IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-12 E-ISSN: 2347-2693

A Trust Proxy Node (TPN) Based Black hole Attack Detection Mechanism in MANET Using AODV

Amit Saraf[1*] and Megha Singh[2]

[1]M Tech, Scholar CIIT Indore, India
[2]Asst. Professor, CIIT Indore, India
www.ijcseonline.org

Received: 27/Nov/2015 Revised:09/Dec/2015 Accepted:21/Dec/2015 Published: 31/Dec/21015

Abstract—A mobile ad hoc network (MANET) is auto-configuring network without any infrastructure. It is temporary network created by, mobile nodes which are capable to communicating with each other without the use of network infrastructure. Ad hoc networks are vulnerable to many type of security attacks due to their open medium, dynamic topology, distributed co-operation. For successful data transfer nodes are depend on each other. To believe on the other node for wireless data transmission, consider as trust problem. Our aim in this review is to present schemes which are mainly focused on security based on trust value of node in MANET. This work proposes a approach for trust calculation based on Trust proxy node (TPN). The route discovery is achieved through a routing decision based on trust sequence certificate exchange by Trust proxy node (TPN). Trust proxy node (TPN) is an additional node having extra responsibility for trust calculation of Black hole node. Trust proxy node (TPN) will act as monitoring node for routing decision. After the trust value index is calculated the TPN node issues a certificate to every node in its network. To participate in routing the nodes must have two trust index (TI) certificates & can be consider as a reliable node by TPN. The directory of this certificate is maintained in a Trust Index (TI) Table. This TI table is shared with the server by this centralized TPN. This TPN will also monitors the behavior of nodes in a specific range continuously to avoid unwanted action

Keywords—MANET, AODV, TPN(Trust proxy node), Milisious Node, Black Hole

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of devices that transmit across a wireless communication medium based on radio frequency without any fixed infrastructure and centralized control. Intermediate nodes is important to forward packets on behalf of each other when destinations are out of their wireless transmission range. There will be no centralized control for a MANET to be set up, thus making its deployment fast and inexpensive. The ability to move freely node ensures a flexible and versatile dynamic network topology which is another important feature of a MANET. Some of the MANET applications includes emergency disaster relief, military operations over a vulnerable infrastructure and community networking through health monitoring using medical sensor network (MSN) [1]. There are many issues in MANETS such as IP addressing, radio interference, routing protocols, power Constraints, security, mobility management, bandwidth constraints, QOS, etc;. As of now some hot issues in MANETS can be related to the routing protocols, routing attacks, power and bandwidth constraints, and security, which have raised lot of interest in researchers. Even though in this paper we only focus on the routing attacks and security issue in MANETS. The inherent features of mobile ad hoc networks make them more vulnerable to a wide variety of attacks by misbehaving nodes. Such attacks can be listed as passive and active attacks. In active attacks, we mainly consider the internal attacks for network layer such as black hole attack, gray hole attack, worm hole attack, message tampering, routing attacks. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services [2]. Misbehavior can be divided into two categories [3]: routing misbehavior (failure to behave in accordance with a routing protocol) and packet forwarding misbehavior (failure to correctly forward data packets in accordance with a data transfer protocol). These two are employed using AODV (Ad hoc on demand distance vector protocol) routing strategy. This approach detects and prevents misbehaving nodes (malicious) capable of launching any of the network layer attacks. This work focus on improving the more secure mechanism to this forged message detection & valid packet dropping by malicious node identification. Better the timing of identification of these misbehaving nodes, it's easy to identify them but requires some standard protocol parameters [4]. Trust can be consider a well known parameter for node behavior whose value is continuously exchanged between all the adjacent neighbor nodes. The proposed work of TPN & TI will also categorize the parameters to define unwanted behavior of the node. These unwanted behavior of node can be find out by the trust value of that node. Which is calculated on basis of previous participation in data transfer. Thus this trust value calculation & the exchange of this trust table needs to be

secure. The work categorizes in to two related domain areas first is invalid trust value due to malicious node behavior is legitimate at certain condition. & second is trust packet modification by fabrication (Masquerade) type of attack. The paper will also discuss the framework and a relevant algorithm with AODV protocol implementation that deal with these attacks.

