MALICIOUS ATTACK DETECTION AND PREVENTION IN AD HOC NETWORK BASED ON REAL TIME OPERATING SYSTEM ENVIRONMENT

JITHESH PUTHENKOVILAKAM

M-Tech Student, Electrical and Electronics Department, Amrita School of Engineering, Tamil Nadu, India,
jithesh_kovil@rediffmail.com

Abstract

This paper deals with Real Time Operating System (RTOS) based secure wormhole detection and prevention in ad hoc networks. The wormhole attack can form a serious threat to wireless networks, especially against many ad hoc network routing protocols and location based wireless security systems. A wormhole is created in the ad hoc network by introducing two malicious nodes. These two nodes form a worm hole link and message is transmitted through this link. The next part of the work is to detect the wormhole link by defining worm hole detection and prevention algorithm. After detecting suspicious links, one node performs a verification procedure for each suspicious link. The detection procedure and verifying procedure of suspicious worm link are used for further prevention of wormhole attack in the ad hoc network.

Index Terms: *An algorithm to detect worm hole attack in a wireless network…*

----------***----------

1. INTRODUCTION

An ad-hoc network is a decentralized wireless network in which each node can participate in routing by forwarding data to other nodes .A wireless network uses radio waves instead of cables to relay information to and from your computer. There is less need for technical support in setting up due to their simple nature .Even though the wireless networking provides many advantages, but it is also prone to many security threats which can potentially alter organization's overall information security risk profile. The reason is that in many organizations the security information flows through the wireless network .The worm hole attack is one of the those security threats. The proposed algorithm for worm hole attack detection and prevention can provide better understanding to a designer in setting up wireless networks which have high productivity with fewer security risks. The ad-hoc network which is free from worm hole attack will have the capacity to avoid unauthorized intrusions to a wireless network.

The wormhole attack is one of the severe malicious attacks, happening in the ad-hoc network .The two nodes in any end points in the network form a tunnel, known as worm hole tunnel. In this attack two existing nodes become malicious or two node can intrude into any point in the network and create worm hole link. These nodes are called worm hole nodes. In the wormhole attack, a worm hole node copies packets at one location in the network, tunnels them to another location through the another worm hole node. These packets can be retransmitted into the network or captured, depends on the intention of the attacker who establishes this attack.

The wormhole attack is very powerful, and preventing the attack is very difficult because all the nodes between the worm hole link are shielded or got bypassed A strategic placement of this worm hole link can result in a significant breakdown in communication across a wireless network. In the optimized link state routing protocol (OLSR), if a wormhole attack is launched routing is easily disrupted because of the combined effect of two worm hole nodes.

2. RELATED WORKS

In the paper by Farid Na¨ıt-Abdesselam[1] an efficient method is devised to detect and avoid wormhole attacks in the OLSR protocol. These methods first attempts to pinpoint links that may, potentially, be part of a wormhole tunnel. Then, a proper wormhole detection mechanism is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbours (endpoints of the wormhole).The proposed solution exhibits several advantages, among which its non-reliance on any time synchronization or location information, and its high detection rate under various scenarios .In the paper by Shalini Jain, Dr.Satbir Jain[2] a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means is presented. In the paper by Yih-Chun Hu [3] a general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and implementing leashes is presented.

3. SYSTEM ARCHITECTURE

A wireless network is set up using Zig Bee based on Optimized Link State Protocol Optimized Link State Protocol (OLSR) which is a proactive routing protocol, so the routes are always immediately available when needed. It is a proactive protocol which does not maintain the routing table even it does not want transmission. Proactive protocols produce higher routing efficiency than reactive protocol.

It provides low single packet transmission latency. Routing table structure is the main data structure where all needed information about the routes is stored. The routing table has the information about next hop as well as predecessor node. Initially a wired network consists of five nodes, is established. The first node communicate with the second one through DB-9 serial port connector, connected to the UART0 of ARM LPC2148..The UART1 of the second node communicate to the UART1 of the third node using another DB-9 connector and so on. The computer is used as fifth node.The handshaking messages traversed from node 4 are displayed on the hyper terminal of the computer which is the fifth node.

3.1 METHODOLOGY

OLSR uses control messages: Hello .Hello messages are used for finding the information about the link status and the host's neighbours. Each node in the network establishes bidirectional link with the neighbor node by transmitting and receiving Hello packet through single hop communication. The Hello packet contain information about source addresse,destination addresse,size of data message ,status of willingness.The typical hello message used here is "A008".A is the source address .'0' is the willingness bit.8 indicates the size of the data message transmitted in bits.

