Security In MANET Using Cross Layer Technology

Dr.K.Suresh Babu
Assistant Professor in CSE
School of IT
JNT University Hyderabad, India.
Kare_suresh@yahoo.co.in

S.Saikumar
Masters in Technology
School of IT
JNT University Hyderabad, India.
Saikumar2012@gmail.com

***Abstract*—Security provision is one of the major challenge in Mobile Ad-hoc Networks. In this paper we provide security in MANETs using cross layer technology. In this paper we create a MANET with different nodes having different transmitting and receiving powers (txPower and rxPower). We set threshold values for transmitting and receiving powers. If the transmitting or receiving power of a node doesn't match the threshold value we identify it as malicious node and isolate corresponding nodes from the network. Finally the packets should get forward only through the nodes which are satisfying the threshold limit. The proposed method helps in detection and isolation of malicious node based on transmitting and receiving powers.**

Keywords: MANET,txPower,rxPower,maliciousnode

I.INTRODUCTION

A. Manet:

MANET stands for Mobile Ad-hoc Network. A Mobile ad-hoc network is one which consists of number of mobile nodes which are connected through a wireless channel such as air or freespace. MANETs are temporary and infrastructureless networks. They don't have centralized administration. They are self-organizing and self-reconfiguring wireless networks. They have dynamic topology due to mobility of nodes. Nodes in a MANET utilize the same random access wireless channel, and cooperates among themselves in a friendly manner in forwarding the data packets from source to destination.. The nodes in a MANET not only acts as hosts but also as routers that routes data in forwarding the data.

As MANETS are wireless networks, it is very important to provide security during data transfer between the nodes. Several methods have been proposed in order to provide security in MANETS. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches.

The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks.

B. Cross Layer Technology:

In order to provide security in MANETs several new technologies have been proposed. Among these methods Cross-Layer technology is one of the most efficient method to increase the security and quality of service in MANETs.

Cross-layer design is one which enables different layers of the communication stack to share state information or to coordinate their actions in order to jointly optimize network performance. In order to understand the importance of cross-layer design it must be compared with the traditional layered architecture. In a traditional layered approach the protocols at the different layers are designed independently.

II.LITERATURE REVIEW

Abderrezak Rachedi et al in paper [4] have proposed new cross-layer approach based on physical, MAC, and routing layers for a monitoring mechanism[14]. A new analytical model is proposed to illustrate the parameters' effect on these different layers. The impact of the signal to noise ratio (SNR) and the distance between monitor and monitored nodes are clearly introduced. Arjun P. Athreya et al in paper [8] have proposed the cross-layer strategy to use RSSI measurements in the physical layer to define node neighborhood, ETX measurement from the link layer and node forwarding behavior from network layer to study path reliability via a utility function. Rakesh Shrestha et al in paper [9] have proposed a novel cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. Leovigildo Sánchez-Casado et al in paper [10] have proposed an intrusion detection system for detecting malicious packet dropping in mobile ad hoc networks, by collecting features from the MAC and network layers[15]. The cross-layer approach uses a heuristic to detect packet dropping attacks under several circumstances which are not usually taken into account in previous works and which can cause a high number of false positives in detection.

In these previous works it is learnt that, the techniques have not implemented any features like route changes to the IDS in order to provide accuracy for the detailed information about attack detection. There is no mechanism which has considered the routing attacks like black hole and gray hole. There is no authentication for nodes and packets. They have

used an isolated approach for detection method that is not suitable for the mobile networks.

III. SECURITY IN MANETS USING CROSS-LAYER TECHNOLOGY

A. Proposed Method:

In the proposed technique, we create a wireless adhoc network in ns2 with different nodes having different transmission and receiving powers using tcl script. Here, I have used AODV protocol as routing protocol. The transmission energy of a node is obtained by multiplying transmission power and time required in transmitting the packets similarly the receiving energy is obtained by multiplying receiving power and time required for receiving the packet. Here the time duration is taken as Δt.

Transmission power = txPower.

Receiving power = rxPower.

Transmission energy = Et = txPower*Δt.

Receiving energy = Er = rxPowe*Δt.

We calculate the transmission and receiving energies of all the nodes which are in between sender and receiving nodes dynamically. Now we have to use these transmission and receiving energies for routing in MANETS. The calculated transmission and receiving energies are used for making routing decision in MANET. The transmission and receiving powers are physical layer parameters of a network. In general in AODV protocol routing decisions are taken in network layer. Here we are detecting malicious node by using physical layer parameters in network layer which is satisfying the principle of cross-layer technology. In this project we set some threshold values for transmission and receiving powers of a node, if the transmission or receiving power of a node is not satisfying the threshold value we detect that particular node as a malicious node and identify it by a red mark. Once a malicious node is detected we have to isolate it from the network. In order to isolate it from the network we have to make it to drop Request To Route packets(drop(p, DROP_RTR_NO_ROUTE)).

