ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Detecting Sequence Number Collector Problem in Black Hole Attacks in AODV Based Mobile Adhoc Networks

Anand Nayyar, Assistant Professor, Department of Computer Applications & IT, KCL Institute of Management and Technology, Jalandhar E-Mail: anand_nayyar@yahoo.co.in

Abstract— Mobile Ad-hoc Network (MANET) is an autonomous system, where nodes/stations are connected with each other through wireless links. MANETs are highly vulnerable to attacks due to the open medium, dynamically changing topology, lack of centralized monitoring and management point. The possible and the commonest attack in ad hoc networks is the black hole attack. In the black hole attack, a malicious node advertises itself as having the shortest path to the destination node. In the existing method a detection method based on checking the sequence number in the Route Reply message by making use of a new message originated by the destination node was developed but the drawback here is that a malicious node can play a role of sequence number collector in order to get the sequence number of as many other nodes as possible. In this Research Paper, a system is being proposed via which the sequence number collector problem is overcome by classifying the nodes into three categories based on the behavior. The malicious node is isolated from the active data forwarding and routing. The association between the nodes is used for the route selection. The scheme which is proposed in this research paper not only increases the routing security but also make the nodes cooperate among each other in the adhoc network.

Index Terms— Secured Routing, AODV, Black Hole Attack Detection, Malicious Nodes, Adhoc Network.

I. INTRODUCTION

A wireless ad hoc network is a decentralized wireless network. The network is ad hoc because it does not rely on preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly. Wireless ad hoc networks can be further classified by their application as mobile ad hoc networks (MANETs), wireless mesh networks, wireless sensor networks.

A.CHARACTERISTICS OF MANET

One of the classifications of wireless ad hoc network is MANET (Mobile ad hoc network).A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a route. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic[1]. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks are not mobile or not wireless. MANET are highly vulnerable to attacks due to open medium, dynamically changing network topology, co-operative algorithms, lack of centralized monitoring and management point, lack of clear line defense. One of the typical routing protocols for MANET is called Ad Hoc On-Demand Distance Vector (AODV) [2] One of the possible and commonest attacks in ad hoc networks is the black hole attack.

B. Ad-Hoc on-Demand Distance Vector Routing (AODV PROTOCOL)

Ad-hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing. In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a

All Rights Reserved © 2012 IJARCET

request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches. A RouteRequest carries the source identifier ,the destination identifier , the source sequence number , the destination sequence number , the broadcast identifier , and the time to live (TTL) field.

C. BLACK HOLE ATTACK

One of the possible and commonest attacks in Ad hoc networks is the Black Hole attack[3]. In the Black Hole Attack the malicious nodes advertise itself as having the shortest path to the destination node. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue.

II. PROBLEM STATEMENT

When a node moves out of the transmission range of the source node, the source node assumes to be normal node as a malicious node (False positive). When a normal node detects a malicious node the node will broadcast an alarm message. However this alarm message may not arrive at the source node in time for various reasons such as no route to the source node. Thus the source node cannot judge that there is a malicious node in the root and begins to send data along this dangerous route(False negative). The sequence number generated by a destination node is very important, a malicious node can play a role of sequence number collector in order to get the sequence number of as many other nodes as possible by broadcasting request with high frequency to different nodes in MANET, so that this collector always keeps the freshest of sequence numbers of other nodes.

III. RELATED WORK

Satoshi Kurosawa et al.[4] proposed a Dynamic Learning Method to detect black hole attack in AODV based MANET. This paper analyzes the black hole attack which is one of the possible attacks in ad hoc networks. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals is proposed. Latha Tamilselvan et al.[5] proposed a method to prevent black hole attack in MANET. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Handling the timer expiration event is difficult The handling of route reply packet takes more time. Payal N. Raj et al.[6] proposed a dynamic learning system against black hole attack in AODV based MANET. In this paper, a DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of black hole by notifying other nodes in the network of the incident is proposed. The prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbors. The calculation of the threshold value is difficult. Zhao Min et al.[7] proposed a method to prevent cooperative black hole attack for MANETS. Two authentication mechanisms, based on the hash function, the Message Authentication Code (MAC) and the Pseudo Random Function (PRF), are proposed to provide fast message verification and group identification, identify multiple black holes cooperating with each other and to discover the safe routing avoiding cooperative black hole attack. Xiao Yang Zhang et al.[8] proposed a method to detect black hole attack in MANET. Every conventional method to detect such an attack has a defect of rather high rate of misjudgment in the detection. In order to overcome this defect, a new detection method based on checking the sequence number in the Route Reply message by making use of a new message originated by the destination node and also by monitoring the messages relayed by the intermediate nodes in the route is proposed Can detect more than one black hole attacker at the same time. No need of any threshold or trust level. When a node moves out of the transmission range of the source node the source node assumes the normal node as a malicious node. When a normal node detects a malicious node the node will broadcast an alarm msg. however this alarm message may arrive at the source node in time for various reasons such as no route the source node. Thus the source node cannot judge that there is a malicious node in the route and begins to send data along this dangerous route. H.Lan Hguyen et al.[9] made a study of different types of attacks on multicast in MANET. Security is an essential requirement in mobile ad hoc networks (MANETs).In the above study the following are analyzed First, protocols that use the duplicate suppression mechanism such as ODMRP, MAODV, ADMR are very vulnerable to rushing attacks. Second, although the operations of black hole attacks and neighbor attacks are different they both cause the same degree of damage to the performance of a multicast group in terms of packer loss rate. Finally, jellyfish attacks do not

