Asian Journal of Information Technology 13 (11): 715-719, 2014
ISSN: 1682-3915

To Prevent MANET from Black Hole Attacks Using Proposed CCLAM (Classic Cluster Layer Architecture over MANET)

Kuldeep Sharma and G. Mahadevan
Anna University, Coimbatore, India

Abstract: Mobile ad hoc networks used for processing, storage and wireless communication capabilities of mobile devices to create unstructured and low-cost self-configuring networks. Black Hole Attacks are serious problems to establish a communication in MANETs. In this research, we present CCLAM, a new proposed approach using new classic clustering formatted graphs to identify the nodes who are trying to create a black hole. We use well-established architecture to gain information about the network topology, keep eyes on all ordinary nodes and master nodes and maintain database to update all kind of information which use to perform original checks of the routing information generated by the nodes in the network. We assume there is a node in the network generating fake and wrong routing information as malicious node. Therefore, we blow an flag and alarm if the verification check fails. Furthermore, we present promising first simulation results with the new architecture, it is possible to detect the attempt of creating a black hole before the actual attack occurs and prevent the network from malicious attack.

Key words: Mobile, CCLAM, network, flag, MANETs

INTRODUCTION

In Classic Cluster Layer Architecture (Sharma *et al*., 2012) Mobile ad hoc networks (CCLAM), we assume that confidentiality, integrity and authenticity of the forwarded packets are provided by different nodes. Excellent work is available in this field, e.g., making new secure architecture for MANET which refers to an overview of Cryptographic Methods which providing encryption of packets, checksums where nodes are transmitting and access control of all ordinary nodes. However, especially in CCLAM, it cannot be possible that ordinary nodes owning valid cryptographic keys (such as UNID and TNUID) are taken over by an attacker. Therefore, it is difficult to understand whether a node despite having valid keys and recent proper and accurate behavior is behaving correctly or maliciously. There are different layers on which a node can behave maliciously. For example, an application may create fake traffic in order to run a denial-of-service attack. In this study, we focus on recognizing nodes spreading illegitimate routing information. Recent related researchers focuses on securing existing or developing secure protocols to prevent routing attacks or using intrusion detection to detect such attacks (Table 1).

In this study, we present a Classic Cluster Layer Architecture approach for detecting routing attacks against the Optimized Link State Routing protocol (OLSR).

Table 1: Layered wised attackers (Sharma *et al*., 2012)

Layers	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes and application abuses
Transport layer	Authenticating and securing end to end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

This new approach tries to detect fake HELLO messages by performing proper tests at a central node against a network topology graph.

AD HOC NETWORK THREATS CCLAM

In ad hoc networks devices (also called nodes) act as everything such as administrator, database manager and routers. In CCLAM, most of ad hoc routing protocols make's ordinary nodes to exchange network graph information in order to establish perfect communication routes. These informations are sensitive and can become a target for malicious adversaries who think to attack the network or the applications running on it. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information or distorting routing information an attacker could successfully partition a network or introduce a traffic

Corresponding Author: Kuldeep Sharma, Anna University, Coimbatore, India

overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes which might misuse routing information to other nodes or act on applicative data in order to induce service failures. The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today (Karpijoki, 2000).

BLACK HOLE ATTACK AND CLASSIFICATION

In black hole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into black hole in universe. So, the specific node is named as a black hole. A black hole has two properties. First, the node exploits the ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets. Black hole attacks in AODV protocol routing level can be classified into two categories: RREQ black hole attack and RREP black hole attack (Chauhan *et al*., 2012).

Black hole attack caused by RREQ: An attacker can send fake RREQ messages to form black hole attack. In RREQ, black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. Other nodes will update their route to pass by the non-existent node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ mssage as follows (Varshney and Khare, 2012):

- Set the type field to RREQ
- Set the originator IP address to the originating node's IP address
- Set the destination IP address to the destination node's IP address
- Set the source IP address (in the IP header) to a non-existent IP address (black hole)
- Increase the source sequence number by at least one or decrease the hop count to 1. The attacker forms a black hole attack between the source node and the destination node by faked RREQ message as it is shown in Fig. 1

Black hole attack caused by RREP: The attacker may generate a RREP message to form black hole as follows:

