A Secure Model For Prevention Of Black Hole Attack In Wireless Mobile Ad Hoc Networks

TANYA KOOHPAYEH ARAGHI[1], MAZDAK ZAMANI[1], AZIZAH BT ABDUL MANAF[1], SHAHIDAN M. ABDULLAH[1], HODA SOLTANIAN BOJNORD[1], SAGHEB KOHPAYEH ARAGHI[2]
[1]Advanced Informatics School
Universiti Teknologi Malaysia
54100 Kuala Lumpur
MALAYSIA
[2] Faculty of Engineering
Multimedia University Malaysia
63100 Cyberjaya Selangor
MALAYSIA
Tanya.koohpayeh@gmail.com[1], mazdak@utm.my[1], azizah07@citycampus.utm.my[1], mshahidan@ic.utm.my[1], soltanian.hoda@gmail.com[1],s_koohpaeh@yahoo.com[2]

Abstract: - Implementing Ad hoc networks are becoming very prevalent during recent years. Security is the most important issue for developing mobile ad hoc networks (MANETs). They expose to various kinds of attacks because of their unique nature in which every node can easily join to network or leave it. Black hole attack is the most probable attack in MANET. In this research we proposed a model for prevention of this attack. It judges on route replies coming from the intermediate node based on a trusted third party which is the destination node. If the source node received an acknowledgement on the route replies sending by an intermediate node, from destination during a specific time, it decides that the path is safe and intermediate node is not malicious. Meanwhile a counter will be set for counting the number of times that each intermediate node introduced a wrong route reply. Every node that proposes a wrong route reply will be recorded in a black list. The process also will be checked for all one hop neighbors of the suspicious node and the history of these nodes will be gathered in the black list, if they proposed a wrong route reply during the route discovery process. When the counter for each node exceed from a specific value, the chain of suspicious nodes will be introduced as black holes and an alarm will be notified to all nodes in the network to remove these malicious nodes from their routing tables.

Key-Words: - Mobile Ad hoc networks, routing protocols, AODV and black hole attack

1 Introduction

Wireless Mobile Ad Hoc Network (MANET) is a set of autonomous mobile users that communicate with each other without any specific infrastructure. Since the position of nodes changes over time, the network topology modifies unpredictably. Every node is added to the network, as soon as locating in this environment [1, 2].

Each node in MANET can take part to the network freely and accept the action of leading and routing data packets; hence ad hoc networks have a large number of potential applications like the military uses such as joining armed forces or other military purpose, on the battlefields, disaster area, setting up virtual classrooms, hospital data base during emergency situations and historical places where having a fixed infrastructure is difficult [3, 4].

The goal of security issues in mobile ad hoc networks is providing confidentiality, integrity, availability and authentication [5].

Generally, ad hoc networks suffer from lack of physical security because of their unpredictable and erratic structure, so recognition of invaders is more difficult compared with their wired counterparts. For example, the possibility of eavesdropping or impersonating of malicious nodes is very prevalent in such kinds of networks [6, 7].

In this paper we focus on AODV which is a reactive (on demand) routing protocol. The main reason for selecting this routing protocol is that basically, black hole attack misuses the specification of the routing

protocols like AODV and DSR in which if the intermediate node has the freshest route to destination, it can suggest the whole route from source to the destination. In black hole attack this suggestion is a fake suggestion to deviate the route toward malicious nodes and absorb the data packets. Since DSR is not suitable for large networks, we choose AODV, then we introduce different methods for prevention of black hole attacks and finally describe the proposed model, conclusion and future work.

2 Literature Review

When a mobile node tries to communicate to the other nodes, it is necessary to announce its status and position of the other nodes in its vicinity. Considering the mobility of nodes, there are different routing protocols in MANETs classified as proactive, reactive or on demand and hybrid routing protocols. In proactive routing protocols every change will be recorded in routing tables and the route is specified even before it is needed. Reactive or on demand routing protocols perform the route discovery process when they need to send data packets. Hybrid routing protocols are a combination of both proactive and reactive routing protocols [8].

