ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

MICROCONTROLLER BASED HARDWARE IMPLEMENTATION OF ADHOC NETWORK

Reji.M, Krithika.B
Dept. of Electronics and Communication, Saveetha School of Engineering, Chennai, India.
Email: rejime@gmail.com

Received on: 15.08.2016 *Accepted on: 20.09.2016*

Abstract

In this project hardware implementation of single hop ad-hoc network is implemented and analysed using microcontroller. The protocol implemented in this project is primarily based on, Ad hoc On-Demand Distance Vector routing. We adopt On Demand Distance Vector routing solely based on source routing and "On Demand" process, so each packet does not have to transmit any periodic routing information. We use standard metrics to test the performance of the wireless ad hoc networks based on average delay time, delivery ratio of data packets, and throughput.

Keywords: ad-hoc network, AODV, Zigbee, Microcontroller, Routing Protocol, hardware implementation.

I. Introduction

With the appearance of remote systems, the uses of MANETs [1] are boundless from pursuit and salvage operations to individual region systems. Such applications are portrayed by the absence of interchanges framework and focal power. At the same time frequently the nature of administration or the security of the information must be traded off. These properties make MANET very appropriate in numerous fields [2], as in a war zone, salvage operations and individual region systems.

II. Related Works

In this area we survey the current secure directing conventions. There exist numerous protected directing conventions in MANET. These protected conventions can't alleviate a wide range of assault confronted by MANET systems. These conventions are more subjected in distinguishing and disposing of certain class of assaults. These conventions while moderating assaults corrupt the QoS of the system to a huge degree. This inadequacy request a more secure convention, which can alleviate dominant part of the assaults, such that the QoS is not affected.

Sanzgiri et.al [7] have proposed Authenticated Routing for Ad hoc Networks (ARAN), which utilizes lopsided cryptography. Since, it utilizes open key encryption secrecy is ensured and system structure is not uncovered. Despite the fact that the convention keeps up a high PDF, it requires additional memory, alongside high handling overhead for encryption. It is still defenseless against assaults such as a dark gap, wormhole and hurrying assaults. Zapta et.al [8] have proposed Secure-AODV (SAODV), which utilizes computerized marks to confirm non-changeable fields of the directing control messages and one-way hash chains, subsequently securing jump number data. The convention is strong against assaults such as Dos and Black-opening. Be that as it ay, there are potential outcomes of MIM [9] assaults by trespasser hubs. Papadimitratos et.al has proposed SRP, which keeps up a security relationship in the middle of the source and the destination. It can avert manufacture and circles made by malignant hubs. Be that as it may, it experiences reserve harming and wormhole assaults. Wan et.al hasdisplayed a convention (UBSOR-Unobservable Secure on-Demand Routing Protocol) which accomplishes high protection in receptive steering. It shrouds the substance of the bundles by encryption techniques. In any case, it needs outsiders to build up the key, and can't deal with wormhole assaults.

Li et.al [10] have proposed a Trusted AODV (TAODV) steering convention. It utilizes trust suggestion and later on consolidating these to determine a legitimate conclusion. It trades, trust by means of two bundles called TREQ and TREP, which is an additional overhead.

The computational overhead of every validation operation is high, and it might even prompt high activity when there are numerous noxious hubs. Saha et.al [11] have proposed a directing convention, which depends on the idea of loyalty. Devotion is a whole number that is connected with every hub. The methodology lessens the computational overhead to a great deal degree. Be that as it may, the convention can't manage shakedown assaults, nor would it be able to manage greyhole assault successfully. It requires investment to identify and dispense with a vindictive hub from the system.

Dhurandher et.al have introduced a convention (FACES-Friend-Based Routing Protocol) which decides trust of the hubs by sending difficulties and sharing companions' rundowns. Difficulties are sent to validate the hubs, and as needs be they are set in companion rundown or question mark list. Companions are appraised on the premise of the measure of information they transmit and rating got from different companions. In any case, it neglects to battle wormhole or hurrying assaults. In addition, the control overhead is expanded because of occasional flooding of test parcel, and intermittent sharing of companion rundown.

III. Design And Development

Our aim is to give a protected, dependable and ease equipment convention for MANETs. This gets executed through devotion. A second level of dependability is gotten through suggestions and report bundles. This recognizes the noxious nodes, as well as dispose of them from the system.