Upon receiving the node sends back "A1B8".Here willingness bit is changed to 1.B is the address of the second node. The wired network is changed to wireless network using Zig Bee. The Zigbee module is connected to the UART of ARM LPC2148 development board. Zigbee is a low power spin off of Wi-Fi. It is a specification for small, low power radios based on IEEE 802.15.4 – 2003 Wireless Personal Area Networks standard. ZigBee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless M2M networks. The ZigBee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz. The each ZigBee module is configured using X-CTU software before connecting to the node.

3.2 WORM HOLE ATTACK IN WIRELESS NETWORK

A particularly severe attack on routing protocols in ad hoc networks is the so-called wormhole attack in which two or more colluding attackers record packets at one location, and tunnel them to another location for a replay at that remote location

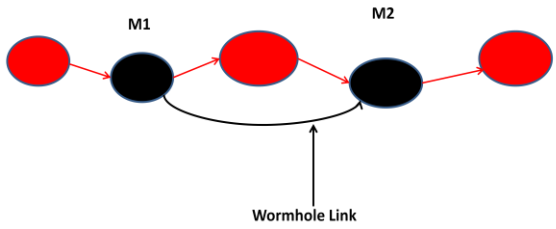

Figure 1 System Flow Diagram

The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. In such attacks two or more malicious colluding nodes create a higher-level virtual tunnel in the network, which is employed to transport packets between the tunnel endpoints. In this paper, we devise an efficient method to detect and avoid wormhole attacks in the OLSR protocol. This method have detecting suspicious link and verification procedure The proposed solution exhibits several advantages, among which its non-reliance on any time synchronization or location information, and its high detection rate under various scenarios.

We study the problem of characterizing the wormhole attack, an attack that can be mounted on a wide range of wireless network protocols without compromising any cryptographic quantity or network node. To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between two points in the network. A direct link can be established via a wire line, a long-range wireless transmission, or an optical link. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point, tunnels them through the wormhole link and replays them in a timely fashion at the other end, referred as the destination point. In the wormhole model, it is assumed that the adversary does not compromise the integrity and authenticity of the communication, and any cryptographic quantity remains secret.

4 DESIGN OF WORM HOLE DTECTION AND PREVENTION ALGORITHM

An algorithm for detecting and preventing the worm hole attack in wireless network and preventing the same is designed. Wormhole attacks are severe attacks that can be easily launched even in networks with confidentiality and

authenticity. The malicious nodes usually target the routing control messages that are related to the topology information or routing information. In this paper, we have presented an effective method for detecting and preventing wormhole attacks in OLSR. The proposed solution is an easy-to-deploy solution. It does not require any complex computation or special hardware. The performance of this approach shows high detection rate under various scenarios.

4.1 ALGORITHM

After network is set up data transmission is to be done. Each node has to store the details of immediate successor and predecessor nodes .When each node receives data succesfully,it has to send acknowledgement back to the predecessor within the time constraints.Store the details of all active nodes in the first node. Make node 2 and 4 worm hole nodes by creating a link between 2 and 4

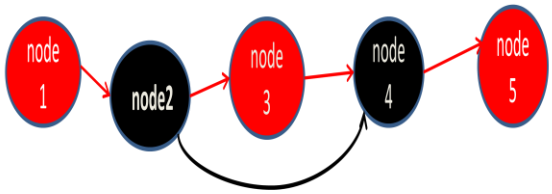

Figure 2 Event Flow Diagrams

The data transmission is started from node1.The node 3 and node 4 receives data from node 2.The node 4 forwards to node5.The node 3 receives data and sends to node 4.The node 4 does not respond to it as it is part of worm hole link. Within the time limits, Node 3 does not receive the acknowledgement from Node 4. It sends the information to Node 1 The Node 1 put successor node status as malicious. In the verification procedure, node 1sends probe packets to node2,4 and 5.From the response it confirms that worm hole link is established between 2 and 4.Node 2 and 4 is removed from the network by changing the link.The successful data transmission is done through node 1,3 and 5

5. EXPERIMENTAL SET UP

The hardware required for the wired network based on the OLSR is four ARM LPC2148 development boards and one personal computer, and DB-9 connectors. The hardware implementation of wireless network with worm hole detection and prevention include LPC ARM 2148 micro controller and Zig Bee. The network consists of five nodes, out of which four are ARM micro controllers and one is computer. The Zig Bee attached to each microcontroller act as transmitter as well as receiver. Upon setting up of bidirectional link successfully, a led on each node should blink. After this, data is transmitted from source to destination. The computer at the destination will have to display the received data. Afterwards node 2 and node 4 are made malicious. The worm hole detection algorithm executes after which isolate and monitor the worm hole link. This should prevent it and finally new network is established which is free from worm hole attack.