Once the malicious node is isolated from the network the AODV automatically finds a new route without any malicious nodes.

Tcl script is used for creating the network environment with different nodes. Network animator is used for displaying the nodes, moment of nodes and communication between the nodes. The actual routing of packets between sender and receiver is done by modifying existing AODV protocol. The routing algorithm is implemented using C++.

B. Step By Step Implementation:

In TCL script:

1. Create a mobile adhoc network having n-number of nodes with different transmission and receiving powers (txPower and rxPower).
2. Among these nodes set sender and receiving nodes and provide communication between these nodes.
3. Use AODV as routing protocol.
4. Set TCP communication between sender and receiver.

In C++ code(AODV modification):

1. We use txPower and rxPower values of nodes in backend AODV code and calculate transmission and receiving energies (Et and Er).
2. Et and Er values are obtained by multiplying txPower and rx Power with Δt.
   Et = txPower*Δt.
   Er = rxPower*Δt.
3. The actual routing is done in AODV.CC file so we have to use our parameters(Et and Er) in AODV.CC to detect the malicious node.
4. We have to use these values in forward function of AODV.CC and set some threshold value.
5. If a particular node in the forward path doesn't match the threshold limit we detect such a node as malicious node and identify it by setting a RED circle to that malicious node.
6. Once a node is detected as malicious node we have to isolate it, this can be done by making corresponding node to drop RTR packets.
7. Once the node drops RTR packets corresponding node gets isolated and AODV automatically finds a new route and forwards the packets through the new route.

B. Work flow:

When source S wants to send data to destination D, the data packets are transferred from source to destination with the help of intermediate nodes which forward the packets. In the backend AODV protocol we calculate the transmission and receiving energies of each node in the forward path. We set some threshold values to the transmission and receiving energies. If the calculated values matches with the threshold level there are no malicious nods in the path and S sends data to D successfully. If the calculated values doesn't match with threshold level such a nodes are identified as malicious nodes and corresponding nodes are isolated from the route and AODV chooses an alternative best route.

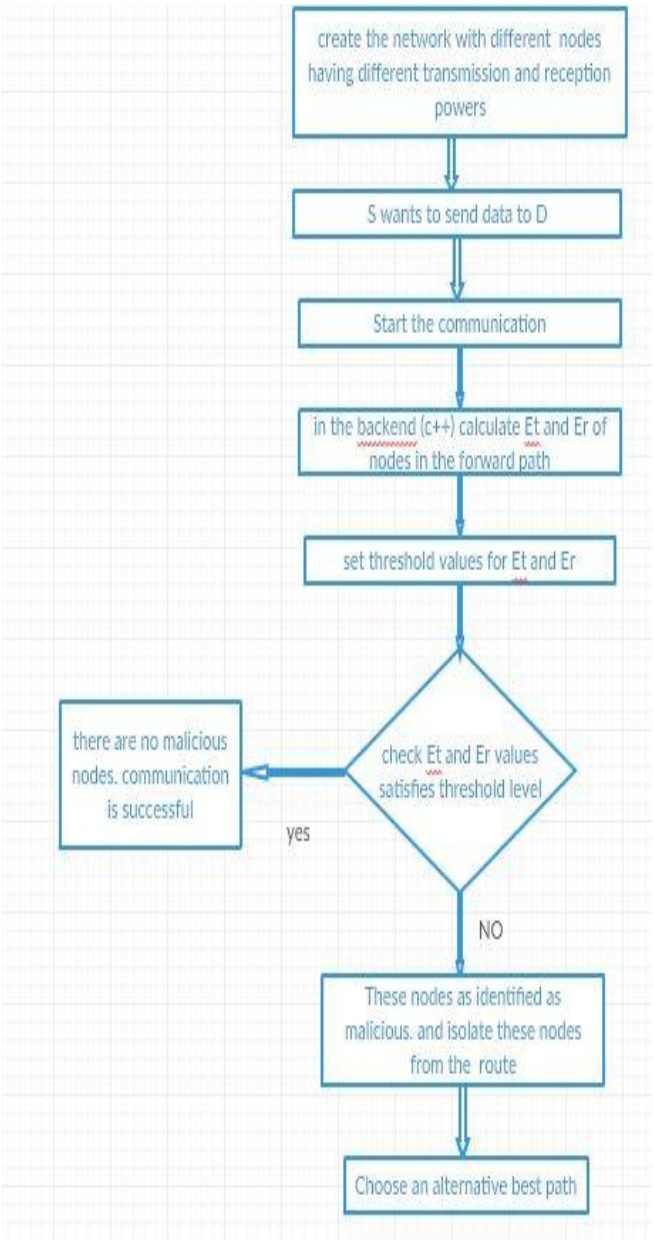

Fig 1. Work Flow

IV.SIMULATION AND RESULTS:

