Detection and Defense Against Packet Drop Attack in MANET

Tariq Ahamad
College of Computer Engineering & Sciences
Prince Sattam Bin Abdulaziz University, Saudi Arabia

***Abstract*—MANET is a temporary network for a specified work and with the enormous growth MANETs it is becoming important and simultaneously challenging to protect this network from attacks and other threats. Packet drop attack or gray hole attack is the easiest way to make a denial of service in these dynamic networks. In this attack the malicious node reflects itself as the shortest path and receives all the packets and drops the selected packets in order to give the user the service that that is not correct. It is a specific kind of attack and protects the network and user from detecting this malicious activity. In this article I have proposed an efficient for step technique that confirms that this attack can be detected and defended with least efforts and resource consumption.**

Keywords—MANET; gray hole; DoS; packet drop; security

I. Introduction

MANET (Mobile Adhoc Network) is a dynamic mobile network that can exist and can be formed without any predefined and preexisting network and communication network1 .The concept of Ad Hoc network depends on the availability of the devices that are to be connected to each other to form the network2. Thus, unlike other existing and traditional networks, these networks do not depend on any pre-existing network or infrastructure to carry out their operations and their this dynamic character reduces their cost and implementation time.

The backbone of the Ad Hoc Network is the routing protocols that enable multi – hop data transfer or communication in these networks[3]. Since the topology of these dynamic networks keep on changing so changes the attacks on these networks and in order to deal with these malicious attacks these routing protocols must be robustic[4]. The pre-existing routing protocols easily deal with changing topologies but the malicious attacks always remain the issue to be fixed. In this article I have evaluated the robustness of existing routing protocols against the malicious attacks and assess the quality and impact of security improvements.

II. Threats in Ad Hoc Networks

Reliability of the devices or nodes that are to be used to form an Ad Hoc network is most important concept to be kept in mind as devices or nodes act both as computers and routers. Since the topology keep on changing due to dynamic behavior of the network, this change is supported by routing protocols so as to establish the dynamic routes[5] . Since routing information is very sensitive and can be targeted by the attackers in order to harm the network or the applications running in the network as illustrated in the figure 1.

Since all the Ad Hoc Networks thoroughly depends on Routing protocols, there are many sources that make use of this idea and attack them and the two major sources are:

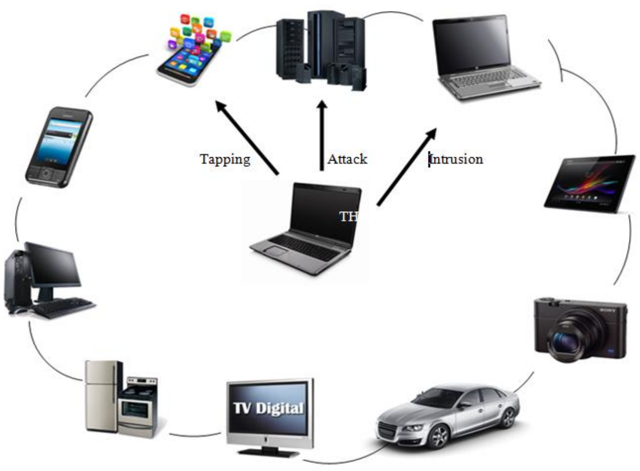

Fig. 1. Attack in Ad Hoc Network

1) As per the basic cyber attack practice, the first comes from explicit attackers. By inserting a new large pool of routes or using old routing information or distracting the current routing pool, an intruder can divide the network or delay the traffic and can cause inefficient routing and affect the quality of service (QoS).

2) The most dangerous and that can cause severe effect to the dynamism and reliability of Ad Hoc Network comes from inside the network by gray nodes or gray hole (compromised nodes) and can exploit the routing information of the other nodes and can affect the service as they are the part of the network.

III. Packet Drop Attack (Gray Hole)

Packet drop attack (gray hole) is a denial of service (DoS) attack in which a router relays or drops data packets instead of discarding for a specific network destination at specific time – a packet after every n number of packets or after every t number of seconds[6]. It is slightly different from black hole as black hole is a general denial of service (DoS) attack that drops packets as its key constraints are very specific. It is an active attack that leads dropping of packets[7]. The attacking node at first agrees to forward data packet or messages then fails to do so and starts behaving like a malicious node[8]. At first the attacker node behaves normally and replies true route replies(RREP) messages to other nodes to invoke route request (RREQ) messages and accepts or takes the sending packets and finally drops few or all packets to launch denial of service (DoS) attack[9]. If nodes in the neighborhood try to send data packets over attacking or victim nodes lose connection to target or destination node or network and may want to discover or rebuild a route again by broadcasting route request (RREQ) messages. Attacking node send route reply (RREP) messages to establish route[10]. This process doesn't stop until attacking node achieves its goal like battery power consumption, bandwidth consumption etc.