II. BACKGROUND

There are many attack in MANET; one of them is Black hole attack. Black hole attack is a type of active attack. In a black hole attack [5], malicious node waits for neighboring nodes to send route request messages (RREQ). When the malicious node receives route request message it sends a false route replay message (RREP) without checking its routing table. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages send by legitimated node and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes access to all routes. All packets are sent to malicious node it notforwarding packets anywhere means it drop all data. This is called a black hole attack. The Black hole node possesses two type of the behavior. They are as follows:-

a) Black hole node showing highest possible destination sequence no. as we know larger the sequence [6] no. means the route is fresh and latest for a particular destination. By this way malicious node divert the source node, who wants to initiate communication.

b) Black hole is an active attack in MANET [6], which except all incoming packets from an intended source. It absorbs the network traffic and drops all packets.

Supposed that the malicious node is positioned in center of the wireless network. To consider the problem of black-hole node identification we show Network Illustration Model in figure1.

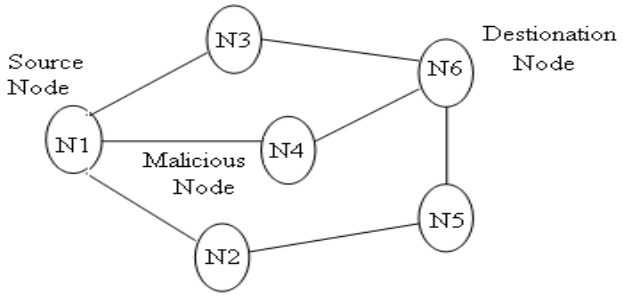

Figure 1: Network Model for Black Hole Detection through ADOV protocol

In Figure.1, we assume that N4 is the malicious node [6]. Suppose source node N1 want to send data destination node N6, and initiates the route discovery process. As we know malicious node N4 does not have any route to destination node N6.When node N4 receives RREQ packet , its immediately response to source node N1.Any other intermediate node that have the route to destination node also give reply. If reply from any legitimated node reaches the source node N1 first then overall work perform properly. The false reply RREP from malicious node is probable reach the source node N1 first. A malicious node N4 does not need to check its routing table because its know that it send false route replay message so that its reply reach the source node N1 first. Basically malicious node send shortest route reply message so the source node select the route by malicious node. Ones the source node route discovery process completed it discard all other route replay message send by other legitimated node. As a result all data packets through malicious node are dropped and effect the network traffic. This malicious node could be said black hole node in network. By this process malicious node access hug amount of network traffic to itself that cause a big loss of data in network. To solve the above discussed problem we proposed a trust proxy protocol trust proxy node(TPN). The Trust proxy node (TPN) will check and provide the trust value to each node at regular intervals. This solution will also assume that any malicious node will unable to participate in data transmission in network.

III. RELATED STUDY

To improve the routing security and avoid the black hole attack there are many approaches in MANET .Some approaches includes authentication mechanisms for detecting multiple black hole nodes working as a group, which could be potentially exploited by malicious nodes [1]. To catch the problems like cooperative black & gray holedetection without any authentication infrastructure, such as a Public Key Infrastructure, which is usually not practical in MANET, authentication mechanisms are based on the concept of the hash function, the PRF and the MAC. The paper [3] propose a methodology to identifying multiple black hole nodes cooperating as a group with modified AODV protocol by introducing data routing information (DRI) table and cross checking. The solution for identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node . Each node manages an additional Data Routing Information table. Many approaches are further proposed to determine the privacy conserving & side channel monitoring by which we can be analyzed the malicious behaviors [4,5].Given solution can be applied to 1.) Detect multiple black hole nodes working with each other in a MANET; and 2.)To avoiding multiple black hole node we discover safe paths from source to destination . Certificate chaining is a malicious node identification mechanism having self organized PKI authentication by a chain of nodes without