- Set the type field to RREP
- Set the hop count field to 1

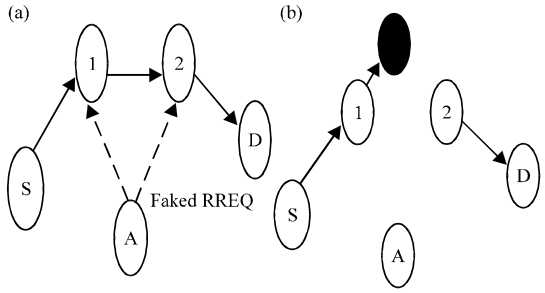

Fig. 1: Black hole is formed by faked RREQ

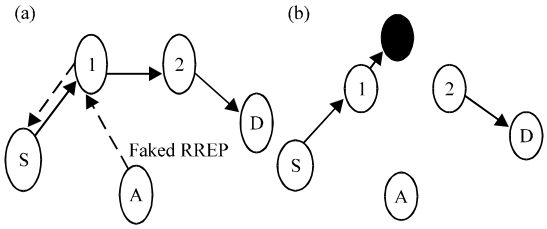

Fig. 2: Black hole is formed by faked RREP

- Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route
- Increase the destination sequence number by at least one
- Set the source IP address (in the IP header) to a non-existent IP address (black hole). The attacker unicasts the faked RREP message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node (Varshney and Khare, 2012). Then, RREP black hole is formed as it is shown in Fig. 2

PROPOSED CCLAM

In clustering my procedure, a representative of each sub-domain (cluster) is 'elected' as a Master Node (MN) and a node which serves as intermediate for inter-cluster communication is called gateway. Remaining members are called ordinary nodes. The boundaries of a cluster are defined by the transmission area of its CH. With an underlying cluster structure, non-ordinary nodes play the role of dominant forwarding nodes.

In this clustering, procedure I have in divided cluster in to three core cluster layers such as core cluster, core cluster layer 1 and core cluster layer 2 (Fig. 3).

MANET can be divided into several overlapped clusters. And cluster can be divided in to three layers. A cluster comprises of a subset of nodes that communicate via their assigned MN. The network is modeled as an

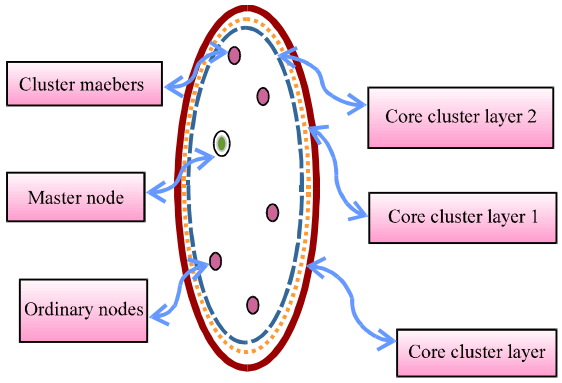

Fig. 3: Cluster layers, master node and ordinary nodes in mobile ad hoc network clustering

undirected graph G(V, E) where V denotes the set of all MHs (vertices) in the MANET and E denotes the set of links or edges (i, j) where i, j∈V.

Working of CCLAM over black hole attacks: As I discussed before how black hole attacks occur in MANET and what effect it do over MANET. In this study by using of my proposed CCLAM Model for MANET I am giving how CCLAM is able to solve and stop black hole attacks in MANET (Fig. 4).

Here, we will try to solve and stop black hole attacks one by one. As we know when researchers apply AODV protocols in MANET that time the possibilities of black hole attack increase. So, first we have to know what happen when AODV protocols research. When we apply AODV protocol that time two major conditions apply one RREQ and second RREP. RREQ says while connecting one node to another node first node should broadcast RREQ packets to next near by all nodes by saying his identification. And another all receiver nodes should reply to sender nodes by sending their identification call RREP. In between this process there is no proper channel to check their identification. And because of there are no proper identification check so that attackers takes advantages come inside over MANET generate black hole attacks.

In my proposed CCLAM I have given solution to stop this black hole attacks by using some tables which will maintained by master nodes and some tables are going to maintain by ordinary nodes available on their cluster. The table maintains IDs of every ordinary nodes and another table is going to maintain master nodes IDs.

In this study, I am proposing how we can stop black hole attacks by using my proposed CCLAM architecture. In my architecture I proposed classic cluster layer who says:

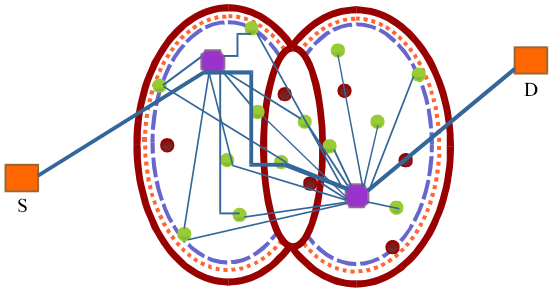

Fig. 4: Working model of new classic cluster layer architecture MANET

- All clusters are having limited range and depending on master nodes range
- Clusters can collapse with each other
- Collapsed area will call common cluster
- Cluster will maintain three separate layer to secure master node position
- Those three layer will called as core layer, core cluster layer 1 and core cluster layer 2

