Enhancement of MANET Security using Cross-layer Technology

Dr. K Suresh Babu, C. Sathvik

Abstract

Adhoc networks are an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. However, this flexibility is accompanied with new security threats. Furthermore, many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where MANET use might be expected. In this paper we propose a **cross layer based defense enhancement technique (CBDET)** to resolve the above mentioned issues. The technique is supported by our simulation results.

1.Introduction

Mobile Ad-hoc Network:

MANET stands for "Mobile Ad hoc Network". It is a infrastructure less wireless network in which the nodes can move randomly resulting in a dynamic topography.[1]. In MANET, nodes can directly communicate with all other nodes within their radio ranges. If the nodes are not in the communication range then the nodes use the intermediate nodes to communicate with each
other.[2]. It is a network in which a set of mobile nodes communicate directly with one another without using an Access Point (AP) or any connection to a wired network. Here the nodes are free to move randomly and they organize themselves arbitrarily.[3] A MANET has applications in emergency search-and-rescue operations, in the battlefield, in data acquisition operations in hostile terrain, etc.[4]. The nature of nodes in MANET that they are dependent over the cooperative behaviour of its neighbour nodes has raised security concerns. In an ad hoc network attackers can attack the network from any direction at any node that is different from the fixed hardwired networks with physical protection at firewall gateways. .

Security attacks in MANET:

The characteristics of MANET such as infrastructure less network, mobility of nodes, closure communication medium, lack of centralized control and frequent topology changes brings more security risks in the network. The use of wireless links makes MANETs vulnerable to attacks.[5]. Since, MANET is a wireless network; security is entirely different from many fixed hardwired networks. Attacks can be occurred at any node from any direction. Therefore, every mobile node in the network must be equipped with security mechanisms.

Cross-Layer Design:

MANETs have to take in their account the basic inherent characteristics of the network which are: Dynamic topology, variable link capacity and bandwidth constraints, energy constraints nodes and multi-hop communications. All these characteristics are seriously challenged the OSI layer design which is characterised by the modularity , and permit to create a new methodology named Cross-layer.

Cross-layer design breaks away from traditional network design, where each layer of the protocol stack operates independently and exchanges information with adjacent layers only through a narrow
interface.[6]. In the cross-layer approach information is exchanged between non-adjacent layers of the protocol stack, and end-to-end performance is optimized by adapting each layer against this information Cross-layering is not the simple replacement of a layered architecture, nor is it the simple combination of layered functionality: instead it breaks the boundaries between information abstractions to improve end-to-end transportation. The Cross Layering has the following features.

- By giving out and distributing information on multiple layers, cross layer approach becomesan efficient mechanism to deal with traffic in the network. Further, the information gathered in a layer can be used in other layers to regulate the

ISSN: 2278 – 1323

performance of the protocol. [7].

- Using cross layer architecture, protocols are aware of their network current state from the point of local node. Further, Quality of Service (QoS) of applications can be enhanced by cross layer approach.[8].
- The overall performance of adhoc networks like wireless sensor network (WSN), mobile adhoc network (MANET) and wireless mesh networks (WMN) are enriched using cross layer architecture. [9].
- It resolves many open issues in MANET by sharing network information in multiple layers while still maintaining separate layers.[10].

2.CBDET (Cross Layer Based Defence EnhancementTechnique):

2.1 Overview:

CBDET is a cross layer based mechanism to detect the malicious nodes and to provide security by making AODV to change its path avoiding the malicious node . It gathers various features from the bottom three layers of the OSI model, by providing cooperation between the layers. Based on this features, the CBDET tries to provide the security to the mobile Ad Hoc network. In this technique, after deploying nodes in the network, using the physical layer, each node measures its energy levels, and is calculated each time a node forwards the packet.

Each individual node maintains this value. AODV checks for this value at each node in its path and if the value doesn't fall in the limits of threshold values then it stops forwarding the packets through that node, and changes the path of communication.

Energy, a physical layer parameter is used by network layer for choosing the secure routing path.

2.2 Calculation of energy at each node

each node calculates its residual energy (E_r), using energy model.

iEnergy = iNode->energy_model()->energy()

...(1) (in aodv.cc)

iNode = present node

iEnergy = E_r ,residual energy of that particular node.

2.3 Deciding the threshold values

Generally, energy consumption of a node is mainly due to the transmission and the reception of data or controlling packets (such as RREQ, RREP, RERR, HELLO). Let us take an example of Selfish Node (or) an eavesdropping node. In the case of Selfish Node the energy levels will be high as it does not forward the control packets(RREQ packet). Whereas for a eavesdropping node this metric will be lesser than the normal. So the limit (99,18) is set as the threshold values for Er. (we are assuming that the energy of malicious node will be different from a normal node i.e. either more or less.)

E_{th} = (99, 18)

E_{th} = threshold energy

Upper limit(E_{thu}) = 99 and

Lower limit(E_{thl}) = 18.

2.4 Proposed Algorithm

If S (source) wants to send data to D (destination) then

{

AODV ( ) // finds a route between S and D.

{

For (each node participating in communication between S and D)

{

Calculate energy of each node with the help of Energy Model

present energy of the node (E_r)

When any node receives a packet

{

If (E_{thl}<E_r<E_{thu})

{

Receive RREQ packet and forward it to next Hop.

}

Else

{

Drop RREQ Packet

It sends a RERR to the last node and source need to call AODV () again

}

}

}

}

}

3. Simulation Results

Simulation is done using ns2. We created an environment of 27 nodes whose characteristics are stated below.

ISSN: 2278 – 1323

Simulator	NS 2.35
Routing Protocol	AODV
Propagation model	Two Ray Ground
No. of nodes	27
Environment size	700 * 510
Traffic type	TCP
MAC	802_11
Initial Energy	100
Queue length	50

Table 1: showing the characteristics of simulation set up.

