International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

A Survey on Detection of Packet Dropping Attacks in Wireless Adhoc Network

Shridevi K[1] ,Naziya Parveen[2]

[1] Department of Computer Network Engineering,
Secab Institute of Engineering and Technology Vijayapur

[2] Department of Computer Network Engineering,
Secab Institute of Engineering and Technology Vijayapur

Abstract

Wireless adhoc network is emerging fast due to its unique feature such as easy to deploy. There are various security issues. These security issues are due to the packet drops in the network. The nodes in the network co-operate each other to forward the packets from source to destination. The adver zry may exploit this cooperative nature by dropping the packets. The packet dropping may be either by the presence of malicious node or link error. There are various methodologies to detect and isolate the cause for the packet drop. In this paper the survey is carried out for the detection and isolation of packet drop.

Keywords: Link error, adhoc network.

1. INTRODUCTION

A wireless adhoc network [1] is a collection of wireless nodes that can be dynamically self-organized into an arbitrary and temporary topology to for a network without necessarily using any pre-existing infra-structure. In adhoc networks each node may communicate directly to each other. Nodes that are not directly connected can communicate through intermediate nodes. The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes so that messages can be delivered in a timely manner. There are some security issues related to the wireless adhoc network such as unstructured and/or time varying network topology which is because of the nodes mobility, the network topology changes which makes the network unstructured, scalability due to huge number of nodes in the network, low-quality communications due to the open nature, wireless network are affected by the environmental factors and due to the exploitation of adversary nodes in the network.

This paper demonstrates the detection of cause for the packet drop attacks which is due to the malicious node or due to the link error. In this paper we are comparing the packet dropping attacks using different protocols. The protocols considered are dynamic source routing protocol, adhoc on-demand distance vector routing protocol, and optimized link state routing protocol.

The rest of the paper is organized as follows. Section 2 describes an overview of DSR protocol, Section 3 provides an overview of AODV protocol, Section 4 deals with an overview of OLSR protocol, Section 5 presents the Solutions to the packet dropping attacks, Section 6 presents a comparison table among the solutions and finally, conclude the paper with plan for future work in Section 7.

2. OVERVIEW OF DSR PROTOCOL

The Dynamic Source Routing protocol (DSR) [3] is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use.

3. OVERVIEW OF AODV PROTOCOL

The Ad-hoc On-Demand Distance Vector (AODV) [4] is a reactive routing protocol designed to have intention for use in mobile ad hoc networks. It finds a route to a destination when a node likes to transfer a packet to that destination. Routes are maintained by the source node as long as they needed. Route discovery process is based on the route information is stored in all intermediate nodes along the route in the form of route table entries. Every node has routing table, it has the fields like destination, next hop, number of hops, destination sequence number, active neighbors and lifetime respectively. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are used to find the freshness of routes towards the destination. When a route is not available for the destination, a route request packet (RREQ) is flooded

throughout the network. The RREQ contains source address along with request ID is incremented each time the source node sends a new RREQ and identifies it uniquely. On receiving a RREQ packet, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters the new RREQ packet will be discarded Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP packet: once a RREP packet is received, the route is established . A source node may receive multiple RREP packets with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information. While transmitting RREQ packets through the network, each node notes the reverse path to the source. When the destination node is found, the RREP packet will travel along this path.

4. OVERVIEW OF OLSR PROTOCOL

An Optimized Linked State Routing (OLSR) [5] is an important proactive routing protocol designed for adhoc networks. It employs periodic exchange of messages to maintain topology information of the network at each node. Based on topology information each node is able to calculate the optimal route to a destination. In OLSR routes are immediately available when needed and the key concept of this protocol is the use of Multipoint Relays (MPR). Each node's selects the set of its neighbor nodes as its MPR. The nodes which are selected as MPR's are only responsible for generating and forwarding topology information. The core functionality of OLSR protocol includes neighbor sensing, multipoint relay selection, topology diffusion and routing table calculation.

5. SOLUTIONS TO THE PACKET DROPPING ATTACKS

L.Buttyan and J.-Y Hubux [6] demonstrated a paper titled "Stimulating Cooperation in Self-Organizing Mobile Adhoc Networks". This is based on credit system which provides the incentives (nuglets) for co-operation or for the packets they forward and spend the credit to transmit their own packets. In this system nuglet counter and tamper proof hardware called security module is maintained. Nuglet counter to record the nuglets and security module prevents the counter from becoming negative or being modified. The secure module is required to ensure the withdraw or deposition of correct number of nuglets. There are two models for the payment of packet forwarding namely packet purse model and packet trade model. In the packet purse model the sender pays and thus loads the packet with a number of nuglets. Each intermediate node takes one nuglet when it forwards the packet. If there are no nuglets left at an intermediate node the packet is dropped. If there are nuglets left in the packet once it reaches the destination the nuglets are lost. In the packet trade model the destination pays for the packet. Each intermediate node buys a packet from the previous node and sells it to the next for more nuglets. Since charging the destination can lead to an overload of the network. This model leads to the loss of nuglets which have to be re-introduced into the network by a central authority.