2.1 AODV Routing Protocol

AODV is a method of leading messages between mobile computers. It permits the mobile nodes sending messages by means of their neighbors to the nodes that they are not able to communicate with them directly. AODV performs this by finding the routes along which messages can be transmitted. AODV makes sure these routes do not contain loops and tries to find the shortest possible path. It borrows the idea of the destination sequence number from DSDV, to preserve the most recent routing information among nodes [9] utilizing sequence numbers to judge whether the routing message is fresh or not. It also provides a fast, dynamic network connection, featuring low processing loads and low memory spending. Routing messages in a network can be separated into path discovery and path maintenance messages. The first one includes the Route Request (RREQ) and the Route Reply (RREP), while the second one includes Route Error (RERR) and Hello messages [10, 11].

Processing the RREQ, an intermediate node first checks for existing a corresponding reverse route in its routing table, if exists, the node would generate an entry for a reverse route and if the sequence number of the destination in this entry is less than the source sequence number in the RREQ (a larger number means fresher information), it would be changed with the information in the RREQ. If this intermediate node has a path to the destination, and the route is not expired, the intermediate node will return the RREP to the source by the reverse path. Nevertheless, the RREQ will be broadcasted to resume searching a route to destination. While the destination node, or one intermediate node, which knows a route to the destination receives a RREQ, it will respond a RREP to the source by a unicast method [12].

2.1.1 Sequence Numbers

Sequence numbers utilized as time stamps. They let nodes compare how “fresh” their information to other nodes is. Each time a node sends out any kinds of message it increases its own sequence number. Each node registers the Sequence number of all the other nodes in communication with. A higher Sequence number indicates a fresher route. As a result, it is possible for other nodes to discover which one has more accurate information [13].

2.2 Black Hole Attack

A malicious node that falsely replies for any route request without having an active route is a black hole. Its purpose is to specify the destination and drop all the receiving packets. If several malicious nodes work together as a group the damage will be extremely serious. It is called cooperative black hole attack [14, 15].

The main problem that causes this attack in MANETs is sending fake route replies from the intermediate node. When the source node asks a route request (RREQ) from its neighbors for a route to destination, all of the nodes in the network who have a route to destination should refer to their routing table and send a route reply (RREP) to the source node.Since the malicious node does not check its routing table, it is usually the first node that sends route reply (RREP) to the source node and it happens by claiming either to have the shortest path to the destination or providing the highest sequence number. The source node is deceived based on this fake claim of the intermediate malicious node and sends the data packets to this node. Then the malicious node who gets the data packets easily drops them and does not pass them to its neighbor. This attack is known as black hole attack [3].

ISBN: 978-1-61804-171-5

2.3 Related Works

Since the black hole attack can be defined as sending fake route replies from intermediate node, various solutions proposed for prevention of this attack.

In prevention of a co-operative black hole attack (PCBHA) [16], a fidelity table will assign to every node which acts as a measurement for reliability of nodes participating in the route discovery process. The route replies are gathered in a table named response table which maintains the fidelity level of each node participates in the route discovery process. When a data packet is received by destination, it will send an acknowledgement to the source and enables the source to add the fidelity level of intermediate nodes otherwise the fidelity level for intermediate nodes will be decrement by the source node. If the level of any node drops to 0, it will regard as a malicious node and will be eliminated as a black hole node. This solution provides better packet delivery ratio, but it does not mention about the nodes joining to the network without previous history. It also creates overhead and delays more than AODV and setting a proper value for trust in a real network is difficult.

Distributed and cooperative mechanism (DCM) [17, 18] is another scheme against black hole attack included four phases. In the first stage (local data collection), each node tries to collect the information by overhearing the packets to check whether there is any distrustful node in its vicinity.

In case of finding a node found, the second phase (local detection procedure) will be started for analyzing that if the suspicious node is a wicked black hole node or not. Accordingly, the third phase (cooperative detection procedure) begins with the initial detection node, which notifies to all the one-hop neighbors of the potential suspicious node by broadcasting and make them participate in the detection process deciding that whether the suspicious node is definitely a malicious node or not. As soon as detecting black hole node, the fourth phase (global reaction) is activated. It is an appropriate announcement system to send warnings to the entire network. Simulation results use AODV protocol indicates either packet delivery or detection rate will improve, but this solution creates more overhead than AODV.