Figure 3: Zig Bee board

Figure 4 ARM LPC2148 DEVELOPMENT BOARD

6 PORTING ON RTOS

MicroC/OS-II (commonly termed as uC/OS-II), is a low-cost priority based pre-emptive real time multitasking operating system kernel for microprocessors, written mainly in the C programming language. It is mainly intended for use in embedded systems. uC/OS-II stands for Micro-Controller Operating System Version 2. The uC/OS-II is a highly portable, scalable, preemptive, real-time, multitasking kernel specifically designed for embedded applications

Porting is the process of writing the application code intended for a target on a specific OS or an RTOS. In classical definition porting is defined as “The process of adapting a Software so that an executable program can be created for a computing environment that is different from the one for which it was originally designed for”. For the port of uC/OS-II

to any target embedded platform we first need the uC/OS-II kernel, which is CPU independent. For any port this kernel will be the same. Now the CPU specific code for the corresponding embedded platform used is needed. The third requirement is the BSP corresponding to the board carrying the microcontroller or microprocessor. The code written in c for worm hole detection and prevention is ported on uC/OS-II and built into ARMLPC 2148 development board. The priorities are set for various tasks required to set up the ad-hoc network, introduce worm hole attack, detect and prevent it.

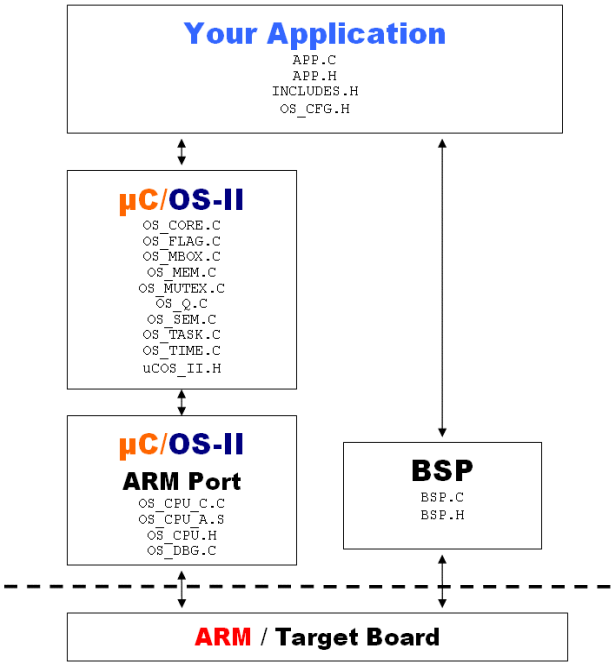

Figure 5 Code required for uC/OS-II Porting

CONCLUSIONS

The proposed algorithm used for implementing this project is developed keeping in mind the fact that it can provide better understanding to a designer in setting up wireless networks which have high productivity with fewer security risks. The wireless networking provides many advantages, but it is also coupled with new security threats which can potentially alter organization's overall information security risk profile.
Properly enhanced, this developed system will have the capacity to avoid unauthorized intrusions to a wireless network.

ACKNOWLEDGEMENTS

Author gratefully acknowledges the facilities available at the Amrita school of engineering, Coimbatore, sincerely thanks to my guide Dr.Madhu and Mr. Anu Kumar for helping me in theoretical and practical section.

REFERENCES:

[1]Issa Khalil, SaurabhBagchi & Ness B. Shroff, "LITEWORP: Detection and Isolation of the Wormhole Attack in Static MultihopWireless Networks". The International Journal of Computer and Telecommunications Networking, Vol. 51, Issue 13, pp 3750- 3772, 2007
[2] Issah Khalil, "Mitigation of Control and data traffic attacks in wireless ad-hoc and sensor networks" IEEE Vol. 6, Issue 3, pp 344-362
[3]Sun Choi, Doo-young Kim, Do-hyeon Lee &Jae-il Jung "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks" IEEE International Conference on Sensor Networks,Ubiquitous, and Trustworthy Computing SUTC'08.pp 343- 348,2008
[4] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Attacks in WirelessNetworks," In IEEE JSAC, Vol. 24, No. 2, pp. 370-380,2006

BIOGRAPHIES

Jithesh Puthenkovilakam is a student at at the Amrita University at Coimbatore and presently doing Master Of Technology in Embedded System. He received the BTech .Degree in Electrical and Electronics Engineering from the Kannur University .Post that he worked as a software Engineer .He was involved in avionics and automotive projects as a low level designer and programmer. In his thesis work at Amrita School of Engineering, he focused on security and performance in wireless ad hoc networks and malicious attacks. His research interests include systems and network security.