S.Marti, T.Giuli, K.Lai and M.Baker [7] proposed a paper titled "Mitigating Routing Misbehavior in Mobile Adhoc Network" where Reputation Based System is used to keep track of the quality of behavior of other node in an adhoc network. Basically reputation is a opinion formed on the basis of watching node behavior. Reputation can be calculated by direct observation and/or indirect observation of the nodes through route behavior, number of transmissions generated by the node, through acknowledgement message and by overhearing node's transmission by the neighboring nodes. The first goal for reputation system to be used in a network is to provide information to check whether a node is trustworthy or not. The second goal is to encourage nodes to behave in trustworthy manner. The drawback of this system is that neighborhood monitoring becomes complex in case of multi channel network. Neighboring nodes may be engaged in parallel transmission in different sectors thus unable to monitor their peers.

K.Liu, J.Deng P. Varshney and K. Balakrishnan [8] proposed a paper titled "TWO ACK: preventing selfishness in mobile ad hoc networks". Here the systems rely on acknowledgements to verify whether the packets are forwarded or not.2Ack system is proposed which is used to detect the misbehavior routing; it also checks the confidentiality of message in adhoc network. In this system the destination node of the next hop link will send back an acknowledgement to indicate that a packet has been received successfully. If 2ack time is less than the wait time and the original message contents are not altered at the intermediate nodes then a message is given to a sender that the link is working properly. If the acknowledgement time is more than the wait time then a message is sent to a sender that the link is misbehaving. At the destination the hash code will be generated and compared with sender's hash code to check the confidentiality of the message.

S.Zhong, J.Chen, and Y.R. Yang [9] proposed a paper titled "Sprite: A Simple, Cheat-proof, Credit Based System for Mobile Adhoc Networks" where credits are provided to the cooperative nodes. When a node receives a message it keeps a receipt of message, later the node reports the message to the credit clearance service (CCS) indicating that the message have been forwarded or received. Then ccs gives the charge and credit to each node involved in the transmission of message depending on the receipt of a message. Advantage is that it removes the use of security module and uses ccs. The drawback is that there is an excessive burden on sender which loses credit for forwarding of its message.

Rekha Kaushik and Jyoti Singhai [10] proposed a paper titled "MODSPIRITE: A Credit Based Solution to Enforce Node Cooperation in Adhoc Network". This system is a modification of SPIRITE system, Here a node when receives a message keeps receipt of the message. It then communicates with the cluster head which is responsible for credit and debit of charges to nodes when they receive

or forward messages to other nodes in the network. Usage of cluster head reduces the burden of security module and CCS.

Bounpadidth, Hidehisa Nakayama, Nei Kato, Yoshiaki Nemoto and Abbas Jamalipour [11] described a paper titled "Analysis of Node Isolation Attack against OLSR based mobile adhoc networks". By using OLSR protocol information regarding neighbor node is obtained by broadcasting the hello message. This hello message performs the task of sensing the neighbor nodes and MPR selection process. A nodes hello message contains its own address, a list of its 1-hop neighbors and a list of its MPR set. Therefore by exchanging hello messages, each node is able to obtain the information about its 1-hop neighbor and can find out which node has chosen it as an MPR. In order to disseminate the topology information the node that were selected as MPR must generate a topology control (TC) message periodically. A nodes TC message contains a list of MPR selector set. Upon receiving TC message of all MPR nodes in the network. Each node learns all nodes MPR set and hence obtains the knowledge of the whole network topology. Based on this topology, the nodes are able to calculate routing table. Each entry in the table consists of destination address, next hop address, distance and nodes own address. The routing table's calculation is based on Dijkstra's algorithm for finding shortest path. The routing table is updated when a change is detected in 1-hop neighbor and 2-hop neighbor. It is recalculated in case of neighbor lost or 2-hop neighbor is created or removed. They have proposed a model called node isolation attack model where victim node is detected and isolated from the network by hearing hello message and TC message periodically. The victim node can only forward the fake hello message but it is unable to generate and forward TC message. The drawback is that it might not detect the attack which is launched by two consecutive nodes who work in collusion.