The method proposed by Zhao Min and Zhou Jiliu were the message authentication code (MAC) and the pseudo random function (PRF) for authentication of route replies (RREPs) [19] in which every node obtains a secret key Ki, that Ki = Gk (ri). The sharing key Ki is secret for all other nodes; so, it is formulated by opting a random number ri and continually applying PRF on ri by k times. Once the source node receives a packet, it checks Ki-d to find out whether the key designed for the MAC is disclosed or not, and checks the MAC when Ki is exposed. Having checked the above two conditions, this packet is considered as an available packet and the route is approved as a safe route. This method also provides a good rate of packet delivery ratio, but increases the control overhead and malicious node also can avoid from detecting by providing false reply packets.

Anita and Vasudevan, 2010 [20] proposed a model using multicast chaining scheme, in which each node issues a certificate for its next hope node for example:

Cert (A->B) = [ID B, KB, t, e, S] KA (1)

ID B is identity of B, KB is the public key of B, t is the time within the certificate issued, e is the expiry time of certification and S is the security level of node B which has been signed by node A. The public key will be calculated through a one way hash function H as follows:

KB = H (ID B) (2)

Every node has a local repository including the certificates issued for this node and certificates issued by this node for others. This repository is being updated periodically for adding new certificates. In case of conflicting or issuing wrong certificates, there is a probability of exporting the certificate by a malicious node so; the certificate will revoke from the node. Although, this solution provides a safe route, it causes memory consumption and consequently low speed. Calculation overhead is also the other problem of this scheme.

Bait DSR (BDSR) is the other scheme proposed in 2011 by Tsou -[21]. In this scheme the source node sends a bait RREQ packet. The target address of this RREQ packet is not real and is quite random. For obstructing the traffic problem and unoccupiying network bandwidth, the life of RREQ packets is just a short period of time. Therefore, malicious nodes can be identified in the first phase, because the RREQ packets take the forged RREP packets in. RREP packets have an extra field which records the sender of RREP packets. Hence, the black hole nodes and their position can be known by the source node. Then all of the replies sent by malicious nodes have to be eliminated. Simulation results have done with QUALNET shows 90% packet delivery ratio and overhead is a little less than BDSR, but this solution cannot detect collaborative black holes and it is difficult to implement.

Ming-Yang Su in 2012 proposed an IDS approach for prevention of black hole attack [22, 23] which is called Anti Black hole. In this method some nodes used as IDS nodes. They act in sniffing mode to check the suspicious value for the other nodes in their vicinity. When the suspicious value exceeds from a threshold, a block message will be broadcasted by the closest IDS node, notifying the nodes in the whole of network to isolate malicious node. Simulation with NS2 shows a good detection rate, but increases the end to end delay [24, 25].

These solutions did not mention about the nodes take part in the route discovery process for the first time without having a previous history while, the proposed model considers this problem. It also quarantines the malicious nodes as well as deleting them from the routing table of the nodes in the network.

3 Proposed Model

Figure 1 shows the stages of this solution. The terms are described as below:
IN= Intermediate Nod
NHN= Next Hop Node
MRREQ= More Route Request
MRREP=More Route Reply
T_{MRREP}= Time of Receiving More RREP
T_{TO}=T of time out (time in which the response is not acceptable)
CL_{IN}=the Concern Level of Intermediate Node
CL_{NHN}=the Concern Level of Next Hop Node

The model judges on the route replies coming from the intermediate nodes based on the trusted third party. The trustworthiness of intermediate node which sends a RREP needs to be proved. In this model destination node copes with this responsibility. When a RREP comes from the intermediate node (IN), it is assumed that this route reply is safe so, the source node sends a more route request (MRREQ) to destination node via the recommended route by the intermediate node, and then waits for a reply. Meanwhile, a timer has been set, if the reply time of the destination was less than the time out, then it means that the intermediate node is right, because firstly, the portion of the path coming from the destination node confirms the intermediate node's path and secondly, it protects raising the sequence number from adversaries because destination node has the latest fresh route and consequently the last sequence number.