the use of a trusted third party [6]. Authentication is represented as a set of digital certificates that form a chain. In the network each node has play identical roles and responsibilities for achieving higher level of node participation. Every node in the network providing certificates to every other node within the wireless communication range of each other. A lot of other encryption based [7] & robust identification based [8] are given by different authors. Cross layer design for detecting black and gray hole attacks in MANET is an adaptive approach . In network layer, the paper [9] proposed a path-based method to overhear the next hop's action. This scheme does not send out extra control packets and saves the system resources of the detecting node. TO estimate dynamic detecting threshold In MAC layer, a collision rate reporting system is established to lower the false positive rate under high network overload. Some approaches trust based calculation for malicious node detection is also proposed which is capable of detecting the trust value of nodes on the basis of their previous behavior [10]. In [11], we proposed a solution to identifying and preventing the black hole attack. Our solution discovers the safe route between source and destination by identifying black hole nodes.

we compare proposed solution existing solutions in terms of average end to end delay, packet loss percentage, throughput and route request overhead. Request routing table is an another good option for black hole detection in which the nodes shares their routing table on regular basis network form further malicious behavior. Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by identifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? The solution presents good performance in terms of packet ratio and minimum packet end-to-end delay and throughput [12] Another detection technique is acknowledgment [13]. To prove that a node has actually forwarded packets to the next hop, the receiver can send acknowledgment in the reverse direction for multiple hops. Two-hop acknowledgment is suggested. However, it fails when more than two malicious nodes are colluding in a row. For example, three malicious nodes one next to another act as a team to drop packets along a data communication path: the one in the middle actually drops packets, while its prior hop simply does not do the watchdog job and its next hop falsely sends acknowledgment. There are many other detection techniques in literature [14, 15, 16]. The main aim at early detection of packet drop attackers during routing process. The general idea is to identify forged routing information by double checking, for example, neighbor information, destination sequence number, or network state, with the nodes after the malicious node or directly with the destination [17]. Due to space limit, we introduce only a few recent proposals.

IV. PROBLEM STATEMENT

After analysis of many paper and their methods we found that the current methods focus on providing security to fake message detection and packets dropping by malicious node. Some process is given which identify malicious node as quick as possible. Behavior of node considers as well known parameter called trust. The trust value continuously exchange with all neighbor node. The problem related to malicious node is categorized in three major security areas. These are –

1. Security – Gives protection against active and passive insider and outsider attack.
2. Privacy – Taking resistance maximization of individual node insider and outsider adversaries.
3. Efficiency – Achieve the above goals with reasonable efficient solution.

While studying the literature ,this work detect that false overhead ,packets drops and false routing will be consider as broad issue in case of malicious node in MANET.
All the method will only focus on single malicious node detection. If this problem is resolved then prevention and detection is possible before the expected loss. Unwanted behavior of the node is also identifying by this work. Trust value is used to find out the unwanted behavior of the node that is calculated on the basis of the previous data transmission by that node.
The trust calculation and trust table exchange is need to be perfume in more secure manner. This work is divided in two related area:

1) False trust value calculation due to behavior of malicious node is legitimated at certain condition.
2) Modification of trust packets by malicious node (Fabrication type of attack).

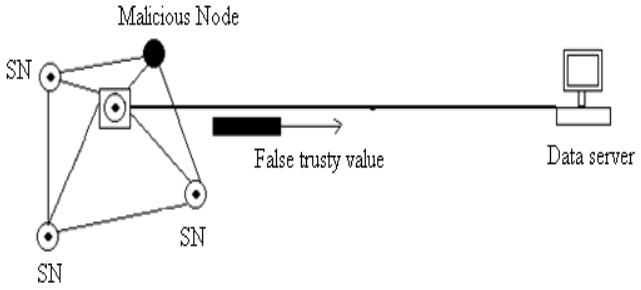

Figure 3: False Trust Value Due to Malicious Node

Proxy node calculates trust value of each node in a network which is further exchange with server for aggregation.