Rajendra Aaseri, Pankaj Choudhary and Nirmal Roberts [12] proposed a paper titled "Trust Value Algorithm: A Secure Approach against Packet Drop Attack in Wireless Adhoc Network". They have proposed an algorithm called Trust Value Algorithm and the protocol used is AODV. This protocol is used to establish the path between source and destination. The trust value algorithm includes three phases namely Initialization, Updating of trust values, Isolating the packet drop from the network. Initially the trust values of all the participating nodes are kept zero and the threshold value is kept 100 and assumption is made 1 trust value = 10 packets dropped. If the packets are correctly transmitted from one node to another then respective nodes trust value is incremented by 1, if the packets are dropped or delayed then the trust value is decremented by 1, if the trusted value of a particular node is less than the threshold trust value then the particular node is treated as malicious node. If the trusted value of a particular node is greater than the threshold value then the node is treated as legitimate node. This reduces the packet drop ratio which results in low false positive rates which leads to the improved security of wireless adhoc network.

K.Urmila Vidhya and Mohan Priya [13] proposed a paper titled "A Novel technique for defending routing attacks in OLSR MANET". They have used the method which uses the hop-information table, 2-hop request and 2-hop reply. The hop information table consists of hello message, sender and its 2-hop neighbors, if a malicious node sends the false hello message to its neighbor node the neighbor node checks their hop information table and verifies whether that node belongs to its table. if not, the node adds it in backlist and discards its hello message.

Bobby Sharma Kakoty, S.M.Hazarika and N.Sarma [14] proposed a paper titled "NAODV – Distributed packet dropping attack detection in MANETs". In this paper, detection and isolation of malicious node is based on Trust level of the nodes. Trust levels of the nodes are dynamically updated based on their qualitative participation in detection of malicious nodes. Upon detection, message will be distributed amongst the nodes in terms of alarm to avoid the malicious nodes for packet forwarding, in this paper the local agent runs on each node to detect packet drop attacks locally, then these agents will collaborate with other agent to confirm packet drop attack in the network. In this the detection of malicious packet dropping is done in distributed co-operative way and after confirmation only it will generate an alarm to avoid malicious node for further packet forwarding. Hence false positive rate will be less. The advantage is that it does not consumes much time for route discovery and there is not so much complex security measures during route discovery, so it delivers more packets in specified time, this implies more throughputs.

Ms Deepa Athawale and Dr Lata Ragha [15] proposed a paper titled "Secure AODV against control packet dropping attack". In this paper they have proposed a solution to monitor, detect and isolate control packet droppers. This solution deals with both the directed and broadcast control packets. For monitoring directed control packets they have used time based solution, redemption strategy for judgment, reputation based approach for isolation applicable to both directed and broadcast control packets. SAODV takes extra time for computation and verification of security fields during route discovery process. Moreover it always prefers the safest path instead of shortest path. This consumes some extra time since throughput depends on the total number of packets delivered in specified time hence it will come down. SAODV is not designed to resist the packet dropping attacks. It provides cryptographic support to secure routing protocols and it shows vulnerabilities to packet drop attacks.

C.Senthil Kumar, N. Kamaraj and S.Rakesh Kumar [16] demonstrated a paper titled "Mitigating of Black hole attack using Trusted AODV". They have proposed a an algorithm called trusted value algorithm. When node sends the data packet to its neighbor node first it will store the source Id, destination ID, sequence number and the data, if the next node is a malicious node then it will alter the contents and forwards it to the neighbor node or dump

the packets. The proposed algorithm will verify whether the sequence number of rebroadcasted route request is equal to the sequence number of same route request that is stored in the routing table of current node. If the sequence number is different then it analyses the nature of identified suspicious node by calculating their trust values and packet drop ratio. If results are not satisfactory then that node is considered as the malicious node. TAODV increases the reliability of packet delivery because this protocol computes the trust values of each node and allows only the trusted nodes to get involved in the routing process.

6. COMPARISON OF VARIOUS SOLUTIONS TO PACKET DROP ATTACKS

The various solutions to the packet drop attacks proposed by several authors are analyzed and a comparison is made based on some parameters as depicted in table 1.

7. CONCLUSION

In this paper, the various methods to detect and isolate packet drops have been proposed using the various protocols such as dynamic source routing (DSR), Adhoc on-demand distance vector(AODV), optimized link state routing(OLSR). These methods are advantageous but still not reliable. Some of the disadvantages are unable to detect the attacks in collusions, reduced throughput and excessive burden on sender. In future effective methods can be designed to overcome the above mentioned disadvantages.