If the more route reply (MRREP) has not been sent in a specific time by the destination, it means that the route is not safe.

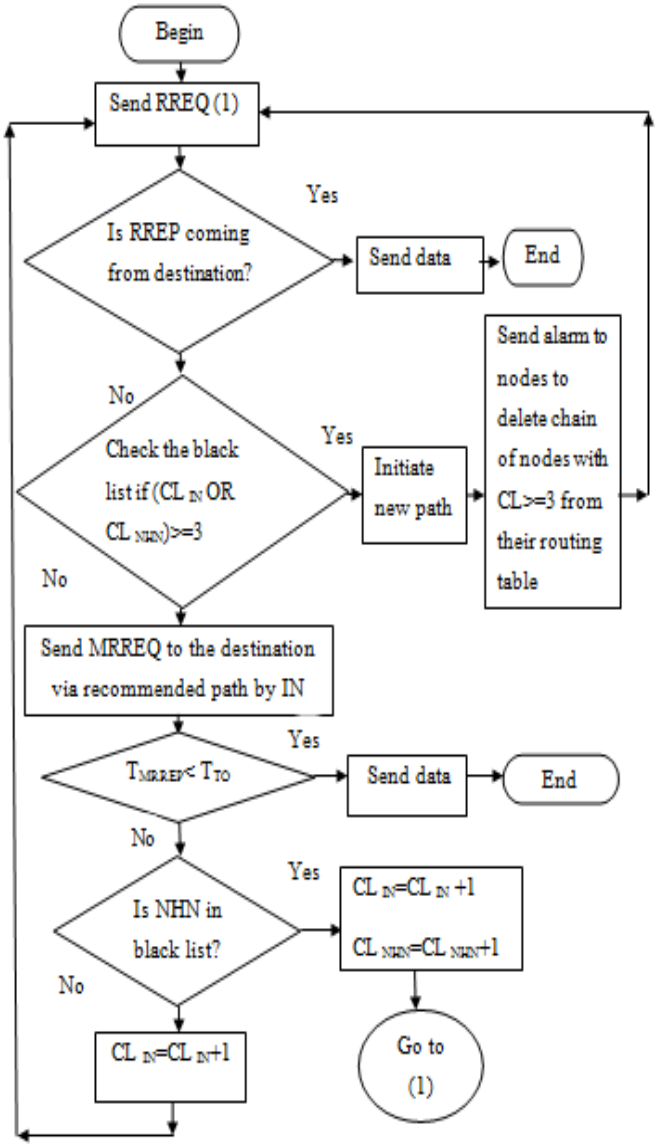

Figure 1. The flow chart of the proposed model

It may signify the existence of malicious nodes in the path or some other problems related to nodes. However, our crucial aim is to avoid unsafe routes to prevent black hole attack. Hence, the particular route has been ignored and a new route will be initiated. On the other hand, a black list and a counter will be initiated and the intermediate node will move to this black list. There is a counter names concern level (CL) for each intermediate node sending a route reply (RREP) which is equal to zero at first. For three times route initiation, the source node trusts to the intermediate node and sends MRREQ to the destination node. If the destination node could not send the MRREP at the specific time, then the source node will check whether the intermediate node or the next hop node (NHN) of the intermediate node is in the black list or not, if the intermediate node is in the black list then the CL will increase by one.

ISBN: 978-1-61804-171-5

If the intermediate node which provides the wrong route is not in the blacklist but one of its one hop neighbors is in black list, then the CL will increase for both intermediate node and its next hop node (NHN). When CL for each node gets more than 3, a RERR message will send by the source node to all of the nodes participating in route discovery process to remove this intermediate node and its neighbors from their routing table and ignores these nodes for their route initiations and a new route will be initiated.