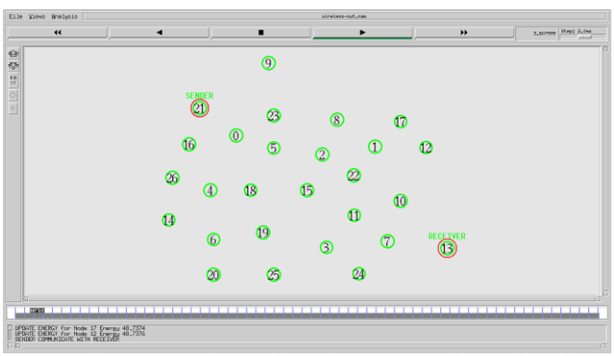

Fig 1: showing nodes with node 21 as sender and node 13 as receiver.

Communication takes place between 21 and 13 with route 21 -> 0 -> 2 -> 10 -> 13.

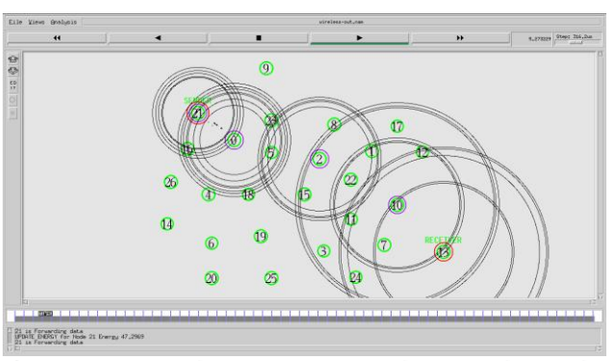

fig 2: Depicting the communication between the sender and receiver.

All the intermediate nodes are shown with a blue circle encircling them. Whenever the energy of a particular node comes down below 18, the AODV avoids that particular node. Here in this case there are 3 such nodes 0,2,10. The new route is shown below.

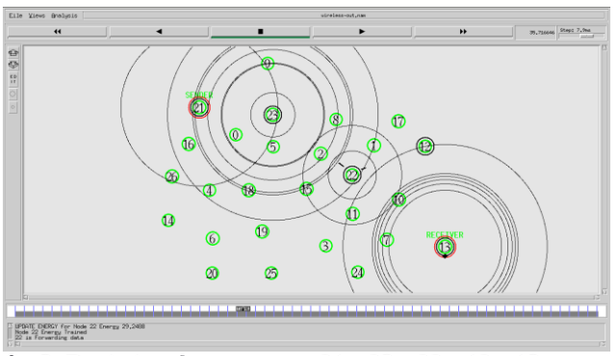

fig 3. Depicting the new route 21->23->22->12->13.

Thus the nodes with energy less than 18 (nodes 0,2, 10) are avoided using this algorithm as we are assuming these nodes to be malicious. (in real time a malicious node will drain its energy faster than that of the normal nodes).

4. Conclusion and Future scope:

In this paper, We have proposed a new technique (CBDET) 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 residual energy 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 selects a new route.

This algorithm can be extended to other metrics such as back-off time, mobility etc..,. to increase the probability of finding the malicious node.

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 AbderrahimBenslimane. "Toward a cross- layer monitoring process for mobile ad hoc networks." Security and Communication Networks 2.4 (2009): 351-368.

5. K.Suresh Babu, K.ChandraSekhariah, “Mobile Ad-Hoc Networks: A Novel Survey”, International Conference

ISSN: 2278 – 1323

On Advanced Computing And Communication Technologies
For High Performance Applications, FISAT, COCHIN, September 24-26' 2008, Vol. 1, Page.262 269.

6.K.Suresh Babu, K.ChandraSekhariah, "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.

[7] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta and Dr. .K.Bandhopadhyay," An Overview and challenges of routing protocol and MAC layer in Mobile Ad hoc network" Journal of Theoretical and Applied Information Technology© 2005 - 2009 JATIT.

[8] Eleonora Borgia, Marco Conti, and Franca Delmastro, "MobileMAN: Design, Integration, and Experimentation of Cross-Layer Mobile Multihop Ad Hoc Networks" IEEE Communications Magazine, Volume: 44 , Issue: 7 Digital Object Identifier: 10.1109/MCOM.2006.1668386, pp- 80-
85, 2006.

[9] Amardeep Singh and Gurjeet Singh, "Security in Multi-hop Wireless Networks" International Journal of Computer Science and Technology (IJCST) ISSN: 0976 – 8491, 2011

[10] NoureddineKettaf, HafidAbouaissa, ThangVuduong† and Pascal Lorenz, "A Cross layer Admission Control On-demand Routing Protocol for QoSApplications"International Journal of Computer Science and Network Security, (IJCSNS) VOL.6 No.9B, September 2006.

About the Authors

Dr.K.SURESH BABU did his Ph.D. from JNT University Hyderabad in the field of Network Secuirty in MANETs(Mobile Computing).He completed M.Tech.(Computer Science) from Hyderabad Central University(HCU), Hyderabad (India). He has a teaching experience of 14 years. His subjects of interests are Computer Networks, Network Security, Operating Systems, Wireless Networks, mobile Computing, Ethical Hacking and Wireless & Web Security. He has published serveral papers in both National and international Journals. He also participated and presented papers in International & National conferences and seminars.

Sathvik has received his B.Tech degree in Electronics and Communication Engineering in 2012 from Maheshwara Engineering College, Hyderabad, Telangana (India). He is crrently pursuing his M.Tech in Computer Networks and Information Security at School of IT, JNT University, Hyderabad. His areas of interest in research are network security and cryptography.

ISSN: 2278 – 1323