Subsequently, keeping up a decent QoS for the system. Our fundamental objective of the convention is to construct an ease MANET, which is utilized viably and inexpensively, in a secured way; both in fields such as safeguard and residential.

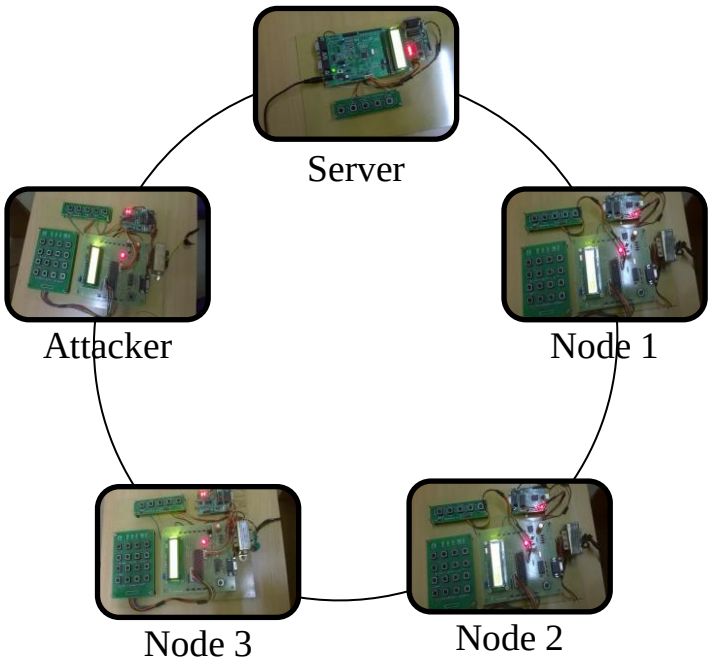

Fig:1 Block Diagram.

The components usedin making the server and nodes are liquid crystal display (LCD), keypad, microcontroller, ZIGBEE, ARM processor and Analog to digital converter (ADC). The information is transferred from server to the nodes. Where the attacker node or hacker node affects the information sent. Therefore, there is a reduction in the packet delivery ratio (PDR) and increase in average delay time. In case of absence of attacker node we find that there is an increase in packet delivery ratio (PDR) and also decrease in average delay time.

III. Experimental Results

We have recreated the convention on the equipment, with every one of the transmitters fitting in with the same PAN ID. While setting up the ZigBee modules it is to be remembered that every one of the hubs must fit in with the same system ID, generally the handset won't identify any signs from alternate hubs. We have taken the id of the hubs as 1, 2 and so on., yet it can be taken as the IP location of the hubs. In our re-enactment, we have considered that one and only hub is sending information and one hub is getting information, alternate hubs go about as a steering hub. Basic

cryptographic images are utilized as a part of the steering calculation, which can be specially crafted by utilization of the system. Hubs move in a 50*26 meter locale, with every hub's transmission range as 15m. In the principal re-enactment, we consider three nodes. The destination hub is not in the source's extent, so the source sends a solicitation to the closest middle hub, i.e., Node 1. Hub 1 finds the destination hub in its neighbour table, and sends the solicitation straightforwardly. The destination answers, which is sent back to the hub. After, the source hub has gotten the ACK, it builds the devotion of Node 1 by one. Hub 1, does not expand the devotion of the destination hub, since it has been accepted that the destination hub is non-malignant.

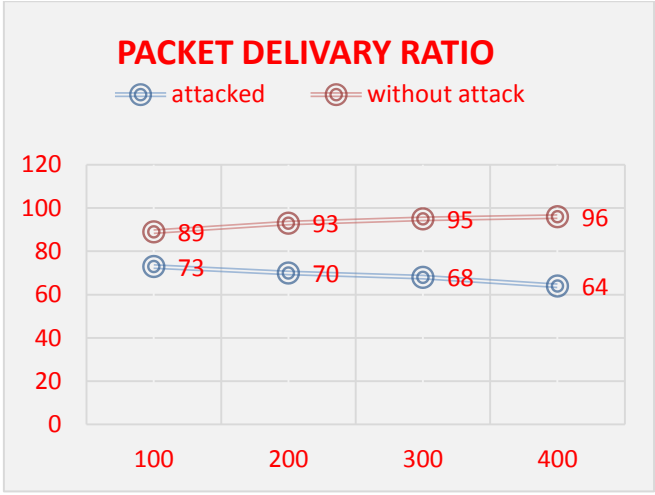

Fig:2 Experimental result for PDR.

