each step as an intermediate relay node.



Above figs show both partitioning. Here we have considered a network in rectangular form. In this rectangle, circles are nodes. Consider one example of routing in ALERT.

In this instance, we first partition the network vertically and horizontally or vice versa and so on. While this partitioning each source node checks whether itself and destination node are in the same zone or not [10]. If they are in the same zone, then partitioning continues. In above fig the zone where the destination is located is called as destination zone denoted as ZD.

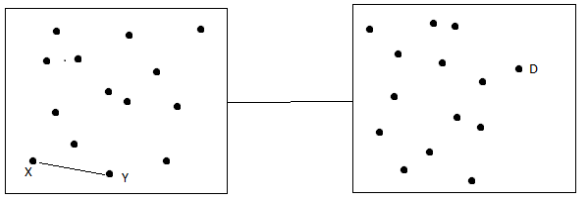


After partitioning the network source node arbitrarily chooses a node in another zone known as a temporary destination (TD) and then uses GPSR routing algorithm to direct the data to node close to TD.A node closer to TD known as Random Forwarder (RF). But in destination zone data is spread in destination zone to k number of nodes which provides k-anonymity i.e intruder or observer are unaware of the destination zone.

Destination node will stay in the same zone during the data transmission process. So it can effectively receive the full data. For successful completion of data diffusion, target node sends an acknowledgement to the source node. If the source node does not get an acknowledgement during predefined period, it will resend packets.

B] GPSR Routing

GPSR is Greedy Perimeter Stateless Routing algorithm. GPSR allows nodes to compute who its nearest neighbors are that are also close to the destination to calculate a path, GPSR uses a greedy forwarding algorithm that will send the information to the destination using the most effective route possible. If the greedy forwarding flops, perimeter forwarding will be used which traverses around the perimeter of the region. Assuming the nodes know their own locations the Greedy algorithm will try to find the closest node which is also the closest to the destination



The GPSR is a receptive and efficient routing protocol for mobile and wireless networks. GPSR can be usseful to Sensor networks, Vehicular networks and ad-hoc networks.

C] Packet Format

For successful routing between source and destination some information is needed, which is embedded in the packet from the source and each packet forwarder node [10]. For ALERT following packet format is used.

RREQ/RREP/NAK		P_S	P_D	L_{z_S}	L_{z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{KN}_{pub}}$	$(Bitmap)_{K^D_{pub}}$		data (NULL in NAK)

Fig. ALERT Packet Format

DOI 10.17148/IJARCCE.2016.53133

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

RREQ/RREP/NAK is used to acknowledge the loss of packets.
Ps- Pseudonym of a source.
Pd – pseudonym of a destination.

Lsz & Ldz – are the locations of Hth partitioned source zone and destination zone.
h- number of divisions.

H – maximium number of divisions allowed.

D] Location of Destination Zone

Zone position is made from the upper left and bottom right Co-ordinates of a zone. It is utilised by each packet forwarder to check whether it is separated from destination zone or not. To evaluate zone position we have H demonstrating total no. of partitions in order to produce destination zones Zd, No.of nodes k and node density ρ,

$$H = \log_2(\rho.G/k)$$

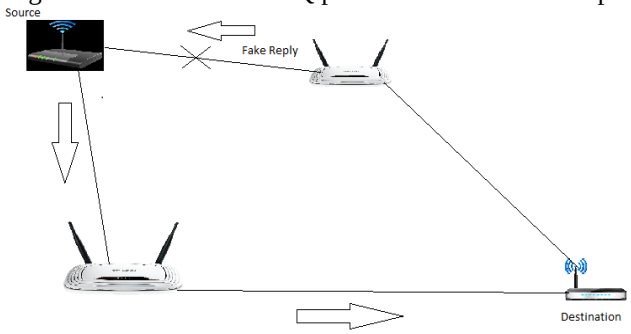
Where,
G=size of entire network area
H=total number of partitions in order to produce Zd.
P=Node density.

E] Algorithm For ALERT Routing

The proposed ALERT-APD algorithm is as follows:
I] Select source and destination for sending packet.
II] Algorithm executes the hierarchical partition module and performs first partition.
III] if (Actual source and destination zone in different Partition)
then, GOTO 5
else GOTO 4
IV] Source (Any source, i.e., actual source or random forwarder) performs toggled partition and verifies whether itself and destination zone (ZD) are in the same zone (i.e., partitioned zone)
if (Source and destination zone (ZD) in different Partition)
then, GOTO 5
else GOTO 4
V] Selects Temporary Destination (TD) in another zone (i.e., the zone in which destination zone lies) and selects a Random Forwarder (which becomes the next temporary source for communication).
VI] Source then sends a RREQ (Routing Request) packet to Random Forwarder and waits for RREP (Routing Response) for a particular time interval (Tw).
if (RREP received within time interval)
then, Source sends data packet to the selected random forwarder uses GPSR algorithm.
GOTO 8
else GOTO 7
VII] Source selects next best choice (RF) for sending data packets. GOTO 6
VIII] if (Source in destination zone)
then GOTO 9
else GOTO 4
IX] Random forwarder broadcasts a RREQ packet to all nodes (k) within the destination zone and waits for a RREP packet for Tw.
if (RREP packet received within Tw)
then random forwarder sends the Data packet to the RREP sender.
GOTO 10
else random forwarder for GOTO 9
X] Exit

F] Detection Of Blackhole Attack Using ALERT

Blackhole attack is a type of packet drop attack in which router that is supposed to relay packet discards them. They attack ad hoc network because wireless architecture has much diverse architecture than wired networks. Intruder locates the source or destination by attacking the packets during transmission of data. A malicious node claims to have a finer route to the node whenever it receives RREQ packets, and directs the REPP with highest destination sequence number and least hop count value to the originator node whose RREQ packets it wants to intercept.