3.1 Assumptions

There are some assumptions considered as the following conditions: Firstly, based on what has mentioned, in black hole attack an intermediate node sends a RREP message and never check its routing table, so it would be the first RREP responder. Proposed model gives three times opportunities to the intermediate node to show its behavior. If the intermediate node or one of its next hop neighbors send fault RREP that destination cannot confirm the path at a given time, then the intermediate node and its next hop nodes are introduced as a chain of cooperative black hole nodes. As a result, the source sends alarm to all participants in the route discovery process to delete this chain from their routing table. Secondly, the source node needs to contain a Black Table including node id and a counter names CL for each node id (CL_{IN} and CL_{NHN}), For example, the node numbers 3 and the value of CL_3, black nodes and malicious nodes. Thirdly, in this model it is assumed that neither source node, nor destination node plays the role of adversaries.

4. Conclusion and future work

This model, first trust the intermediate nodes which send RREP message but gets the acknowledgement from destination. If the acknowledgement was not got by the destination, the history of these malicious intermediate nodes would be stored in a black list for the other times judgements. The CL parameter is a counter which shows the bad behavior for the intermediate nodes each time they send a wrong route reply. If CL for each node is more than 3, the node will be introduced as malicious node and the route recommended by this node will be avoided.

In future work, we intend to implement the simulation and judge on the proposed model by the experimental results stemming from that.

This solution may create false detection when the destination node does not receive the acknowledgement at a specific time. In this case the future work is to decrease the rate of false detection to have a concise prevention method against black hole attack.

References:

[1] Maziar Janbeglou, Mazdak Zamani, and Suhaimi Ibrahim. Redirecting Network Traffic toward a Fake DNS Server on a LAN. 3rd IEEE International Conference on Computer Science and Information Technology. July 9 - 11, 2010. Chengdu, China.

[2] Shohreh Honarbakhsh, Mazdak Zamani, Roza Honarbakhsh. Dynamic Monitoring in Ad hoc Network. 2012 International Conference on Mechanical and Electrical Technology (ICMET 2012). July24-26, 2012, Kuala Lumpur, Malaysia. Applied Mechanics and Materials. Vols. 229-231 (2012). pp 1481-1486. (2012) Trans Tech Publications, Switzerland. ISSN: 1660-9336.

[3] Maziar Janbeglou, Mazdak Zamani, and Suhaimi Ibrahim. Redirecting Outgoing DNS Requests toward a Fake DNS Server in a LAN. IEEE International Conference on Software Engineering and Service Science. July 16-18, 2010, Beijing, China.

[4] Hossein Rouhani Zeidanloo, Azizah Abdul Manaf, Rabiah Bt Ahmad, Mazdak Zamani and Saman Shojae Chaeikar. A Proposed Framework for P2P Botnet Detection. IACSIT International Journal of Engineering and Technology (IJET), Vol.2, No.2, April 2010, ISSN 1793-8236.

[5] Shohreh Honarbakhsh, Maslin Masrom, Mazdak Zamani, Saman Shojae Chaeikar, and Roza Honarbakhsh. “A Trust Based Clustering Model for Dynamic Monitoring in Ad hoc Network”. International Conference on Computer and Computational Intelligence (ICCCI 2010). December 25-26, 2010. Nanning, China.

[6] Maziar Janbeglou, Mazdak Zamani, Suhaimi Ibrahim. Improving the Security of Protected Wireless Internet Access from Insider Attacks. Advances in information Sciences and Service Sciences. Volume4, Number12, July 2012.

[7] Mojtaba Alizadeh, Mazdak Zamani, Ali Rafiei Shahemabadi, Jafar Shayan, Ahmad Azarnik. A Survey on Attacks in RFID Networks. Open International Journal of Informatics (OIJI). Vol 1 (2012).

[8] Mojtaba Alizadeh, Wan Haslina Hassan, Mazleena Salleh, Mazdak Zamani, Eghbal Ghazi Zadeh. Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID. Journal of Next Generation Information Technology.

[9] Shima Beigzadeh, Mazdak Zamani, Suhaimi Ibrahim, and Maslin Masrom. Design and Implementation of a Web-Based Database-Centric Management Information System for a Social Community. 2011 International Conference on Information Systems and Computational Intelligence (ICISCI 2011). January 18, 2011. Harbin, Northeastern China.