So, if any attackers will try to come in the network he has to face first challenge to get in the network because ones he entered in the network master node will ask him his identification and master node will only verify whether given identification is correct or not. Before giving solution how CCLAM is going to stop let me explain small description about master node:

Master node characteristics:

- All master nodes will be dynamic
- Every cluster should have one master node
- All master nodes should maintain all database tables
- Only master nodes can change time being assigned unique Id for nodes and master nodes
- After changing of TNUI of every nodes and own every master nodes will share all changed new updated database
- After changing of TMNUI master nodes will share the update with every nodes and every master nodes of each cluster
- After every updating master nodes will verify with all shared nodes and master nodes
- If any nodes cross cluster layer 2 instant one message will go to master nodes available on that cluster
- Master node will send one MSG to that nodes and inform him that he is going out of range
- If that node will not listen and continuing to go out of cluster layer 1 then again master node will send him warning that not to move out of rang otherwise your will become defaulter node

- After crossing of core cluster layer MN will send a request to all MN that any node has entered in your area
- If that node entered in other cluster area then that's node responsibility to update himself with new clusters MN
- If all MN will reply that no updating that time that node will become defaulter and that will go to defaulter_node_table

As we have seen that how and what MASTER Nodes do and what are the master nodes responsibilities (Madan and Anu, 2014).

STOP BLACK HOLE ATTACKS (PROPOSED)

Scenario 1 (attackers will try to come in side the cluster): As we know master node will sent one information massage to his clusters all ordinary nodes to get information about what are the nodes are available in cluster and after that master node verify those ordinary nodes Ids from his available data base where he is maintaining one table named Cl_Node_Table who contain information of all nodes available at clusters range include common cluster nodes. Common nodes will contain by both cluster table. This table will contain by master nodes and all nodes.

So, if attackers try to come in side the cluster he has to face first verification and information massage asked by master nodes.

Scenario 2 (attacker node can hack any ordinary nodes Ids and reply with those Ids): As we seen master nodes are containing tables in the named of Ms_Node_Table, TNUI_Node_Table and Node_Table 1 whom job is to maintain free nodes and busy nodes contain unique Ids and temporary unique IDs by which every nodes has to follow some rules and reply to master nodes.

Here, if attackers use hacked ordinary nodes ID he can hack only TNUI (Temporary Unique node ID) but if he want to hack NUI (Node Unique ID) which is going to maintained by only master node is not possible. So, he can hack only TNUI which is going to change every certain time and while changing that node id master node use to verify TNUI and NUI and this condition master node will get twice same TNUI so easily we can identify there is some problem with some nodes and easily we can get the information who is the node by cross verification.

In cross verification master nodes will send one massage who will contain TMNUI (Time being assigned Master Node Unique Id), TNUI, CLUID (Clusters Unique ID) with last five changed TNUI which are going to change by master node and which is going to contain in record in master nodes. Definitely those information are not available with attackers node so that that attackers node will be drop.

Algorithm to prevent cooperative black hole attack in MANETs:

Notations:
MN: Master Node
SN: Sender Node
IN: Intermediate Node
RN: Receiver Node
NON: Next Ordinary Node
TRq: Tempory Request
TRp: Tempory Reply
Reliable node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identification of the node
TNUI: Tempary Node Unique Identification
UNI: Unique Node Identification

1. SN broadcasts RREQ
2. IN receives RREP
3. Check Authentication of IN through MN
4. IF (RREP is from DN or a reliable node) {
5. Route data packets (Secure Route)
6. }
7. ELSE {
8. Do {
9. MN send TRq to SN ask ID with proper TNUI
10. Receive TRp with given step 9
11. Varify SN ID with UNI
12. IF (TNUI is of reliable node) {
13. Check IN for black hole using DRI entry
14. IF (IN is not a black hole)
15. Route data packets (Secure Route)
16. ELSE {
17. Insecure Route
18. IN is a black hole
19. All the nodes along the reverse path from IN to the node
20. that generated RREP are black holes
21. }
22. }
23. ELSE
24. Current IN = NHN
25. } While (IN is NOT a reliable node)
26. }

SIMULATION AND RESULTS

To test the method, we develop an event driven simulator by using NS2. The NS2 program is used to set up the simulation environment and compute the actions of all nodes between route discovery processes. Then, we visualize the simulation results by using NS2.

