ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Multi-Hop Communication for Home Automation with Enhanced Security Using ARM and RTOS

Jithesh Puthenkovilakam

Assistant Professor, Electrical and Electronics Department, Cochin College of Engineering and Technology,

Valanchery, Kerala (India)

Abstract: This paper deals with the design of home automation system through multi-hop wireless communication using ARM. The multi-hop communication means the nodes within the network can able to communicate with the help of two or more nodes, which are acting as the relay nodes, between the source and destination node. In the computer program the user can create actions what should happen with devices connected to the destination node in the network. The end devices such as monitoring equipment using sensor, industrial motor, power transmission equipment, network equipment for routing and data transmission, automotive robot can be connected to the destination node depend on real time application and automation. This real time control and monitoring is achieved using uC/OS-II based ARM system with minimum power consumption and highly enhanced secure avoidance of malicious attack.

Keywords: OLSR based multi-hop communication with enhanced secure avoidance of malicious attack.

I. INTRODUCTION

The OLSR based 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 Study of wireless network protocols to implement multi-hop communication and detection of malicious attacks has been an active area of research for past several years. 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 with minimum power consumption. Properly enhanced, this developed system will have the capacity to avoid unauthorized intrusions to a wireless network and thus providing highly efficient home automation using multi-hop communication and
uC/OS-II based ARM system.

The malicious attacks such as wormhole attack is very dangerous to wireless network, powerful and preventing the attack has proven to be very difficult. A strategic placement of this intruder 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. Here to avoid it en efficient algorithm is introduced to detect and prevent it with minimum power consumption and developed on real time operating system. This makes the secure multi-hop communication to automate the end devices devoid of security threats. To achieve this priority based pre-emptive scheduling is used with the help of real time operating system and is ported on ARM microcontroller.

II. RELATED WORK

An In the paper by Farid Na¨ıt-Abdesselam[1] an efficient method is devised to detect and avoid wormhole attacks in the OLSR protocol in multi hop wireless system for home automation. 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 .Even though this 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 ,but is less efficient and predictable in comparison with uC/OS-II based ARM system .The controlling of the end devices are easily blocked in the case of security threat in the earlier method. 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 to achieve secure multi hop communication. In the paper by Yih-Chun Hu [3] a general mechanism, called

DOI 10.17148/IJARCCE

packet leashes, for detecting and thus defending against malicious attacks, and implementing leashes is presented to establish multi-hop communication.

III. ARCHITECTURAL VIEW OF SYSTEM

There are 4 components in the network providing multi-hop communication. Through the user interface, controlling action goes to node 1 which in turn gives to node 2 and finally it reach the node 4 through hop to hop communication. The JARM Board-LPC2148 is used for making nodes in this OLSR based wireless network system. A PC can be connected to source node displays the input on hyper terminal that is transmitted over hop to hop communication. The end point of destination node can be used to connect the electrical devices which can be controlled remotely by the user. This 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. As implementation of proactive protocol power saving mode registers of ARM are selected, it enhances the performance because it ported on real time operating system with priority based pre-emptive scheduling. 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. . The handshaking messages traversed from node 4 are displayed on the hyper terminal of the computer which is the fifth node.

IV. SYSTEM METHODOLOGY

JARMBoard-LPC2148 is a development board for LPC2148 ARM7TMDI based microcontroller. The LPC2148 microcontroller has 512KB of internal flash and 32+8K RAM, can be clocked up to 60Mhz. LPC2148 features include USB 2.0 device, 2xUARTs, RTC, 2x10bit ADCs each with multiple channels, 1xDAC,2xI2C, 1xSPI, 1XSSP, 2x32-bit TIMERS, 6XPWM, FAST I/0 support and WDT.LPC2148 also supports In System Programming (ISP).For efficient handshaking, OLSR uses control messages .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. Power saving mode of LPC2148 and ZigBee ensures the high productivity with fewer risks. 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. 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 which facilitate multi-hop communication.