The Network Simulator (NS2), is used for the simulation of proposed architecture. In the simulation, the mobile nodes move in a 700 meter x 510 meter region for 500 seconds of simulation time. The transmitting and receiving powers(rxPower and txPower) of nodes up to index 7(0 to 7) are set to 2 watts. The transmitting and receiving powers(rxPower and txPower) of nodes above index 7 are set to 5 watts. Nodes whose transmitting and receiving powers are equal or grater than 5 are to be identified as malicious.The simulation traffic is CBR and TCP communication is provided between the communicating nodes. and affiliation lines.

Setting node 2 as source and node 12 as destination the simulation results are as follows.

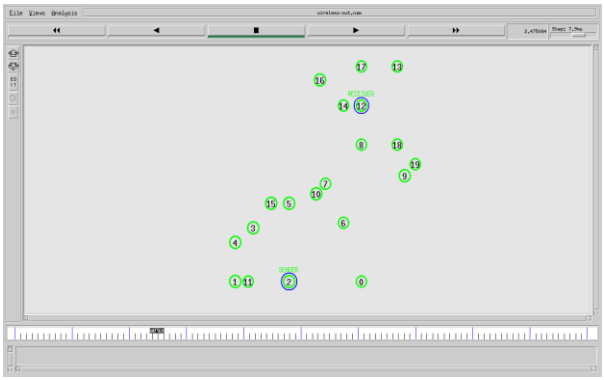

Fig2. Before communication under normal AODV

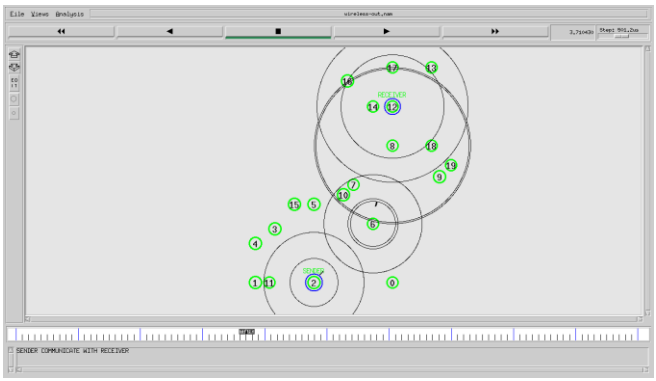

Fig3.communication under normal aodv through nodes 6 and 18.(2→6→18→12)

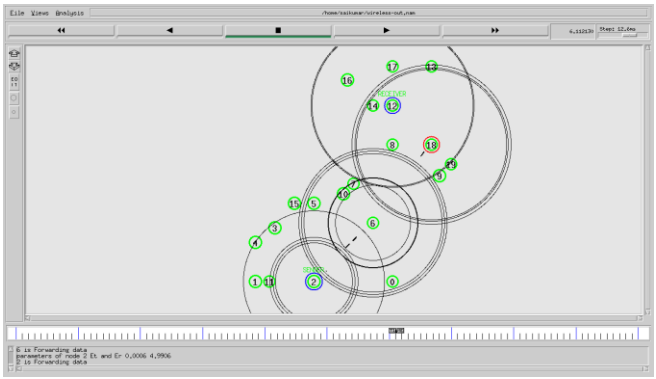

Fig4.communication under modified aodv. Node 18 is identified as malicious by indicating a red colored circle.

Here node 18 doesn't satisfy the threshold(rxPower and txPower are equal to 5), hence it is identified as malicious.

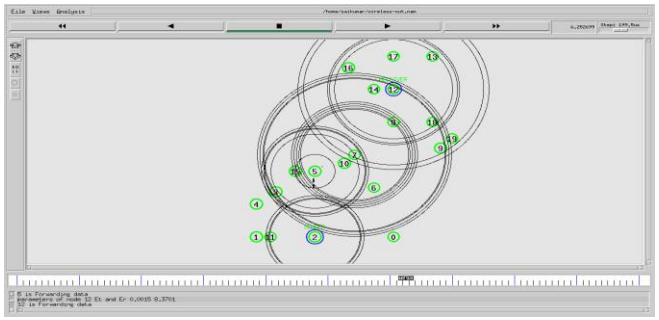

Fig5. communication under modified aodv node 18 is isolated from the network. Packets moving in new route.(2→5→7→12)

Here node 18 doesn't satisfy threshold level hence it is isolated from the old path and a new route is established between nodes 2 and 12. The new route is (2→5→7→12). In the new route all the nodes(5,7) satisfies the threshold level(rxPower and txPower less than 5).