We assumed each node is distributed randomly by the simulator and each node will send and receive packets with different delays in an allocated range. The source establishes a route discovery broadcast by sending the RREQ packet. Here is one ordinary node who is sending again and again RREP packet in response of RREQ so, we simulated with finding the face ordinary node and block that ordinary node. Here, for the time being entire route destroyed and sender node again started from beginning to establish new route for making

perfect route between sender and receiver. The source node then selects the legal routes. Furthermore, the simulator allows users to input the RREPlim value for each simulation. We can input different RREPlim for each simulation and the simulator completes the request as required.

In this study, we give experiments to show the performance of the proposed CCLAM Model and protocol. In Table 2, we give the parameters used in the experiments.

Here, we perform the simulation in two way first without black hole attack and second with black hole attack. When we check with black hole attack immediate one warning packet generated by master node and forwarded to all ordinary nodes available in cluster and same packet forwarded to another clusters master nodes by giving information of fake ordinary node (Fig. 5).

As we seen how CCLAM is able to stop black hole attack here I am going to explain overall how CCLAM is working in case of black hole attack. Ones if any unidentified node will try to get in CCLAM he has to face so, many verification process. Which all he can clear by knowing the any ordinary nodes IDs. If any condition he will be able to hack ordinary nodes Ids and definitely master node will come to know similar ids so master node will start next verification process where master node will ask those thins which has been assigned confidentially to every ordinary nodes and here master nodes has given one another table to all ordinary nodes named TMNUI_Node_Table where while replying to master node during verification ordinary node has to reply with using master nodes time being assigned unique IDs which will be cross verified by master nodes. After all verification only master nodes will allow communication till that time those two nodes will not allowed for any communication process. So, by using this proposed solution we can easily stop black hole attacks.

Table 2: Parameters for experiments

Parameters	Values
Number of CCLAM	3
Number of ordinary nodes in one cluster	300
Field dimensions (MN max range)	2,000×2,000 m
Radio range (Max. of ON)	250 m
Node delay random	At the rate of 0.05~0.075 msec
Trial	50 times

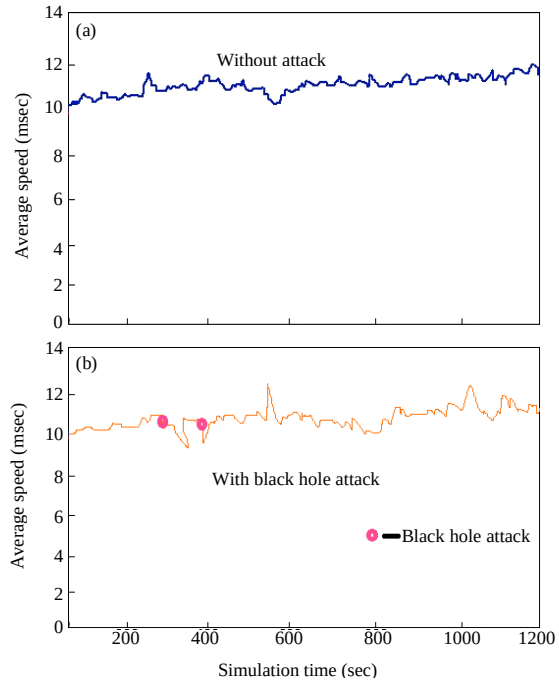

Fig. 5: Simulation result without attack and with attack

CONCLUSION

The proposed CCLAM architecture is able to stop all kind of attackers and its easy to implement in real life. This CCLAM architecture is very different from other architecture available in market because the architecture and protocols which are available in market they all are not sufficient to stop attackers. As per my proposed solution I tried to stop all attackers and I used only available protocols like AODV.

RECOMMENDATIONS

In future I am trying to find out loop holes in this architecture and I am going to make this architecture stronger then strong. And still I am testing this architecture with all other attackers.

REFERENCES

Chauhan, Y., J. Singh, M. Tiwari and N. Khare, 2012. Performance Evaluation of AODV based on black hole attack in ad hoc network. Global J. Res. Eng.: Electr. Electron. Eng., 12: 39-43.

Karpijoki, V., 2000. Security in ad hoc networks. Proceedings of the Helsinki University of Technology Seminar on Network Security, December 4-5, 2000, Finland, pp: 1-16.

Madan, A. and Anu, 2014. Survey of security mechanism in wireless AODV. Int. J. Adv. Res. Comput. Sci. Software Eng., 4: 612-615.

Sharma, K., N. Khandelwal and S.K. Singh, 2012. New proposed Classic Cluster Layer Architecture for Mobile adhoc network (CCLAM). Int. J. Comput. Sci. Secur., 6: 94-102.

Varshney, H. and A.R. Khare, 2012. Mobile adhoc network routing security analysis: Blackhole detection and prevention. Global J. Comput. Applic. Technol., 2: 948-951.