Table 1: Comparision of various solutions to packet drop attacks

AUTHOR	TITLE	METHODOLOGY	PROTOCOL	ADVANTAGE	DISADVANTAGE
L.Buttyan and J.-Y Hubux	Stimulating Cooperation in Self-Organizing Mobile Adhoc Networks	Credit Based System	DSR	Security Module prevents counter from being negative or being modified	Security module is too expensive to integrate
S.Marti, T.Giuli, K.Lai and M.Baker	Mitigating Routing Misbehavior in Mobile Adhoc Network	Reputation Based System	DSR	It provides the information to check whether a node is trustworthy or not	It might not detect the misbehaving node in ambiguous collision
K.Liu,J.Deng P. Varshney and K. Balakrishnan	TWO ACK: preventing selfishness in mobile ad hoc networks	Acknowledgement Based System	DSR	Reliable, Improves Performance	If ack_time >wait_time then Link is misbehaving
S.Zhong, J.Chen, and Y.R. Yang	Sprite: A Simple,Cheat-proof,Credit Based System for Mobile Adhoc Networks	Credit Based System	DSR	Removes Security Module Uses CCS	Excessive Burden on sender
Rekha Kaushik and Jyoti Singhai	MODSPIRITE:A Credit Based Solution to Enforce Node Cooperation in Adhoc Network	Credit Based System	DSR	Usage of cluster head reduces the burden	It is for limited number of intermediate nodes in the network
Bounpadidth, Hidehisa Nakayama, Nei Kato, Yoshiaki Nemoto and Abbas Jamalipour	Analysis of Node Isolation Attack against OLSR based mobile adhoc networks	Node isolation attack model	OLSR	High Throughput	Not detects the attacks in collusions
Rajendra Aaseri, Pankaj Choudhary and Nirmal	Trust Value Algorithm: A Secure Approach against Packet Drop Attack	Trust value algorithm	AODV	Reduces the packet drop ratio	

Roberts	in Wireless Adhoc Network				
K.Urmila Vidhya and Mohana Priya	A Novel technique for defending routing attacks in OLSR MANET		OLSR	High Throughput	Not detects the attacks in collusions
Bobby Sharma Kakoty, S.M.Hazarika and N.Sarma	NAODV – Distributed packet dropping attack detection in MANETs		AODV	High Throughput	
Ms Deepa Athawale and Dr Lata Ragha	Secure AODV against control packet dropping attack	Cryptographic approach	AODV	Provides integrity and authentication	Reduces Throughput
C.Senthil Kumar,N. Kamaraj and S.Rakesh Kumar	Mitigating of Black hole attack using Trusted AODV	Trusted value algorithm	AODV	Increases the reliability and QOS of the network	

References

[1] https://en.m.wikipedia.org/wiki/wirelessadhoc_network.

[2] H. Deng, W Li, DP Agrawal, “Routing Security in Wireless Adhoc Networks” in Communications Magazine,IEEE Volume:40,Issue:10), 2002.

[3] D.B.Johnson, D.A.Maltz, and J.Broch,”DSR: the dynamic source routing protocol for multi-hop wireless adhoc networks”, Chapter 5, Ad hoc Networkig, Addison –Wesley, Pages 139-172, 2001.

[4] Dr. Baruch Awerbuch & Dr. Amitabh Mishra, “Ad hoc On Demand Distance Vector (AODV) Routing Protocol” in Chapter 6, Sections 6.1-6.3, 6.5 – Ad Hoc Networking, Perkins, Addison Wesley, 2001.

[5] P.Jacquet , P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, “Optimized Link State Routing Protocol for Adhoc Networks”, in Multi Topic Conference,2001. IEEE INMIC 2001, Pages: 62-68, ISBN: 0-7803-7406-1.

[6] L.Buttyan and J.-P Hubaux,”Stimulating Cooperation in Self-Organizing Mobile Adhoc Networks”, ACM/Kluwer Mobile Networks and Applications, 8(5),October 2003”.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks” Proceedings of Mobicom 2000, Boston, MA, USA, Aug. 2000.

[8] K.Liu, J.Deng P. Varshney and K. Balakrishnan, “TWO ACK: preventing selfishness in mobile ad hoc networks”, in Proc.of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, March 2005, IEEE.

[9] S. Zhong, J. Chen, and Y. Yang, “Sprite: a simple, cheat-proof, credit based system for mobile ad-hoc networks”, IEEE INFOCOM 2003, San Francisco, CA, USA, April 2003.

[10] Rekha Kaushik and Jyoti Singhai, “MODSPIRITE: A Credit Based Solution to Enforce Node Cooperation in an Ad-hoc Network”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[11] Bounpadith Kannhavong, Hidehisa Nakayama,Nei Kato,Yoshiaki Nemoto and Abbas Jamalipour, “Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks” in computer Networks,2006 International Symposium, pages:30-35, ISBN: 1-4244-0491-6.

[12] Rajendra Aaseri, Pankaj Choudhary, Nirmal Roberts, “Trust value algorithm: A Secure Approach against packet drop attack in Wireless ad-hoc networks” in International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013.

[13] K.Urmila Vidhya, M. Mohana Priya, “A Novel technique for defending routing attacks in OLSR MANET” in 2010 IEEE International Conference on Computational Intelligence and Computing Research.

[14] Bobby Sharma Kakoty, S. M. Hazarika, N. Sarma, “NAODV-Distributed Packet Dropping Attack Detection in MANETs” , in International Journal of Computer Applications (0975 – 8887) Volume 83 – No 11, December 2013.