ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Mitigating Routing Misbehaviour of Packets using Cryptographic Approach in Wireless Adhoc Network

Shridevi K, Naziya Parveen

Assistant Professor, Dept of Computer Science, Secab Institute of Engineering and Technology, Vijayapura, India

M.Tech Student, Dept of Computer Science, Secab Institute of Engineering and Technology, Vijayapura, India

ABSTRACT: A wireless network is susceptible to many security attacks due to open nature of wireless medium. The reason for packet loss in wireless adhoc network is due to link error and vicious node. This work demonstrates identifying whether the packet losses are due to the link error or the combined effect of both link error and vicious node .To detect these kinds of packet drops, correlation between lost packets is calculated. The conventional methods are restricted to static wireless network and single vicious node identification. In this work frequent change on topology and identification of number of vicious nodes as well as the performance parameters such as throughput, packet delivery ratio and packet loss is considered.

KEYWORDS: Wireless Network, Adhoc Network, link error, vicious nodes.

I. INTRODUCTION

A wireless adhoc network 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.
The Dynamic Source Routing protocol (DSR) 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.

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 identifying the packet dropping attacks using dynamic source routing protocol. In this paper more than one malicious node is identified.
The rest of the paper is organized as follows. Section 2 describes the related work; Section 3 provides an overview of proposed work, Section 4 deals with simulation results Section 5 presents the conclusion and future work, finally the references.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

II. RELATED WORK

L.Buttyan and J.-Y Hubux [1] 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. 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 [2] 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 [3] 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 [4] 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 [5] 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.

Rajendra Aaseri, Pankaj Choudhary and Nirmal Roberts [6] 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

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 [7] 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 [8] 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 [9] 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 [10] demonstrated a paper titled "Mitigating of Black hole attack using Trusted AODV". They have proposed 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.

III. PROPOSED WORK

The DSR protocol is utilised to set up the route by sending the request for the path. Once the route is established the sender forwards the encrypted packets to the destination through intermediate nodes and maintains the copy in its cache. After sending the packet the sender monitors the neighbour node, once the neighbour node forwards the packet the sender cancels the packets from its cache and the previous process is repeated for every node within the network. If neighbour node does not forwards the packet the node waits for some time say T_{th} and sends the message to the auditor

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

to check the misbehaviour, after receiving the message the auditor launches the investigation on the misbehaving nodes and informs the sender about the misbehaviour node and tells to establish a new route, path is established from sender to receiver and the packets are transmitted.
Advantages of Proposed System are multiple vicious nodes are identified, auditor detects the routing misbehaviour of the packets, link error is identified and the network proves to be efficient.

IV. SIMULATION RESULTS

This section deals with the results and analysis on the simulation work carried out using ns2 along with the graphical representations.

Throughput without attack

The figure 1 displays the throughput of the network in absence of vicious node. For the given time span all the packets are delivered form source to the destination. The throughput achieved in absence of attack is about 100%.

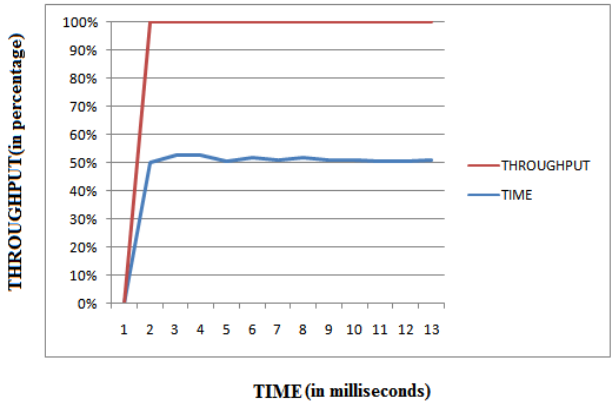

Figure 1: Throughput without attack

Throughput with attack
The throughput is the ratio of packet received to the packet sent at the given time interval. The figure 2 displays the loss of packets during transmission under attack.

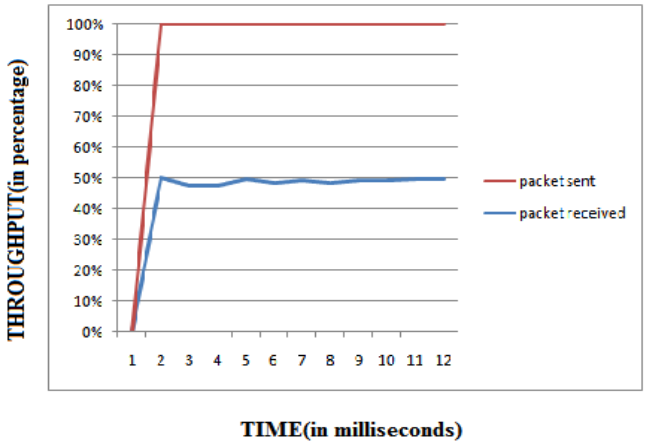

Figure 2: Throughput with attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Packet delivery ratio

It is the proportion of various number of packets delivered to the total number of packets forwarded to the destination. The higher value of PDR means the good performance of the protocol used.