When malicious node in the network act as an actual node (for some time) , the calculation of trust value is incorrect. This may cause access gain by malicious node in network and after some time will drop the packets. So it is necessary to find out malicious node in network as quick as possible.

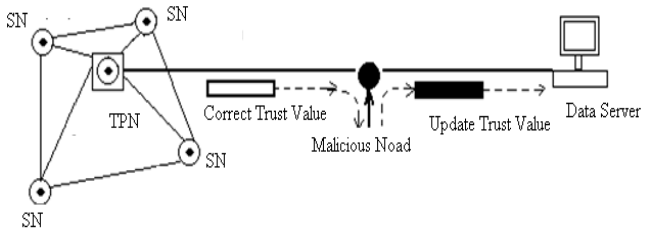

Figure2: Modification of Trust Table by Malicious node.

In Scenario (ii) the trust value calculation is correct but this will need to exchange between node and server. When we trying to exchange trust value table between nodes and local server , it will modified by the malicious node in the route. To stop this modification needs that the packets relay from a particular node. Previous information about the node direct us to find out the malicious node as quick as possible so that the trust table exchange by which is easily avoided.

V. PROPOSED MECHANISM

Trust proxy node (TPN) based malicious node trust calculation is critical issue in MANET .This work propose a novel approach for trust calculation based on Trust proxy node (TPN). The route discovery is achieved through a routing decision based on trust sequence certificate exchange By Trust proxy node (TPN). Trust proxy node (TPN) is an additional node having extra responsibility for trust calculation of malicious node detection. Trust proxy node (TPN) will act as monitoring node for routing decision . We use AODV protocol to analyze the result of proposed mechanism. In AODV , for Discovering route the sender node send Route request(RREQ) Packet to each node in network and will expect Route reply(RREP) for existence of route. The malicious node will reply fast as compared to legitimated node . Due to this , malicious node look like active shorter link . So this in malicious node will add into the source node routing table which will cause the packets drop or denial of service(DOS) attack. To solve the above problem current work also add an additional wait for 20 seconds for reply to other node. During this time period Trust Proxy Node(TPN) come into act for authentication of each neighbor node through trust certificate exchange mechanism proper sequence. Firstly on the basis of precious participation of node in data transmission , trust value of the node is calculated. If trust value is more than threshold value which decided on basis of node behavior and issue trust certificate to that node . This trust certificate is exchange between all neighbor node and update the routing table of each node with latest information. The node have at least two trust certificate in sequence can participate in data transfer. The node have less than two trust certificate is indentify as malicious node. After this Trust Proxy Node(TPN) will transmit a malicious alert message to all node in the network. Each node receive this alert message and update our routing table and delete information about the malicious node. Trust Proxy Node(TPN) protocol used to find out malicious node on basis of trust table which is continuously update and analyze the behavior of node. Each and every node in network must acquire two trust certificate are capable to participate in data transfer. The node parameter and trust certificate store in trust value table. The Trust Proxy Node(TPN) prepared the trust value table and exchange by data server(local server). The benefits to applying the proposed Trust Proxy Node(TPN) methods are-

a) The malicious node find out in early stage and remove immediately.

b) Malicious node are easily identify Trust Proxy Node(TPN).

c) Not make any modification in operation of AODV protocol.

d) Small modification provide better performance.

e) Only few things are added so less memory overhead occurs.

The detection of black hole node through their behavior will create complex routing decision , Trust Proxy protocol also kept solution of routing overhead. The Trust Proxy Protocol will more efficiently work to detect the unwanted behavior from its previous existing old data about the node.