All Rights Reserved © 2012 IJARCET

affect the packet delivery ratio or the throughput of a multicast group, but they severely increase the packet end-to-end delay and delay jitter. The performance of a multicast session in MANETs under attacks depends heavily on many factors such as the number of multicast senders, the number of multicast receivers, the number of attackers as well as their positions.

IV. PROPOSED SCHEME

This section presents the extension of Association based Routing which is to be applied over the AODV protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experiences that the node has with its neighbor nodes.

In proposed scheme we classify the Association among the nodes and their neighboring nodes in to three types as below

UNASSOCIATED (UA)

The nodes that newly joined the network and those nodes which have not forwarded any message comes under this category. The trust levels are very low and the malicious behavior is very high.

ASSOCIATED (A)

The nodes that have started to send message but have some more messages to forward come under this category. The trust levels are neither low nor too high, probability of malicious nodes in the network is to be observed.

FRIEND (F)

The nodes that have forwarded all the messages to the corresponding destination falls under this category and the trust levels between them are very high, probability of malicious behavior is very less.

The following table shows the Association Table of Node 1 in Fig. 1

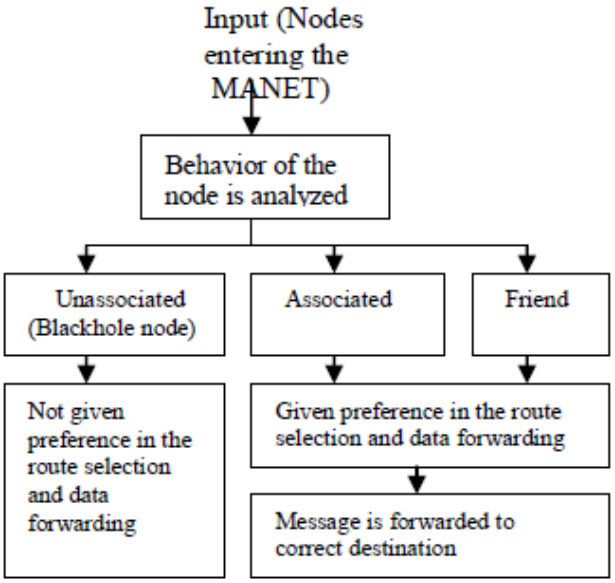

Fig.1: Block Diagram

B. CALCULATION OF TRUST VALUE

The trust values are calculated based on the following parameters of the nodes. We propose a very simple equation for the calculation of trust value.

R= The ratio between the number of packets forwarded and number of packets to be forwarded. The threshold trust level is calculated by using (1)

A=Acknowledgement bit.(0 or 1)

T= tanh (R+A)

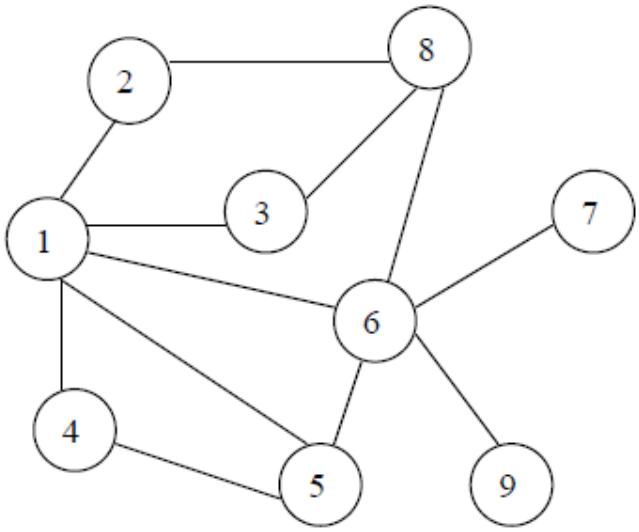

Fig: Nodes in Ad-hoc Network

All Rights Reserved © 2012 IJARCET

The following table shows the association table for Node 1

Neighbors	Nature of Association
2	F
3	F
4	A
5	F
6	UA

The threshold trust level for an unassociated node to become associated to its neighbor is represented by TA and the threshold trust level for a associated node to become a Friend of its neighbor is denoted by TF. The Associations are represented as