V. DESIGN OF PREVENTION ALGORITHM TO PROVIDE SECURE MULTI-HOP COMMUNICATION

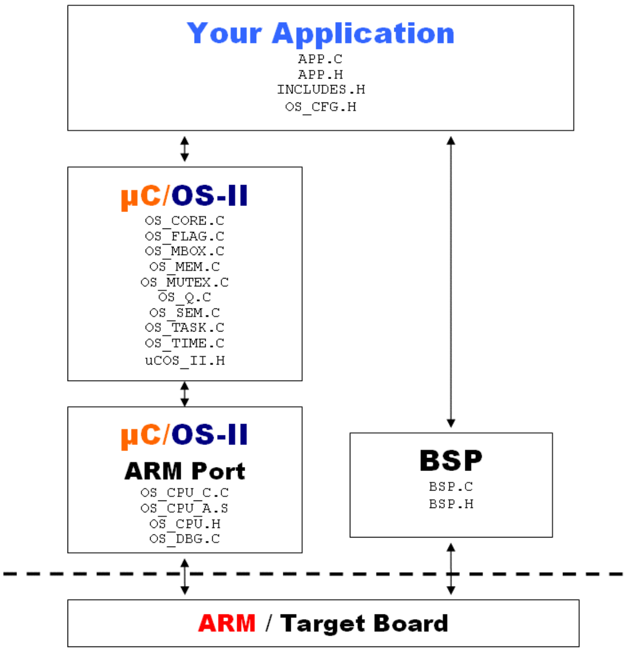
An algorithm for detecting and preventing the worm hole attack in wireless network providing multi-hop communication for automation of real time end devices using power saving mode of ARM based real-time operating system is designed. Wormhole attacks are severe attacks that can be easily launched even in networks with confidentiality and authenticity. The malicious nodes usually target the routing control messages that are related to the

DOI 10.17148/IJARCCE

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 operation of end devices is easily monitored using priority based real time interrupt programming. After network comprised of five nodes, 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 successfully, 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.The performance of this approach shows high detection rate under various scenarios. If threat is detected, it immediately stops the operation the end devices being automated and displays the error signal.

VI. SOFTWARE DESCRIPTION AND PORTING ON UC/OS-II

The µVision IDE from Keil combines project management, make facilities, source code editing, program debugging, and complete simulation in one powerful environment. The µVision development platform is easy-to-use and helping you quickly create embedded programs that work. The µVision editor and debugger are integrated in a single application that provides a seamless embedded project development environment. uC/OS-II stands for Micro-Controller Operating System Version 2. It 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. The uC/OS-II is a highly portable, scalable, pre-emptive, 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. 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 and introduce multi hop communication using OLSR and control the end devices. The program developed on real time operating system can provide home automation with highly secure avoidance of network threat. By introducing the malicious attack and removing it ,it can be validated and verified. Offering unprecedented ease-of-use, µC/OS-II is delivered with complete 100% ANSI C source code and in-depth documentation. µC/OS-II runs on the largest number of processor architectures, with ports available for download from the Micrium Web site. µC/OS-II manages up to 250 application tasks. µC/OS-II includes: semaphores; event flags; mutual-exclusion semaphores that eliminate unbounded priority inversions; message mailboxes and queues; task, time and timer management; and fixed sized memory block management.



VII. CONCLUSION

The proposed algorithm used for security threat free system to automate the end devices is able to provide highly efficient multi hop communication. It can detect and prevent malicious attacks in wireless network is developed keeping in mind the fact that it can provide better understanding to a designer in setting up wireless networks with minimum power consumption using ARM and real time operating system .It also eliminate risk of security threat. The wireless networking provides many advantages which can potentially alter organization's overall information security risk profile if this algorithm with power saving mode of ARM is used. The developed system will have the capacity to avoid unauthorized intrusions to a wireless network without affecting the performance of the automation.

ACKNOWLEDGMENT

Author gratefully acknowledges the faculties available at Cochin College of Engineering and Technology, Valanchery and the Amrita school of engineering, Coimbatore, sincerely thanks to my guide **Dr. Kumar** and **Mr. Vineeth** 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 Multihop Wireless 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 Wireless Networks," In IEEE JSAC, Vol. 24, No. 2, pp. 370-380,2006

BIOGRAPHY

Jithesh Puthenkovilakam is presently working as Assistant Professor in the Department of EEE, Cochin College of Engineering, Valanchery, Kerala, India. He did Master of Technology in Embedded System. from the Amrita University at Coimbatore. He received the B.Tech .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. He has published papers in national and international journals on wireless and embedded system. His area of research interest includes modelling and simulation of wireless networks, robotics and electrical power applications. He is guiding B.Tech students in the area of embedded systems and Wireless Networks .In his paper work at Cochin College of Engineering, he focused on security and performance in wireless ad hoc networks and malicious attacks.

DOI 10.17148/IJARCCE