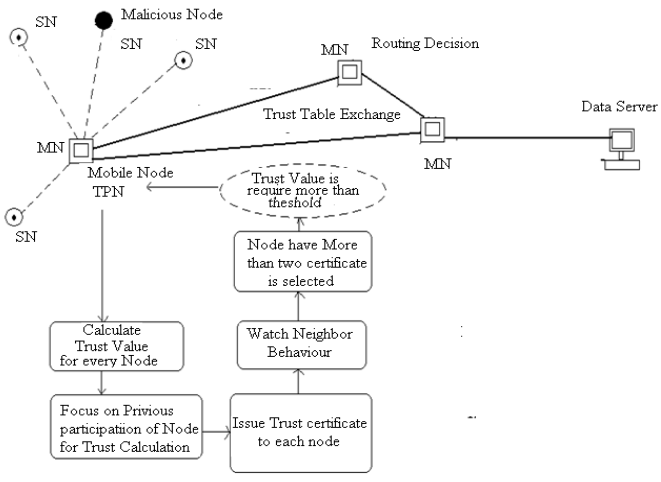

Figure 4: Trust Proxy Node (TPN) Protocol Working

Trust Proxy NODE (TPN) Algorithm

S1: Source, D1: Destination, WN: Watcher Node, MN: Mobile Node, RT: Record Table, TC: Trust Certificate;

Initiate AODV Transmission ()

S1 wants to communicate with D1.

// TPN Starts new process for data transmission. For directional routing the node must transmit the packet in specific range

S1 broadcast the RREQ.

//after every 3 sec for latest updates //During this period TPN Start sensing the network.

D1 replies with RREP.

//Malicious node Reply very fast without checking its TP Index.

If (Reply< Set Timestamp)

MN uses TPN to contain Trust

//Stores trust value of its all preceding and successor nodes //Condition Check

If (Node=New node)

Assign initial Trust Value=0;

Else If (Trust value>= Threshold)

Behavior Ok;
Else

Verify malicious behavior;

TPN Issues Trust certificate

//To every successor node

If (TC>=2)

Not malicious node;

End if (TC<2)

Black hole node;

//Remove Entry from Trust Value Table between other nodes. Send Message to delete entries from other nodes TP table

Exit TPN;

VI. PERFORMANCE EVALUATION

In this proposed approach, we have considered four network parameters to evaluate the performance of network. We can extend it to a few more parameters based on density of network. For identification and prevention of network layer attacks, we can extend the algorithm.

Routing overhead – Routing overhead is the number of routing packets transmitted per data packet delivered at the destination.

Packet delivery ratio (PDR) – PDR is the ratio of the number of packets which received at the destination node and the number of packets sent by the source node. The method of calculation of Packet delivery ratio is = (no. of packets received/no. of packets sent).

Throughput- Throughput is sum of bits. It is sum of number packets also. The Packets included generated/sent/forwarded/received packets which are calculated at every time slice. It is shown in bits. Time slice length is equal to one second by default.

Power consumption- Time taken to transmit a message from sender to receiver is called the power consumption.

We can consider various approaches with respect to the power consumption of node. When we compare power com to the other approaches ,this proposed work show a simple one hope acknowledgement and trust certificate named semantic security mechanism .It reduce transmission time and traffic overhead in network. The transmission of sending and receiving the data takes only few milliseconds.