IV. Proposed Mechanism

We will start by making some assumptions and are going to be considered for formulating network model and later present the complete details of the proposed system.

A. *Basic network model*

The first thing that we are going to consider is assuming that a MANET (Mobile adhoc network) consists of almost similar types of devices. Every device may travel aimlessly or stay immobile in a specific location for a temporary slot of time. Also every device may leave or join the network or even fail at any instance of time. The MANET (mobile adhoc network) follows peer to peer networking principals over fixed shared bandwidth and multihop wireless nodes. Assuming a non-zero ID for each node to differentiate between them and all the channels and links in the MANET (mobile ad hic network) to be bidirectional. The proposed technique doesn't make any assumption malicious mode operations of the wireless nodes interface as compared to current security frameworks. The malicious node may not only experience or face extra computation and power consumption in processing the moving data packets, but also will not be effective where devices have equipped directional antennas. The number of packet drop nodes may vary at different instances of time in the MANET (mobile adhoc network) and may disturb or decline the MANET communication by cooperating with each other.

B. *Modules of the proposed mechanism*

My Suggested technique will use two detection procedures i.e., local and cooperative detection models to recognize malevolent node (grayhole) in MANET (Mobile Ad Hoc Network. The moment malevolent node is recognized and confirmed the mechanism has a notification procedure added that sends a message to all the nodes , so as to identify the malevolent node and isolate the malevolent node and make sure that it is not allowed any access to anypart of the MANET and its resources.

My mechanism is a four step scheme and all the four steps are invoked sequentially. Following are the four steps.

1) *Multihop Data Collection (MDC)*
2) *Local Anomaly Detection (LAD)*
3) *Collective Anomaly Detection (CAD)*
4) *MANET Alarm*

C. *Multihop Data Collection (MDC)*

Every node in the MANET gathers packet forwarding data in its surrounding multihop zone and saves that in the Data Routing Information Table (DRIT). Figure 2, shows DRIT of node 5 and the numbers used in DRIT shows that node 5 maintains data routing information of neighboring nodes 4, 6, 7, 8, 9. As per table 1, in row one column "from" indicates as node 5 has sent the packet received from corresponding one and column "thru" from same row indicates that node 5 has sent the data packet to that node. So, node 5 neither received nor sent any packet towards node 4 as mentioned in the Table 1. However, node 5 forwarded and collected data packet from and to node 6. So, following this approach each node creates and maintains a DRIT. After a fixed time interval, every node recognizes its hop nodes with which it hasn't been involved for data communication and calls on a detection procedure to investigate them further. This investigate is done on those nodes which have 0 (zero) entries in both the columns i.e., "from" and "thru" in DRIT. Thus as per table 1, node 5 invokes local detection scheme for node 4. In row one of DRIT with column "RTS/CTS", the ration "RTS/CTS" gives an approximate idea regarding the amount of entreaty approaching for communication and amount of data packets transmission that the selected node is executing in real time. The importance and use of "checkbit" in Data Routing Table is explained in the next step.

D. *Local Anomaly Detection (LAD)*

This method or mechanism is initiated by a node after recognizing and confirming a node as suspicious by inspecting DRIT. Initiator node initiates or invokes the LAD procedure and chooses cooperative node in the neighboring nodes after checking its DRIT and cybercasts a RREQ (route request) packet to its first-hop nodes, seeks route thru cooperative node. The initiator node will receive a good amount of RREP (route reply) packets from its multihop area to its RREQ (route request) message and surely will receive and experience a RREP (route reply) from the doubtable one as well, if it really is a packet drop node. Once RREP is sent by the suspected node and the moment it is received from the suspected node (SN), the initiator node sends enquiry or probe data packet to the cooperative node (CN) thru the suspected node (SN) and enquires the cooperative node whether it received the enquiry packet or not , right after given interval of time i.e. time to live (TTL). The initiator node updates its data routing information table by using adding 1 (under "chekbit" against suspected node's NID), right after it receives confirmation that the cooperative node has received the enquiry data packet. In case , if the enquiry or probe packet does not reach the cooperative node then the initiator node rises its degree of intuition about suspected node and invokes the (CAD) co-operative anomaly detection scheme.