[10] Hossein Rouhani Zeidanloo, Azizah Abdul Manaf, Payam Vahdani Amoli, Farzaneh Tabatabaei and Mazdak Zamani "Botnet Detection Based on Traffic Monitoring". IEEE, International Conference on Networking and Information Technology. Philippines. 2010.

[11] Eghbal Ghazizadeh, Mazdak Zamani, Jamalul-lail Ab Manan,Reza Khaleghparast, Ali Taherian. A Trust Based Model for Federated Identity Architecture to Mitigate Identity Theft. The 7th International Conference for Internet Technology and Secured Transactions. London, UK. 10th- 12th December 2012.

[12] Maryam Gharooni, Mazdak Zamani, and Mehdi Mansourizadeh. A Confidential RFID Model to Prevent Unauthorized Access. 3rd International Conference on Information Science and Engineering (ICISE2011). Sep 29-Oct 1, 2011. Yangzhou, China.

[13] Eghbal Ghazizadeh, Mazdak Zamani, Jamalul-Lail Ab Manan and Abolghasem Pashang. A Survey on Security Issues of Federated Identity in the Cloud Computing. The 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2011). Dec 3 – 6, 2012. Taipei, Taiwan.

[14] Somayeh Nikbakhsh, Mazdak Zamani, Azizah Abdul Manaf, and Maziar Janbeglou. A Novel Approach for Rogue Access Point Detection on the Client-Side. The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA-2012). Fukuoka, Japan, March 26-29, 2012.

[15] Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh shooshtari, Payam Vahdani Amoli, M. Safari and Mazdak Zamani, "A Taxonomy of Botnet Detection Techniques". International Conference on the 3nd IEEE International Conference on Computer Science and Information Technology. Chengdu, China, July 2010.

[16] Dokurer, S., Simulation of Black hole attack in wireless Ad-hoc networks. 2006: Atılım University.

[17] Weerasinghe, H. and H. Fu, Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. International Journal of Software Engineering and Its Applications, 2007. 2(3): p. 362-367.

[18] Tamilselvan, L. and V. Sankaranarayanan, Prevention of co-operative black hole attack in MANET. Journal of Networks, 2008. 3(5): p. 13-20.

[19] Yu, C.W., et al., A distributed and cooperative algorithm for the detection and elimination of multiple black hole nodes in ad hoc networks. IEICE Transactions on Communications, 2009. E92-B(2): p. 483-490.

[20] Sara Farahmandian, Mazdak Zamani, Ahad Akbarabadi, Joobin Moghimi Zadeh, Seyed Mostafa Mirhosseini, Sepideh Farah Mandian. A Survey on Methods to Defend against DDoS Attack in Cloud Computing, 12th WSEAS International Conference on Software Engineering, Parallel and Distributed Systems. Cambridge, UK. February 20-22, 2013.

[21] Ahad Akbarabadi, Mazdak Zamani, Sarah Farahmandian, Joobin Moghimi Zadeh, Seyed Mostafa Mirhosseini. An Overview on Methods to Detect Port Scanning Attacks in Cloud Computing. 12th WSEAS International Conference on Software Engineering, Parallel and Distributed Systems. Cambridge, UK. February 20-22, 2013.

[22] Min, Z. and Z. Jiliu. Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. 2009: IEEE.

[23] Anita, E.A.M. and V. Vasudevan, Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining. International Journal of Computer Applications. 2010. 1(12): p. 22-29.

[24] Mojtaba Ali Zadeh, Mazdak Zamani, Jafar Shayan, Touraj Khodadadi. "Code Analysis of Lightweight Encryption Algorithms Using in RFID Systems to Improve Cipher Performance." The 2012 IEEE Conference on Open Systems. Malaysia. 2012.

[25] Shima Beigzadeh, Mazdak Zamani, Suhaimi Ibrahim. Development of a Web-Based Community Management Information System. The Fourth International Conference on Information and Computing. 25-27 April 2011. Phuket, Thailand.