VII. CONCLUSION

In mobile ad hoc networks, protecting the network layer from attacks is an important research topic in wireless security. This work describes a robust trust based security service scheme for network-layer security solution in ad hoc networks, which protects both, routing and packet forwarding functionalities without the context of any data forwarding protocol. This approach tackles the issue in an efficient manner since four attacks have been identified commonly. The overall idea of this algorithm is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. This work explores a novel Trust proxy NODE(TPN) based authenticity mechanism which is continuously exchanging

with its neighbor. It is a robust and a very simple idea, which can be implemented and tested in future for more number of attacks, by increasing the number of nodes in the network. To this end, we have presented an approach, a network-layer security solution of Trust proxy Node (TPN) approach which will work on a specific node named as TPN node. This node will work as monitoring node & checks the behavior of nodes against attacks that protects routing and forwarding operations in the network. As a potential direction for future work, we are considering measurement of more number of network parameters, to analyze the performance of such a network using the proposed approach. In future the results will show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

VIII. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in future. Such as with the help of pre-emptive approach more information can be added for exact timely analysis of malicious node. It can also be used for quantitative & qualitative analysis, rank ordering to each nodes etc. We also embed source code of our proposed scheme in NS2. In our proposed scheme so as to use the benefits of approach like open source.

IX. REFERENCE

[1] D He, C Chen, S Chen, J Bu & A B. Vasilakos, "ReTrust:Attack Resistant & Lightweight Trust for Sensor Network" in IEEE Transaction on IT in volume-16/ No 4 Page No (623-632), July 2012.

[2] Z Min & Z Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks" in IEEE Transaction ISBN 978-0-7695- 3686 Page No(26-30),16-17 May 2009.

[3] S Ramaswamy, H Fu, M Sreekantaradhya, J Dixon & K Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" in Department of Computer Science, IACC 258, Page No(1-7) March, 2008.

[4] K E Defrawy& G Tsudik, "Privacy-Preserving Location-Based OnDemand Routing in MANETs" in IEEE Transaction of selected Journal in communication, Volume 29 Issue 10, Page No(1926-1934), Dec. 2011.

[5] Xu Li, R Lu, X Liang, & X Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks" in IEEE ICC, Nov.2011.

[6] E. A .Mary Anita & V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining" in IJCA (0975 – 8887) Volume 1 – No. 12, Page No (1-8), Jan 2010.

[7] P H. Yu and U W. Pooch, "Chapter on Security and Dynamic Encryption System in Mobile Ad-Hoc Network" in A&M University, Dept of CSE Texas, USA, ISBN 978-953-307-402-3 Page No(469-490), Jan 2011

[8] G. S. Mamatha& Dr. S. C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS" in IJCSS Volume 4, Issue 3, page No(275-284), July 2010.

[9] J Cal, P Yi, J Chen, Z Wang & N Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" in IEEE Proceedings, 1550-445X/10, 2010.

[10] R Karandikar, R K Khanuja, S Shukla, "Proposed solution to prevent Black Hole Attack in MANET" in IJRIM ,Vol 2, Issue 2, ISSN 2231- 4334, Page No(1-5), Feb 2012.

[11] H Weerasinghe and H Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" in IJCA, Volume 2 ,No 3 July, 2008.

[12] PoojaJaiswal& Dr. Rakesh Kumar "Prevention of Black Hole Attack in MANET" in IRACST, ISSN: 2250-3501 Voume.2, No5,Page No (599-606) October 2012.

[13] Sarita Choudhary & Kriti Sachdeva "Discovering a Secure Path in MANET by Avoiding Black/Gray Holes" in IJRTE ISSN: 2277-3878, Volume-1, Issue-3 Page No(1-6), August 2012.

[14] M S Ashraf & M Raheel, "RGB Technique of Intrusion Detection in IEEE 802.11 Wireless Mesh Networks" in IJCSI, ISSN (Online): 1694-0814 Volume. 9, Issue 2, No 2, Page No (306-313),March 2012.

Author Profiles

Mrs. Megha Singh received his BE and Mtech degree in Computer Science & Engg. from University of RGPV Bhopal. He is currently Asst. Professor & Head of Department of Computer Science & Engineering in CIIT Indore (M.P), India. His research interest in network security and mobile technological.

Mr Amit Saraf pursuing his M-tech in Computer Science & Engg. and received his BE in Computer Science & Engg. from University of RGPV Bhopal. Interested research area is Mobile networking, MANET, network security and mobile technological.