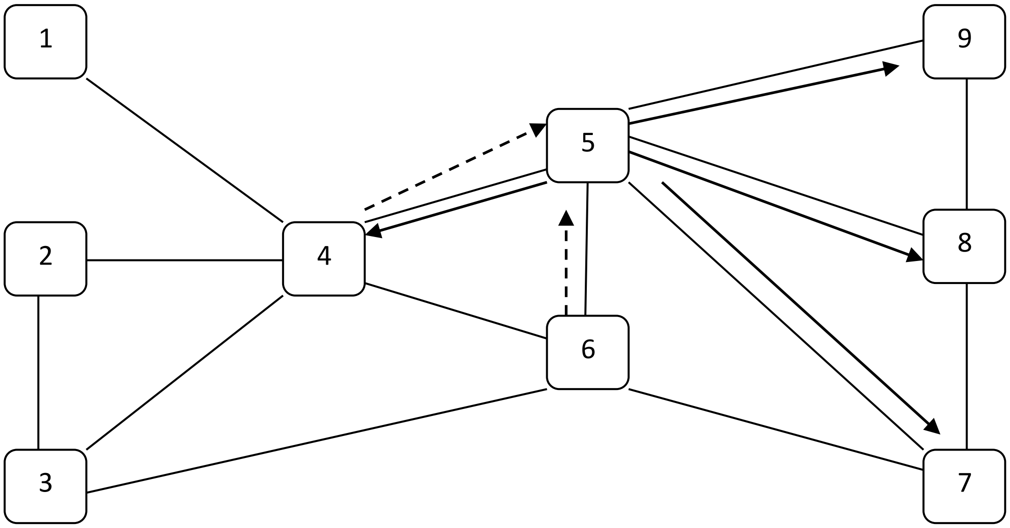

Fig. 2. MANET Topology

TABLE I. DATA ROUTING INFORMATION TABLE (DRIT)

NID	From	Thru	RTS/CTS	Check Bit
4	0	0	15	0
6	1	1	5	1
7	0	1	3	0
8	1	0	6	1
9	0	1	4	0

In figure 1, initiator node, Node 5 invokes LAD procedure for the suspected node (SN) 4 and selects node 6 as the cooperative node because both the entries of node 6 are 1 under "from" and "thru" columns and becomes most reliable and trustworthy node for node 5. Node 5 cybercasts a RREQ (route request) packet to all its 1-Hop nodes i.e. 4, 6, 7, 8, 9 and request for a route to cooperative node Node-6. After receiving a route reply (RREP) from suspected node 4, node 5 sends an enquiry packet to the node 6 via node 4 and confirms from node6 about probe packet. If node 6 confirms that it received the enquiry packet then node 5 makes an entry and adds 1 under "checkbit" column corresponding to node 4 in DRIT. And in case node 6 doesn’t confirm on the arrival of enquiry packet then node 5 initiates the cooperative detection anomaly scheme.

E. Cooperative Anomaly Detection (CAD)

This mechanism increases the detection influence by the decreasing chance of false and fake identification of local anomaly detection (LAD) scheme. The CAD mechanism is initiated whenever an initiator node notice that the enquiry data packet didn’t reach the cooperative node via suspected node. The initiator node initiates cooperative identification scheme (process) and broadcast a CAD request packet to all the 1-hop nodes of the suspected node. When the neighboring nodes of the malicious suspected node accepts the cooperative identification request packet then each of the neighboring nodes sends route request (RREQ) to the suspected node seeking a route to initiator node. Once the suspected node reacts with a Route reply (RREP) message, every node forwards a "further-enquiry-packet" to the initiator node including the same route. This route definitely will include suspected node because suspected node is 1-Hope (neighbor) of every requesting node even the initiator node. Each neighboring node of suspected node (except initiator node) now informs the initiator node that one more packet called "further-enquiry-packet" has already been forwarded to it and this alerting packet from every neighboring node is forwarded towards the initiator node thru the routes that do not involve node. This step is extremely important to assure that suspected node is not aware of this ongoing process of cross check. The initiator node will receive a lot of further-enquiry-packets and alerting packet. The initiator node prepares a Probe-Check-Table and will have only two fields i.e. NID (Node ID) and PS (ProbeStatus). NID field will have identifiers of nodes from which it have received the notification message. Entry "1" is put under the PS (ProbeStatus) communicating to the nodes which sent Further-Enquiry-Packet to initiator node as shown in Table II.

TABLE II. NID=NODEID, PS=PROBE STATUS

NID	PS
6	0
7	1
8	1
9	1

If the suspected node behaves like a malicious node or packet drop node, it is kept away and secluded from MANET by initiating the global-alarm-detection procedure. The frequency of invoking the detection and identification procedure is key factor for assuring the expected output in the MANET because packet drop node can shift its state from good to bad frequently. The frequency of the invoke calls of the identification procedure must be prepared on highest number of data packet drops that the MANET app tolerates. In the worst case scenario, malicious node shifts its state from nice to worst right after the invoked wound of detection algorithm is done and can return back to nice state before the next invoke call. Although these situations are rare, the invoke call frequency must be calculated on the approximation of the amount of data packets dropped by packet drop node during that time slot and the highest value of packet drops that is applicable to maintain the expected and sought QoS (Quality of Service).