V.CONCLUSION

In this paper, We have proposed a new mechanism for detection and isolation of malicious nodes in MANETs using cross-layer technology. My simulation results revealed that the proposed mechanism worked very well under AODV protocol. I have calculated transmission and receiving energies from transmission and receiving powers of nodes and identified malicious node based on threshold value. Once a node is detected as malicious corresponding node is isolated from the network by dropping RTR packets. Now the AODV protocol automatically selected a new route.

V.REFERENCES

1. Rajaram, A., and Dr S. Palaniswami. "A trust based cross layer security protocol for mobile ad hoc networks." arXiv preprint arXiv:0911.0503 (2009).
2. Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.
3. Gopinath, S., S. Nirmala, and N. Sureshkumar. "Misbehavior Detection: A New Approach for MANET."
4. Rachedi, Abderrezak, and Abderrahim Benslimane. "Toward a cross-layer monitoring process for mobile ad hoc networks." Security and Communication Networks 2.4 (2009): 351-368.
5. Joseph, John Felix Charles, et al. "CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS." Computer Networks 54.7 (2010): 1126-1141.
6. Amardeep Singh, and Gurjeet Singh, "Security in Multi-hop Wireless Networks", IJCST Vol. , Issue 2, June 2011.
7. Manikandan, K. P., and Satyaprasad2 K. Rajasekhararao. "A Cross Layered Architecture and Its Proposed Security Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks."
8. Athreya, Arjun P., and Patrick Tague. "Towards secure multi-path routing for wireless mobile ad-hoc networks: A cross-layer strategy." Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on. IEEE, 2011.
9. Shrestha, Rakesh, et al. "A novel cross layer intrusion detection system in MANET." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.
10 S'nchez-Casado, Leovigildo, Gabriel Maci'-Fern'ndez, and Pedro Garcia-Teodoro. "An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
11. Cai, Jiwen, et al. "An adaptive approach to detecting black and gray hole attacks in ad hoc network." Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010.
12. K. Suresh Babu, K.Chandra Sekhariah. "Security in MANETs Using Cross Layer Design (CLD)", Proc of 2nd International Conference on Advanced Computing Methodologies (ICACM – 2013), ELSEVIER Publications, pp 448 – 452, August 2013.
13. K.Suresh Babu, K.Chandra Sekhariah, "*Securing AODV With Authentication Mechanism Using Cryptographic Pair Of Keys", International Journal of Computer Science and Information Security (IJCSIS)*, USA, Vol 11 No. 2, pp 42-45, February 2013.
14. K.Suresh Babu, K.Chandra Sekhariah, B.Sasidhar, "Issues Related to Routing and Security in Mobile Adhoc Networks", CI-4.7, *International Conference Systemics, Cybernetics and Informatics ICSCI-2009, January 07-10 2009*
15. K.Suresh Babu, K.Chandra Sekhariah, "Cross Layer Based Security in Manets", *International Journal of Advanced Research in Computer Science(IJARCS), INDIA,* page 57-60, Vol. 4, No.4, May 2013.
16. K.Suresh Babu, K.Chandra Sekhariah, "CLDASR: Cross Layer Based Detection and Authentication in Secure Routing in MANET", *IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.4, No2, April 2014.*

.

AUTHORS PROFILE

Dr.K.Suresh Babu has done his Ph.D. from JNT University, Hyderabad in the field of Network Security in MANETs. He completed M.Tech(Computer Science) from Central University, Hyderabad. He has a teaching experience of 12years. His subjects of interests are Computer Networks, Network Security, Wireless Networks and Mobile Computing, Security in Mobile Computing. He published several papers in international journals and national journals, also participated and presented papers in International and National Conferences. He is presently course coordinator for M.Tech

(Computer Science). He is also Program Officer for Nation Service Scheme(NSS) Unit at School of IT. He is also Cisco Certified Academy Instructor(CCAI).

S.Saikumar is doing his M.Tech (Computer Networks and Information Security) from School Of Information Technology, JNT University Hyderabad. His Subjects of interest are Computer Networks, Network Security, Wireless Networks and mobile computing.