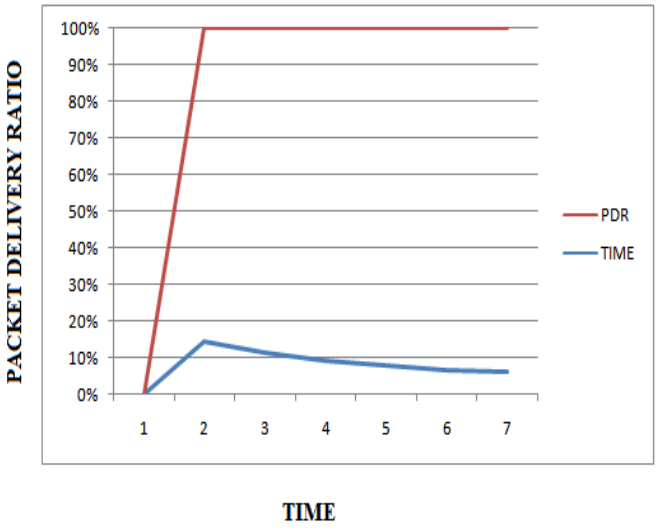

Figure 3: Packet Delivery Ratio

Packet Loss during Transmission

Packet loss is nothing but the number of packets dropped either due to link error or due to the presence of vicious node while carrying out the simulation. The lesser value of the packet loss indicates the better performance of the protocol used.

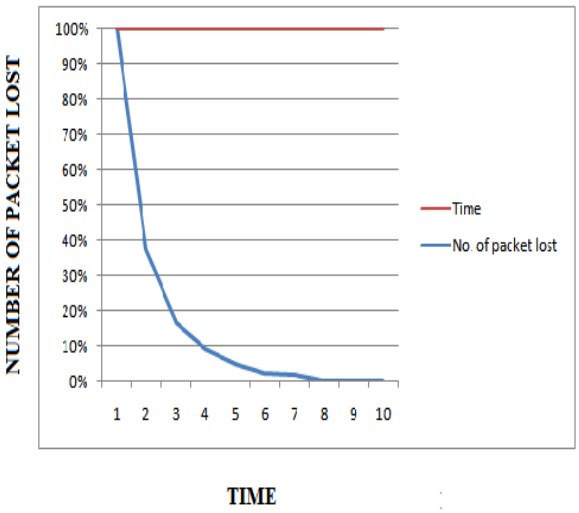

Figure 4: Packet Loss during Transmission

V. CONCLUSION AND FUTURE WORK

In this work mitigating routing misbehaviour of packets using cryptographic approach in wireless adhoc network is proposed. In this work the packet dropping due to link failure and presence of number of vicious node is identified.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Proposed method works on dynamic source routing protocol. Network performance is measured using parameters such as throughput, PDR and packet loss. Results obtained using the proposed approach proves to be efficient. In the future work the other parameters can be considered and can be proved to be efficient.

REFERENCES

[1] L.Buttyan and J.-P Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Adhoc Networks", ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.
[2] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks" Proceedings of Mobicom , Boston, MA, USA, Aug. 2000.
[3] 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.
[4] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit based system for mobile ad-hoc networks", IEEE INFOCOM, San Francisco, CA, USA, April 2003.
[5] 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.
[6] 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.
[7] K.Urmila Vidhya, M. Mohana Priya, "A Novel technique for defending routing attacks in OLSR MANET" , IEEE International Conference on Computational Intelligence and Computing Research 2010.
[8] 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.
[9] Ms. Deepa Athawale and Dr. Lata Ragha, "Secure aodv against control packet dropping attack" in International Journal of Technical Research and Applications e-ISSN: 2320-8163, Special Issue 31, PP. 296-300, September, 2015.
[10] *C.* Senthilkumar, N. Kamaraj and S. Rakesh Kumar, "Mitigation of Black hole Attack Using Trusted AODV", Australian Journal of Basic and Applied Sciences, 9(23), ISSN:1991-8178, Pages: 596-603, July 2015.