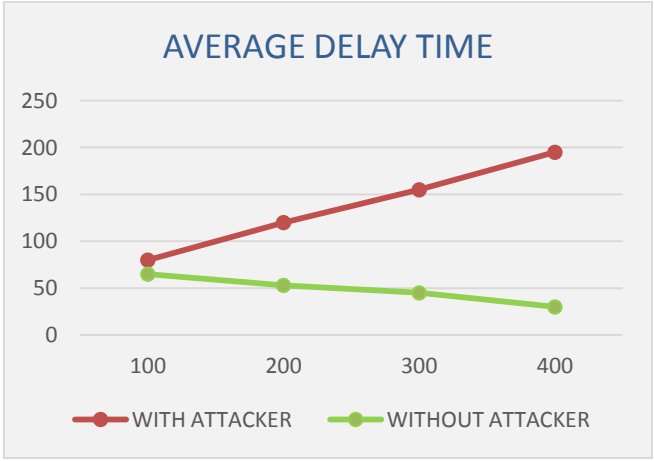

Fig:3 Experimental result for Average Delay Time.

In the following recreation, we consider four nodes. The source hub now has two neighbour hubs. Since, Node 2 has constancy zero, the source sends the solicitation to the destination through Node 1. After the source hub gets an answer from the destination, it advances the information from the same course. Give us a chance to assume that Node 1 is a noxious hub, with greyhole assault; then it will drop the ACK bundle rolling in from the destination hub. After the sitting tight time for the source hub is over, it decreases the constancy of Node 1 by one. The server sends a course demand to Node 2, sends the information effectively and its devotion is expanded by one.

IV. Results

A broad recreation model having situation of 10 versatile hubs is utilized to think about between layer collaborations with a territory of 50 meter x 26 meter, with every hub's extent as 15 m. We have considered Node 1 as the source and Node 10 as the destination node. We change the quantity of hubs from 2 to 10, with the portability model as an irregular waypoint model. The normal rate is 1 m/s with respite time of 30 seconds.

At the point when each of the 10 hubs begin steering and couple of transmissions have occurred, the hubs 2, 6, 8 are made malevolent, and they begin their assault in a steady progression. We have adjusted the positions of the middle hubs haphazardly and taken the normal estimation of all such hub situations. The same situation has been likewise utilized for execution 46 Hardware Implementation of Fidelity in light of Demand Routing Protocol in MANETs assessment of other secure conventions with which our convention has been analyzed i.e. ARAN, SAODV, TAODV. We consider these conventions as they are surely understood among the safe on interest directing conventions. Additionally, we attempt to demonstrate that our convention stands route superior to the next secured convention.

In the first place, we figure the parcel conveyance portion (PDF) for every one of the conventions. The chart demonstrates that FBOD demonstrates a normal PDF of 89.6%, which is diminished to 83.25% in vindictive environment. Other convention demonstrates vacillations in benevolent and fall in a malignant domain, since none can dispense with the malevolent hubs. FBOD then again, utilizes bundles like report and proposal to boycott the malevolent hubs. Once the vindictive hubs get boycotted, the parcel conveyance division increments, as on account of FBOD. Second, we figure the standardized steering load (NRL) for the conventions as appeared in Fig. 20, 21. In the kindhearted environment, the normal NRL for FBOD convention is 0.82, which increments to 1.05 in malignant environment. TAODV indicates high NRL, because of its additional parcels to assemble trust. SAODV and ARAN similarly demonstrates normal NRL, since with incorporation of pernicious hubs parcel of confirmation procedure needs to occur. If there should be an occurrence of FBOD, however constancy it quantifies the trust of the neighbour, and also takes out these pernicious hubs from the system.

Fig:4 Delay Time.

Fig:5 PDR Result.

Fig:6 Without Bad Node.