A (node x → node y) = F when $T \geq TF$

A (node x → node y) = A when $TA \leq T < TF$

A (node x → node y) = UA when $0 < T \geq TA$

Also, the Association between nodes is asymmetric, (i.e.,) A (node x → node y) is an Association evaluated by node x based on trust levels calculated for its neighbor node y. A (node y → node x) is the Association from the Association table of node y. This is evaluated based on the trust levels assigned for its neighbor. Asymmetric Associations suggest that the direction of data flow may be more in one direction. In other words, node x may not have trust on node y the same way as node y has trust on node x or vice versa.

C. Path Selection for Active Data Forwarding

The following table shows the path chosen based on Proposed Scheme

Best Path P1	Best Path P2	Path Selection
F	F	F is chosen in P1 or P2 based on the length of the path.
F	A	F is chosen in P1
A	F	F is chosen in P2
A	A	A is chosen in P1 or P2 based on the length of the path
F	UA	F is chosen in P1

When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighboring nodes; The ROUTE REPLY obtained from its neighbor is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a friend, then that path is chosen for message transfer. If its one-hop neighbor node is a Associated node, and if the one hop neighbor of the second best path is a friend choose C. Similarly an optimal path is chosen based on the degree of Association existing between the neighbor nodes.

The source selects the shortest and the next shortest path. Whenever a neighboring node is a friend, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between friends. If it is a associated or unassociated, transfer is done based on the ratings. This protocol will converge to the AODV protocol if all the nodes in the ad hoc network are friends. In the proposed scheme the route is not selected on the basis of first arrival of RREP and waits till it gets the RREP from all neighboring nodes and decides the routing path based on the nature of Association between them. Thus the black hole nodes are identified as unassociated in both the hops and were not given preference in the route selection.

V. CONCLUSION

In this paper we have discussed the characteristics of mobile adhoc network and about the Black hole attacks. The proposed scheme of Association based AODV protocol increases the routing security and also encourages the nodes to cooperate in the adhoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing. Since the black hole node is the one which do not forward any message to the destination and consumes the entire message our proposed scheme identifies more than one black hole attacker node and the data is not allowed to pass through the black hole node path thus delay and overhead in route selection is reduced.

REFERENCES

[1] Elizabeth M, Royer, and Chai-Keong Toh: "A Review of CurrentRouting Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, (April 1999).

[2] C.E. Perkins, S,R, Das, and E. Royer: "Ad-I-Ioe on Demand Distance Vector(AODV)", RFC 3561.

[3] H. Lan Nguyen and U, Trang Nguyen: "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Network,VoI.6,No. I, (2007).

[4] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto: "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by Dynamic Learning Method", International Journal of Network Security, Vo1.5, PP.33S-346, (November, 2007).

[5] Latha Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANEr", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007).

[6] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against Black Hole Attack In AODV Based Manet", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[7] Zhao Min, Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", International Symposium on Information Engineering and Electronic Commerce, 2009.

[8] Xiao Yang Zhang, yuji Sekiya and Yasushi wakahara, "Proposal of a Method to Detect Black Hole Attack in

All Rights Reserved © 2012 IJARCET

MANET", Autonomous Decentralized Systems, pp 1-6, ISADS 2009 .

[9] H.Lan Hguyen and U.Trang Nguyen, "A Study of Different Types of Attacks on multicast in Mobile Ad Hoc Networks", Ad Hoc Network,Vol.6, No.1, 2007.

[10] N.Bhalaji, Dr.A.Shanmugam, "Association between nodes to combat blackhole attack in dsr based manet", 2009.

[11] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edulnsnam.

Anand Nayyar (B.Com, MCA, M.Phil, M.Tech(IT), C-Cyber Law, C-IPR) an Academician, Researcher, Author and Innovator. He is certified in A+, CCNA, MCSE, MCTS, MCITP, RHCE, OCP, CEH and many more. He has published more than 100 Research Papers and has written 7 books on Computer Science Topics. He is actively researching on Networks, Wireless Communications, Adhoc Networks, Mobile Adhoc Networks and Swarm Intelligence. Anand Nayyar is a part of more than 100 Journals Editorial Boards and Review Boards and has reviewed more than 400 Research Papers. He is Life Member of various Research Societies like **ISTE, IAENG, IACSIT, AIAER, ISITA, ACM-CSTA, ISOC, SDIWC, UACEE, IAEST, ICST, GERA, IACAT, IAOE, APCBEES, SCIEI, MCDM, IAEME, British Science Association, EURO, ISI, PASS and many others.**

All Rights Reserved © 2012 IJARCET