F. MANET Alarm

This scheme is initiated to form or create a "network-wide-notification-system" in order to send alarm packet to all the nodes and devices in Mobile Adhoc Network (MANET) about the (malicious node) packet drop node that has been detected by CAD scheme. It also certifies that none of the network resources or services to be allowed to these malicious nodes and are kept isolated from the rest of MANET (Mobile Adhoc Network).

A security problem arises after the identification and isolation procedures of suspected nodes. A set of malicious nodes (gray hole) can collaborate to hurl a malign attack by falsely incriminating legal node and segregate it from the MANET (simple isolates a legitimate node). To prevent this in the MANET. I suggest a procedure that is somehow similar to existing thresh hold cryptography. In my proposed procedure, when a cooperative-detection-procedure identifies and confirms a SN to be gray hole initiated by a node, broadcast an alarm message digitally signed using its private key. The complete sign is created only when at least “n” number of nodes put their signs into the alarm message. The suspected node (malicious node) is kept away from the MANET after the alarm message is verified and authenticated with full signature. Thus our proposed mechanism is strong and feasible against collusion that involves maximum n-1 malicious nodes (gray hole) in an area inside MANET. Once the node is identified and confirmed as malicious node, its NID (node ID) is entered into “Malicious_node_list” a global list file of malicious node. This Malicious_node_list is broadcasted in the MANET periodically whenever an update is made to it. The Malicious_node_list can be adjoined with the routing message RREQ and RREP. So that there must not be any extra overhead. On the other hand, every node may keep a partial record of faulty nodes which are in its 1-Hop neighborhood. This existing partial record must change and update whenever its neighborhood changes. Since the nodes require to know the whereabouts of its multihop nodes for routing only, this procedure will be best fit for protocols, AODV in particular.

V. Conclusion

In my research article, I have proposed a reliable and efficient mechanism for detecting packet drop attack in Mobile ad hoc networks (MANET). Due to their dynamic phase shifting character, it is difficult to detect them. My proposed technique will boost the reliability by presciently initiating a cooperative scheme that involves neighboring nodes of malicious node. Suspect and detection decision are done with the help of consensus algorithm that is based on thresh hold cryptography. The proposed mechanism is efficient and effective with controlled overhead and great detection rate.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2015/2016 under research number 2015/01/3850.

References

[1] Ahamad T, Aljumah A. "Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology. 2015 Dec Vol 8(33).

[2] Aljumah A, " Detecting Distributed Denial Of Service (Ddos) Attack Using TTLv Constraint In Mobile Adhoc Networks (MANET) ", Science Internationals, 2015 Dec Vol 27(6),5037-5040.

[3] Ahamad T, Aljumah A. ,"Ad Hoc Network & Black Hole - Threat and Solution". American Journal of Scientific Research , Issue 104 , Nov, 2014.

[4] Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.

[5] Abdelhaq M, Hassan R, Ismail M. A study on the vulnerability of AODV routing protocol to resource consumption attack. Indian Journal of Science and Technology. 2012 Nov; 5(11):3573–7.

[6] Ahamad T, Aljumah A," Hybrid Approach Using Intrusion Detection System", International Journal of Engineering Research & Technology, Vol. 3 Issue 2, February - 2014

[7] Tsou PC, Chang JM, Lin YH, Chao HC, Chen JL. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 13th International Conference on Advanced Communication Technology: Seoul; 2011 Feb 13-16. p. 755–60.

[8] Baadache A, Belmehdi A. Avoiding black hole and cooperative black hole attacks in Wireless Ad hoc Networks, International Journal of Computer Science and Information Security. 2010; 7(1):10–6.

[9] Arunmozhi S.A., Venkataramani Y."A Flow Monitoring Scheme to Defend Reduction-of- Quality (RoQ) Attacks in Mobile Ad-hoc Networks", Information Security Journal: A Global Perspective, Vol.19, No.5, 2010, pp.263- 272.

[10] Hyojin K, Ramachandra B. C., JooSeok S,"Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010, pp. 579-582.

[11] Mistry N, Jinwala D. C., Zaveri M,"Improving AODV Protocol against Blackhole Attacks", Proceedings of the International Multiconference of Engineers and Computer Scientist, Hong Kong, Vol. II, 2010.