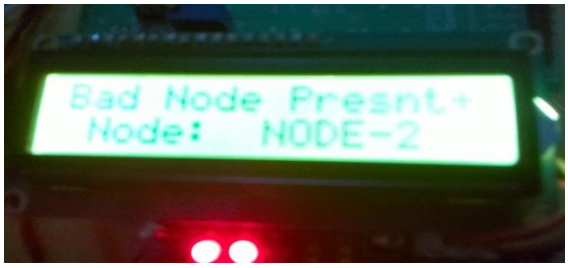

Fig:7 With Bad Node.

At long last, we figure the end to end delay for the conventions in kind hearted environment as appeared in Fig. As the quantity of hubs build, the end to end delay increments. Our convention demonstrates a normal deferral of 15.2 sec in kind and 20.9 sec in malevolent environment. Our convention demonstrates a littler increment at last to end delay, contrasted with other convention, since we can successfully identify and dispose of pernicious hubs, there taking the system back to steadiness. Also, we don't utilize substantial parcels like TAODV, or overwhelming validation plans like SAODV and ARAN, which builds the deferral.

V. Conclusion

Our proposed model has numerous interesting components which makes it stand not quite the same as other existing secure on-interest conventions. AODV is a lightweight convention and doesn't require any flooding of additional bundles or additional memory, which is not in the situation of TAODV and ARAN. Also, it is a unicast convention, in this manner making the system free from numerous assaults. The safe course determination mitigates assaults like wormhole and surging assault, which is not in the situation of SAODV. As the constancy of different hubs builds the odds of black hole hub getting chose will diminish. In addition, the tally esteem screens the greyhole and extortion assaults effectively. In our convention, devotion parameter guarantees that just reliable hubs are available in the system. The utilization of the bustling hold up keeps the cycling of RREQ parcels. Parcels like report and proposal

help in rapidly distinguishing pernicious hubs and killing them from the system. Once the vindictive hubs are killed, the NRL diminishes back to that on account of amiable environment. We can have watched that our equipment execution works preferred in malevolent environment over other well-known secure steering conventions, with high PDF, low NRL and normal End-to-End delay; thus making it economically practical.

VII. Reference

1. R.K. Nekkanti and C.W. Lee, "Trust based adaptive on demand ad hoc routing protocol," In: Proceedings of the 42nd Annual Southeast Regional Conference, pp 88–93, 2004.
2. S. Sharmila1, G. Umamaheshwari and M. Ruckshana,"Hardware implementation of secure aodv for wireless sensor networks," ICTACT Journal On Communication Technology, Vol.1, Issue 04,pp.218-229, December 2010
3. S. Corsonandz J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," Network Working Group, RFC: 2501, January 1999.
4. M.Frodigh, P. Johansson and P. Larsson, "Wireless ad hoc networking: the art of networking without a network," Ericsson Review, No. 4, pp. 248-263, 2000.
5. R.K. Guha, F. Zeeshan and M. Shahabuddin, "Discovering man-in-the-middle attacks in authentication protocols," Military Communications Conference, MILCOM IEEE, pp 29-31, October 2007.
6. M. Zapata and N. Asokan, "Securing ad hoc routing protocols," In: Proceedings of the 1st ACM Workshop on Wireless Security (WiSe), pp.1-10, September 2002.
7. A. Passarella and F. Delmastro, Multi-hop Ad hoc Networks from Theory to Reality, Nova Science Publishers,ch.9,2007, pp.153-177.
8. K. Sanzgiri, B. Dahill, B.N. Levine, C.Shields and E.M. Belding-Royer, "A secure routing protocol for ad hoc networks," In: Proceedings of 10th IEEE International Conference on Network Protocols (ICNP), pp.78-87, November 2002.
9. S. Dalu, M.K. Naskar and C.K. Sarkar," Implementation of a topology control algorithm for manets using nomadic community mobility model," Industrial and Information Systems, pp.1-5,2008.
10. H.N. Saha, D. Bhattacharyya, P.K. Banerjee,"Fidelity based on demand secure (FBOD) routing in mobile adhoc network," Advances in Parallel Distributed Computing, Springer Berlin Heidelberg, pp 615-627, 2011.
11. K. Komali, V. Mahesh and R.Y. Kumar, "A novel secured protocol for data transmission in ad hoc networks using clustering," (IJCSIT),Vol. 5(5),pp. 6567-6571, 2014.