G] Algorithm For Blackhole Detection

I]. Initialize,
a. C_t = Current System Time
b. $T_t = C_t + w_t$
c. $HM_R(sn_d, n_i) = \{\}$
d. $IM_{MN}(n,i) = \{\}$
II]. while (Timer $t<T_t$)
Initialize,
a. SN_D = packet.destination_sequence_number
b. N_I = packet.node_ID
Perform: HM_R -> HM_R U (SN_D, N_I)
III]. Iterate(HM_R),Initialize: i = 0
entry (isn_d, in_i) -> $HM_R(i)$
if (isn_d >>>> SN_S)
then
HM_R -> HM_R - entry(isn_d, in_i)
IM_{MN} -> IM_{MN} Uentry(isn_d, in_i)
IV]. Sort(IM_{MN}), Criteria: SN_D
V]. BLACK_HOLE = IM_{MN}.max(entry)
VI]. EXIT

V. RESULTS

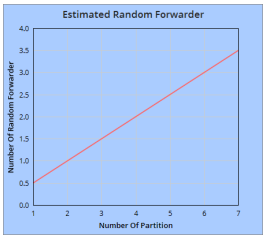


Fig. 1 Estimated Random Forwarders

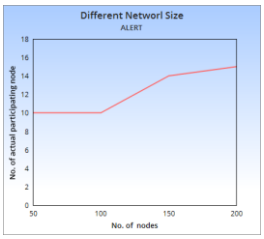


Fig. 2 Number of Actual Partitioning Nodes

Fig. 1 and 2 demonstrates the cumulated actual participating nodes in ALERT with 200 and 300 nodes moving at a speed of 2 m/s, respectively. ALARM and AO2P are similar to the GPSR routing system and thus have similar number of authentic participating nodes, GPSR also represent ALARM and AO2P in conversing the performance difference between them and ALERT. ALERT generates many actual participating nodes since it produces many different routes between each S-D pair.

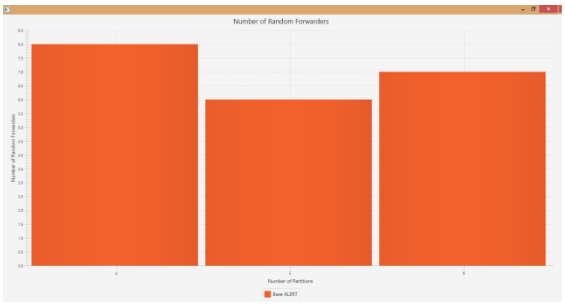


Fig. 3 Number of Random Forwarder

Fig. 3 shows the number of RFs versus the number of partitions in ALERT. The average number of RFs follows approximately a linear propensity as the number of partitions increases. A higher number of partitions H leads to more RFs, hence high anonymity protection. Thus, k should be set to a value that will not generate a high cost for dissemination as well as provide high anonymity protection. Therefore, it is important to discover an optimal tradeoff mark for H and *k*.

VI. CONCLUSION

The Anonymity in MANET is a big issue. The ALERT can provide route anonymity, source anonymity and destination anonymity. ALERT improves anonymity protection with low cost. Internal unavailability is also another issue which will be Solvable by ALERT-APD algorithm Active attack like black hole attack detection over ALERT protocol is done by ALERT-BHS. In future we can overcome attacks and provide more security.

ACKNOWLEDGMENT

The authors would like to thank the publisher, researcher for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support.

REFERENCES

[1] R. S. Pressman, Software engineering (3rd Ed.): A Practitioner's Approach. New York, NY, USA: McGraw-Hill, Inc., 1992.
[2] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," Network, IEEE, vol. 15, no. 6, 2001.
[3] K.-W. Chin, J. Judge, A. Williams, and R. Kermode, "Implementation experience with Manet routing protocols," ACM SIGCOMM Computer Communication Review, vol. 32, no. 5, 2002.
[4] R. Kaur and M. K. Rai, "A novel review on routing protocols in manets," Undergraduate Academic Research Journal (UARJ), ISSN, pp. 2278–1129, 2012.
[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer,"A secure routing protocol for ad hoc networks," in Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, pp. 78–87, IEEE, 2002.
[6] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: self-organized network-layer security in mobile ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 261–273, 2006..
[7] 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.
[8] 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.
[9] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Pro
[10] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.

BIOGRAPHIES

Akshay Jaitpal pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from University of Pune.

Pavan Kodihal pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from University of Pune.

Pratik Gothiwadekar pursuing BE in Computer Engineering from D. Y. Patil Institute of Engineering and Technology from University of Pune.